



Cyber Glossary

3462 terms collected from the sheets in this collection; [brackets] name the source sheets

A

AAA — Authentication, Authorisation, Accounting: the switch asks a central server (TACACS+ or RADIUS) who may log in, what they may run, and records what they did. *[Access Switch Audit Grid: DAT-NT-025 R1-R71; CISSP Domain 4: Communication and Network Security]*

AAA / RADIUS / TACACS+ — Authentication, Authorization, Accounting; RADIUS (Remote Authentication Dial-In User Service, UDP, used for Wi-Fi 802.1X and VPN) and TACACS+ (Cisco, TCP, for network device admin logins). *[Networking Ports and Protocols]*

AAB — Android App Bundle: the upload format required by Google Play for new apps since August 2021; Play builds and signs device-specific split APKs from it. *[Android Application Internals and Security]*

AAL — Authenticator Assurance Level in NIST SP 800-63B (Digital Identity Guidelines): AAL1 single factor, AAL2 two factors, AAL3 hardware-based phishing-resistant. *[Identity Protocols: OAuth, OIDC, SAML, FIDO2]*

AAL (Authenticator Assurance Level) — NIST SP 800-63B strength of authentication: AAL1 single factor, AAL2 two factors, AAL3 hardware-bound phishing-resistant. *[CISSP Domain 5: Identity and Access Management]*

ABAC — Attribute-Based Access Control: policies on subject attributes (clearance, role), resource attributes (classification, owner) and environmental attributes (time, location, patch state of the device). Basis of the PA-111 architecture. *[ANSSI Zero Trust Model]*

Abend — Abnormal end of a batch job; reruns must be authorized and logged. *[CISA Domain 4: IS Operations and Business Resilience]*

ABM (Apple Business Manager) — Apple web portal where the organization owns its device serial numbers (from Apple or authorized resellers), assigns them to an MDM server and manages Managed Apple Accounts. *[macOS Security for Defenders]*

Abstraction and orchestration — The two techniques that make a cloud: resources are abstracted from physical hardware into

pools, and orchestration software carves and delivers them to consumers on demand. Security therefore moves to the APIs and consoles that drive the orchestration. *[CSA Security Guidance v4: the 14 Domains]*

Abuse cases and antipatterns — Abuse case = misuse story written next to each user story ('as an attacker I replay the reset link'); antipattern = recurring bad design (shared service account, flat network, hard-coded secret). *[Compliance, Threat Modeling and AI Security]*

Acceptable — No known security risk; may be used. *[NIST Cryptographic Standards]*

Accès de proximité / Close access — Attacks over wifi and radio waves. **Accès local** (also 'close access'): attacks with physical access to the network. Both differ from remote access. *[ANSSI CyberDico FR/EN Glossary]*

Access (accès) — A copy of the container key encrypted for one recipient: under a password-derived key, a certificate (RSA public key) or a functional key. *[ANSSI Encryption Tools: Zed! and Cryhod (1/2, Zed!)]*

Access mask — bit field of rights requested on an object; for processes 0x0010 = PROCESS_VM_READ, 0x1000 = PROCESS_QUERY_LIMITED_INFORMATION, 0x1FFFFFF = PROCESS_ALL_ACCESS. *[Windows Internals for Defenders]*

Access port — Belongs to one data VLAN, sends and receives untagged frames; may add one **voice VLAN** carried tagged to the IP phone (the phone learns it via CDP or LLDP-MED, LLDP Media Endpoint Discovery). *[Switching: VLANs, Trunks, Spanning Tree, EtherChannel]*

Access tier — Edge switches where endpoints, phones and access points connect. Enforces port security, 802.1X and VLAN assignment; provides Power-over-Ethernet (PoE). *[Classic Enterprise Network Architecture]*

Access token — Bearer credential the client presents to APIs (e.g. UserInfo); whoever holds it can use it. *[ANSSI Identity: MFA, AD Tiering, OpenID Connect; Identity Attacks and ITDR: Entra ID and Okta]*

Account lockout — throttle after few attempts per window *[Network and Authentication Attacks]*

Accountability — Answerability for an outcome; stays with the owner even when the work is delegated. *[CISM Domain 1: Information Security Governance]*

Accountability (9.3) — Responsibility (roles assigned, per SP 800-130 framework for key management systems) and traceability: any access to a plaintext key SHALL be traceable to the human, device or process. *[Crypto Mechanisms, Key Policy and AES Internals]*

Accounting — Recording what the identity did and for how long (login events, RADIUS accounting records, session logs) for billing, audit and investigation. *[Fundamental Security Concepts]*

Accreditation (homologation) — Formal acceptance of the residual risks of a system by its accreditation authority before go-live; the baseline chosen (ANSSI level, CIS profile), the compliance reports and the residual risks are part of the file (PA-097 R1: refurbished computers must be covered too). *[ANSSI Endpoint Security: Overview and Windows]*

ACID — Atomicity, Consistency, Isolation, Durability: properties of reliable database transactions. *[CISSP Domain 8: Software Development Security]*

AcidRain — Wiper malware for MIPS-based modems and routers, found by SentinelLabs after the KA-SAT attack: it overwrites flash storage and device files, then reboots, leaving the device unusable. Defence: signed firmware with a protected recovery image, and control of who can push files or commands to the fleet. *[Space and Satellite Security]*

ACK — Acknowledgement number is valid; set on every segment after the SYN *[TCP and UDP Deep Dive]*

ACL — Access Control List: extra per-user or per-group permissions beyond owner/group/other (setfacl, getfacl). *[Linux Security Command Line]*

ACME — Automatic Certificate Management Environment (RFC 8555): protocol used by Let's Encrypt and others to prove domain control and issue certificates without humans. *[TLS and Certificates in Practice]*

Acquirer / PFI — Acquirer = the merchant's bank for card payments, told first of a card-data breach; PFI = PCI Forensic Investigator it may require. *[Reporting and Communication]*

Acquisition — Bit-for-bit image with a hardware write blocker (disk) or a trusted agent (memory, cloud snapshots, mobile via Cellebrite/GrayKey); hash before and after; work only on copies. *[Incident Response, Forensics, Automation]*

ACS (access control services) — PCIe feature that forces peer-to-peer traffic up to the IOMMU; without it, devices behind one switch share an IOMMU group. *[Virtualization Internals and VM Isolation]*

Action plan types — Configuration management (baseline fix), patching (version upgrade), compensating controls (WAF, segmentation), awareness / education / training (phishing, secure coding), changing business requirements (retire the feature or system). *[Reporting and Communication]*

Actions on Objectives — exfiltration, integrity or availability attacks, lateral hop *[Pentest Methodologies]*

Activation secret (Sec. 3.2.10) — PIN or biometric verified locally to unlock a multi-factor authenticator; not sent to the verifier. *[Digital Identity Guidelines SP 800-63-4]*

Active defence — Honeypot (decoy host), honeynet (decoy network), honeypot / canary (fake credential, document, AWS key that alerts when used). Legal: deception yes, hack-back no. *[Threat Intelligence, Hunting and SOC Efficiency]*

Active PFC — Power factor correction: brings PF (real watts / apparent volt-amperes; 1.0 = ideal) near 0.99 and allows auto-ranging 100-240 V input; old PSUs had a manual 115/230 V switch (wrong setting = dead PSU). *[Power, Displays, Peripherals and Printers]*

Active scan / spider — The proxy sends its own crafted requests (spider = follows links to map the site; active scan = injects test values). Only for targets you are authorised to test. *[Web and API Testing Toolkit for Your Own Apps]*

Active / SIA — No feasible successor: the route goes **active** and queries neighbours. No reply within 3 min = SIA (stuck-in-active), the neighbour is reset. Limit query scope with stub routers and summarisation. *[Routing II: EIGRP, BGP at the Enterprise Edge, Redistribution]*

Actively exploited vulnerability — CRA Art. 3(42): a vulnerability for which reliable evidence shows a malicious actor has exploited it in a system without the owner's permission. *[Cyber Resilience Act and AI Act]*

AD CS — Active Directory Certificate Services: Microsoft PKI issuing certificates usable for domain logon. *[Active Directory Security; Active Directory Tier 0 Remediation +1]*

AD CS / ESC — Active Directory Certificate Services (the internal PKI); ESC1-ESC16 = published classes of certificate-template and CA misconfigurations that let a user obtain a certificate for an admin. *[Windows and Active Directory for Defenders]*

AD / DC — Active Directory: Microsoft's directory of users, computers and groups for a Windows domain; a Domain Controller (DC) holds a copy and authenticates logons. *[Windows and Active Directory for Defenders]*

AD-integrated DNS — DNS zones stored in AD and replicated with it; DCs register SRV records so clients can locate services. DHCP is a separate role, often paired but not part of AD. *[On-Prem Active Directory Architecture]*

ADCS (Active Directory Certificate Services) — The Microsoft PKI role that issues certificates to users, computers and services; a Tier 0 asset because a rogue certificate can impersonate anyone. *[On-Prem Active Directory Architecture]*

Additional requirement for service providers only — Flag on items merchants skip, e.g. documented cryptographic architecture (3.6.1.1), 90-day rotation of customer passwords used alone (8.3.10.1), segmentation pentest every 6 months (11.4.6), covert-channel detection (11.5.1.1), quarterly checks that staff follow procedures (12.4.2), scope confirmed every 6 months... *[PCI DSS v4.0.1 Requirement by Requirement]*

ADE (Automated Device Enrollment) — formerly DEP: a Mac registered in ABM contacts Apple during Setup Assistant and is told to enroll into the organization's MDM; enrollment can be made mandatory and non-removable, and the Mac becomes supervised. *[macOS Security for Defenders]*

ADE / zero-touch — Apple Automated Device Enrollment and Android zero-touch: devices bought by the company enrol themselves in the MDM at first boot. *[Mobile Device Security and MDM]*

Adequacy decision — European Commission finding that a country protects personal data essentially as well as the EU. *[CISSP Domain 1: Security and Risk Management]*

Adjacent-channel interference (ACI) — Overlapping but different channels (e.g. 1 and 3 on 2.4 GHz): seen as noise, worse than CCI. Never use 2.4 GHz channels outside 1/6/11 in the US plan. *[Wireless, Data-Center Fabrics and Cloud Networking]*

Admin isolation — dedicated admin NIC, network and directory; VM admin apart from platform admin (R13, R20, R21, R40) *[VMware vSphere and ESXi Security]*

Administration IS (SI d'administration) — Workstations, admin network, tools servers, jump hosts and logging used to administer the **administered IS** (SI administré); separated from the office IS (SI bureautique) and the Internet. *[ANSSI Secure Administration of IS (PA-022)]*

Administration partitioning — dedicated administration IS and network (PA-022; PA-108 R104 dedicated ICS admin network), admin workstations used only for administration and never on the Internet (PA-108 R105), bastion for every admin flow. *[Segmentation and IS Mapping]*

Administrative distance — Trust ranking between routing sources: connected 0, static 1, eBGP 20, EIGRP 90, OSPF 110, RIP 120, iBGP 200. *[Networking Fundamentals II - Routing, L2, IPv6, Wi-Fi, Tools]*

Administrator — Grants access per the owner's policy, often through RBAC; may also act as custodian. *[CISSP Domain 2: Asset Security]*

Administrator (PA) — control plane - tells the PEP to open or close the path *[Security Architecture - Resilience, Controls, Zero Trust]*

AdminSDHolder — Template ACL re-applied hourly (SDProp) to protected groups and their members (adminCount=1). *[Windows and Active Directory for Defenders]*

adminSDHolder / SDProp — Template object whose ACL is copied every 60 min by the SDProp process onto privileged accounts (flagged adminCount=1); a rogue entry there re-grants rights automatically. *[Active Directory Tier 0 Remediation]*

Admissibility — whether a court accepts an item as evidence at all; distinct from its weight (how much the judge believes it) *[Digital Evidence and Chain of Custody]*

Admissible evidence — Evidence that is relevant, material and competent (legally obtained). *[CISSP Domain 7: Security Operations]*

Admission control — PSA restricted + ValidatingAdmission Policy/Kyverno for registries, signatures, labels *[Kubernetes Security]*

Admission controller — API server plug-in that validates or mutates an object after authentication and authorisation, before it is stored. *[Kubernetes Security; Kubernetes Admission Control and Policy as Code]*

Admission webhook — An HTTPS endpoint the API server calls with an AdmissionReview; a MutatingWebhookConfiguration or ValidatingWebhookConfiguration registers it with match rules. *[Kubernetes Admission Control and Policy as Code]*

ADR (Architecture Decision Record) — Short dated document recording one design decision: context, options, choice and consequences. *[Designing a Secure SME Network and Cloud Landing Zone]*

Advanced audit policy — the 50+ subcategories configured by auditpol or GPO, replacing the 9 legacy audit categories; ANSSI table 4 sets each one. *[Windows and AD Logging: ANSSI PB-090]*

Adversarial attack — One or more malicious requests aimed at misleading or altering the operation of the AI system. *[ANSSI Generative AI Security]*

Adversarial machine learning (AML) — Study of attacks that exploit the statistical, data-driven nature of ML systems, and of the defences against them. *[AI Security Engineering]*

Adversarial networks — GANs generate evasive malware and adversarial inputs *[AI-Assisted Security]*

Adversary emulation — Chained replay of a specific actor's documented TTPs in order (e.g. an emulation plan for FIN6 or APT29), testing end-to-end response. *[Detection Validation and Purple Teaming]*

AEAD — Authenticated encryption (AES-GCM, AES-CCM, ChaCha20-Poly1305): encryption and integrity in one primitive. *[ANSSI TLS and IPsec Guides: Full R Index; TLS, IPsec and SSH Hardening +3]*

Affiliate — Criminal who breaks in and deploys a RaaS encryptor; the same affiliate may switch brands, so TTPs follow the affiliate, not the logo. *[Threat Actor Profiles]*

After-action report (AAR) — written evaluation of an exercise or real incident: what was expected, what happened, why, and an improvement plan with owners and dates *[Crisis Communication and Tabletop Exercises]*

Agent — An LLM in a loop that **plans, calls tools, observes results and decides the next step** with some autonomy, often with **memory** across sessions and sometimes other agents as peers. Each capability multiplies the impact of **prompt injection** (instructions hidden in content the model reads, which it may obey): the... *[Agentic AI and MCP Security; AI Security Engineering +1]*

Agent access — which tools, scopes and actions an agent may invoke, with approval gates *[Securing AI Systems]*

Agentic AI — An AI system that plans and executes multi-step tasks by calling tools (shell, browser, APIs) with limited human input. *[Security Outlook 2026]*

Agents Rule of Two — Design rule: without human approval, combine at most two of untrusted input, sensitive access and state change or egress. *[Agentic AI and MCP Security]*

Aggregation — Combining individually harmless data items into sensitive information. *[CISSP Domain 8: Software Development Security]*

AH — IPsec Authentication Header: integrity and origin authentication of the whole packet, no encryption; breaks with NAT. *[CISSP Domain 4: Communication and Network Security]*

AH (Authentication Header) — IPsec protocol 51: integrity of payload and IP header, no encryption; legacy. *[VPN and Firewall Security]*

AI Act — EU Regulation 2024/1689: risk-based obligations for AI systems, including cybersecurity of high-risk AI. *[ENISA ETL 2024, DoD Zero Trust, ATT&CK for ICS]*

AI actors — OECD term for those active in the lifecycle (designers, developers, deployers, operators, evaluators, affected parties); the RMF assigns MAP/MEASURE/MANAGE tasks to actors per stage (Appendix A). *[AI Risk Management Framework]*

AI BOM — AI bill of materials: inventory of models, datasets, adapters and libraries with versions and provenance. *[OWASP Top 10 for LLM Applications 2025]*

AI model — A neural network and its parameters (weights, biases). Inherits the **sensitivity of its training data** (regurgitation risk). *[ANSSI Generative AI Security]*

AI system — All technical components around the model: front-end, orchestrator, databases, logging, plugins, filters. *[ANSSI Generative AI Security; AI Governance Programme]*

AIA / CDP — Authority Information Access (issuer URL, OCSP URL) and CRL Distribution Point, used for chain building and revocation. *[TLS and Certificates in Practice]*

AIMS — AI management system: the ISO/IEC 42001 policies, roles, processes and controls for AI, certifiable like an ISMS *[AI Governance Programme]*

Air gap — Physical or network disconnection: no path exists from production to the copy (tape on a shelf, a vault only reachable by pull). *[Backup and Recovery Engineering]*

AIS — Automatic Identification System: VHF broadcast of ship identity, position, course and speed, received by other ships and shore. *[Cyber Security On Board Ships]*

AIS manipulation — AIS broadcasts identity, position, course and speed on VHF without authentication. Attackers create

ghost vessels, alter data or suppress transmissions; no protocol fix exists. *[Cyber Security On Board Ships]*

AiTM — Adversary-in-the-middle phishing: a proxy site relays the real login and steals the session cookie after MFA. *[Cloud and DevSecOps: Self-Assessment]*

AiTM (adversary-in-the-middle) — Phishing proxy that relays the real login page and steals the session cookie issued after MFA. *[Authentication, MFA and Passwords; Social Engineering and Phishing Simulation]*

AiTM (adversary-in-the-middle) phishing — Intuition: instead of a fake login page, the attacker runs a **reverse proxy** between the victim and the real identity provider, so the victim sees the genuine page, types the password and approves MFA, and the proxy keeps the **session cookie** issued after MFA. Replaying that cookie gives the attacker a signed-in... *[Phishing Analysis and E-mail Header Forensics]*

AIW (Acceptable Interruption Window) — ISACA term for the time a service can be down before business objectives are compromised. *[CISM Domain 4: Incident Management]*

AKI / SKI — Authority and Subject Key Identifier: certificate fields that link a certificate to the exact CA key that signed it. *[ANSSI TLS and IPsec Guides: Full R Index]*

ALE / SLE / ARO — Annualised loss expectancy = single loss expectancy (loss per event) × annualised rate of occurrence (events per year). *[EU Governance and Regulation: Self-Assessment]*

Alert — A detection rule's output that needs a human or automated decision; not yet an incident. *[SOC Operations and SOAR]*

Alert fatigue — Desensitisation caused by many low-value alerts, so real alerts are missed or closed too fast. *[SOC Operations and SOAR; Working Life in Security]*

Alert fidelity — share of alerts that are true positives; high-fidelity rules page, low-fidelity rules feed dashboards and hunts. *[SIEM and Detection Engineering]*

ALG (Application Layer Gateway) — NAT helper that rewrites addresses embedded in the payload of protocols such as FTP or SIP (Session Initiation Protocol, VoIP signalling). *[IPv4 Addressing, Subnetting, VLSM and NAT]*

Alias — Short name (ls, ps, gci, %, ?). Handy at the prompt, avoid in scripts and reports so they stay readable. *[PowerShell for Defenders]*

Align with business — objectives, strategy and risk appetite come first *[CISM Exam Strategy]*

Alignment — The authenticated domain (MAIL FROM for SPF, d= for DKIM) matches the Header From domain, exactly (strict) or by organizational domain (relaxed). *[Email Security: SPF, DKIM, DMARC]*

Allow-list — Explicit list of accepted values, hosts, types or fields; everything else is refused. The opposite, a deny-list, always misses a variant. *[Mitigation Techniques; Secure Coding Patterns by Vulnerability Class]*

Alternate data stream — Additional named \$DATA attribute of an NTFS file (file:stream), invisible in normal listings; used for Mark of the Web and for hiding data. *[Storage and Filesystems for Defenders]*

Alternate data streams — NTFS ADS hides data; list with dir /r - invisible to normal browsing. *[Post-Exploitation and Lateral Movement]*

Alternate data streams (NTFS ADS) — Hidden named streams attached to a file (file.txt:hidden.exe); list with dir /r or Get-Item -Stream *. *[Forensics by Data Type]*

Always Encrypted — SQL Server feature where the client driver encrypts chosen columns with keys the server never holds. *[Database Security]*

AMBER — organization and clients *[IR Exercises and Threat Information Sharing]*

AMBER+STRICT — your organization only *[IR Exercises and Threat Information Sharing]*

AMD PSP / ASP — AMD Platform Security Processor / AMD Secure Processor (Arm core): root of trust, fTPM, PSB (Platform Secure Boot), SEV (Secure Encrypted Virtualization) key management. Its firmware ships inside the BIOS image: update the BIOS to patch it. *[Platform Firmware, BMC, DMA and USB Attacks]*

AMF — Association des maires de France: the national association of mayors, co-author of the guide. *[Start-ups, Municipalities, Teleassistance, Open Source]*

AMF / AUSF / UDM — 5G core functions: Access and Mobility Management, Authentication Server, Unified Data Management (holds keys via ARPF, the authentication credential repository). *[Telecom and 5G Security]*

AMFI — Apple Mobile File Integrity: kernel extension and daemon that enforce code-signature and entitlement checks at launch and page-in. *[iOS Application Internals and Security]*

Amplification — Reply much larger (bandwidth) or more numerous (packets) than the request. Usually combined with

reflection. *[DDoS: Protection Options, Response, Non-Participation]*

Amplification factor — Response size divided by request size for a spoofed UDP query: with a factor of 50, 1 Gbit/s of forged requests becomes 50 Gbit/s aimed at the victim. The ANSSI guide cites about 30 for DNS and about 1290 in bandwidth (99 in packets) for NTP monlist. *[DNS, Wi-Fi & DDoS Architectures; L2/L3 Attacks: Detection and Mitigation +1]*

AMSI — Antimalware Scan Interface: lets Defender or an EDR scan script content (PowerShell, VBA, JScript) after de-obfuscation, just before execution. *[Windows Application Control and Endpoint Monitoring; Windows Endpoint Telemetry and Sysmon]*

AMSI (Antimalware Scan Interface) — Windows API through which PowerShell, VBScript, JScript, Office VBA and .NET hand script content to the installed anti-malware after de-obfuscation, just before running it. *[EDR Telemetry, Tamper and Evasion Detection]*

Analyze and report — findings per tier *[Patch, Configuration and Continuous Monitoring]*

Annex III high-risk areas — biometrics (remote identification, categorisation, emotion recognition); critical infrastructure (digital infrastructure, road traffic, water, gas, heating, electricity safety components); education; employment and worker management; access to essential private and public services (credit scoring, insurance pricing,...) *[Cyber Resilience Act and AI Act]*

Annotated tag — Object pointing to another object (usually a commit) with a tagger, date, message and optional signature; a lightweight tag is only a ref, not an object. *[Git Internals and Repository Security]*

Annual affirmation — A senior official affirms continuing compliance in SPRS every year at every level; false affirmations expose the company to the False Claims Act. *[SP 800-171 Rev. 3, CUI and CMMC 2.0]*

Anomaly detection — alerting on deviation from a learned normal baseline (who talks to whom, which function codes, value ranges); strong in cyclic, deterministic OT traffic. *[OT Detection Doctrine, Integrators and Training]*

Anomaly score — Running total of points from matched CRS rules for one transaction; compared with the inbound or outbound threshold. *[WAF and API Gateway Configuration]*

Anonymization — Irreversible removal of the link to a person; truly anonymous data falls outside GDPR. *[CISSP Domain 1: Security and Risk Management]*

ANSSI — Agence nationale de la securite des systemes d'information: French national cybersecurity agency, author of both guides. *[Business Travel and SME Cybersecurity]*

Answer that satisfies all three — eliminate options that fix only part of the requirement list *[SecurityX Practice Scenarios]*

Anti-forensics — Timestomping, log clearing (1102), wiping, encryption, steganography, living in memory. Memory and network evidence often survive disk anti-forensics. *[NIST IR, Forensics, and Exercises]*

Anti-replay — The receiver drops ESP packets whose sequence number is below its sliding window or already seen; heavy QoS reordering can cause false drops. *[VPNs in Depth: IPsec/IKEv2, TLS VPN, WireGuard]*

Anticipation / reaction — The guide's two time frames: 'a froid' preparation before any detection, and actions after detection under time pressure. *[Preparing Cyber Remediation]*

Anycast — The same IP prefix announced by BGP from many locations: each source reaches the nearest site, so a global attack is split across all sites. *[DDoS and Edge Protection]*

API gateway — Single entry point that authenticates callers, enforces quotas and rate limits, validates schemas and routes to the right service. See WAF and API Gateway Configuration. *[Web Application and Microservices Architecture]*

API keys — Exposed in JS bundles, mobile binaries, comments, Postman collections. Regex by known key format. *[Enumeration and Scripting]*

APIPA — Automatic Private IP Addressing: a Windows host that got no DHCP answer self-assigns 169.254.x.x. *[IP Addressing, ICMP, DHCP and Network Triage]*

APK / IPA — Android package / iOS app archive: the installable app file that testers decompile. *[OWASP Mobile - Top 10 2024, MASVS v2.1, MASTG]*

AppArmor — Path-based MAC, default on Ubuntu, Debian and SUSE: a profile per program lists the file paths, capabilities and network access it may use. *[Linux Hardening in Practice]*

Append-only mode — Repository access that can add data but not delete or rewrite it; deletions requested by a compromised client are only logged. *[Backup and Recovery Engineering]*

AppIDSvc — Application Identity service that evaluates AppLocker rules; stopped service = no enforcement. *[Windows Application Control and Endpoint Monitoring]*

Applicability (1.4) — With an existing system: model against the deployed architecture and select compensating controls; without one: model requirements and choose the architecture that removes threat classes (e.g. no passwords → no credential stuffing). **[Compliance, Threat Modeling and AI Security]**

Applicant reference — A person who vouches for the applicant (does not act on their behalf). **[Digital Identity Guidelines SP 800-63-4]**

Applicant reference (3.15.3) — Person who vouches for attributes, identity or a condition of the applicant; SHALL be proofed to the same or higher IAL; use recorded in the subscriber account. **[Proofing Evidence and FAL Requirements]**

Application control — Control embedded in one application's processing: input edits, processing checks, output reconciliation. **[CISA Domain 1: Information System Auditing Process]**

Applications and Workloads — access, threat protection, accessibility, secure dev, security testing **[CISA Zero Trust Maturity Model v2.0]**

Apply unified analytics — across Data, Applications, Assets, Services (DAAS); log each transaction **[DoD Zero Trust Reference Architecture v1.0]**

AppProject — Argo CD object that fences Applications: allowed source repositories, destination clusters and namespaces, permitted resource kinds, signature keys and project roles. **[GitOps and Continuous Delivery Security]**

APT — Advanced Persistent Threat: well-resourced actor (usually state-backed) that keeps long-term access to spy or pre-position, rather than smash-and-grab. **[Threat Actor Profiles]**

APT (advanced persistent threat) — Well-resourced, usually state-sponsored group that gains access and stays hidden for months to steal data or pre-position for sabotage. **[Threat Actors and Threat Vectors]**

AQL — Ariel Query Language - IBM QRadar's SQL-like search language (SELECT sourceip FROM events WHERE ...). Peers: SPL (Splunk), KQL (Sentinel/Defender), EQL/ES|QL (Elastic). **[CompTIA SecurityX CAS-005 - Exam Overview]**

AQSSI — Autorite qualifiée pour la SSI: the head of the establishment, legally responsible for IS security. **[PPST Research Protection and Buying Qualified Security]**

ARC — Authenticated Received Chain (RFC 8617): intermediaries sign the authentication results they saw, so forwarding

does not destroy the evidence. **[Email Security: SPF, DKIM, DMARC]**

ARC (Authenticated Received Chain) — RFC 8617: each intermediary (mailing list, forwarder) adds a sealed set of headers recording the SPF/DKIM/DMARC results it saw before modifying the message; cv=pass means the chain of seals is intact, and a receiver that trusts the sealers may accept a message whose DMARC then fails. **[Phishing Analysis and E-mail Header Forensics]**

Argument vector — List of program arguments passed straight to the operating system (execve) without a shell, so ;, | and \$() stay literal characters. **[Secure Coding Patterns by Vulnerability Class]**

Arm CCA (Confidential Compute Architecture) — Armv9-A RME (Realm Management Extension) adds a Realm world beside Normal and Secure; the RMM (Realm Management Monitor) manages realms; the GPT (Granule Protection Table) assigns every page to a world; silicon deployment still early (verify) **[Confidential Computing and Remote Attestation]**

ARP / NDP — Address Resolution Protocol maps an IPv4 address to a MAC address on the LAN; IPv6 uses the Neighbor Discovery Protocol (ICMPv6 133-137) instead. Neither authenticates answers. **[IP Addressing, ICMP, DHCP and Network Triage]**

ART — Android Runtime: compiles DEX bytecode ahead of time or just in time and runs each app in its own process. **[Android Application Internals and Security]**

Art. 27 testers — highest suitability and reputability, technical and organisational capabilities, certified or adhering to formal codes of conduct, professional indemnity insurance **[DORA: Digital Operational Resilience]**

Artifact — Velociraptor YAML file wrapping VQL queries with a name, description, parameters and output columns; about 500 built-in, plus the community Artifact Exchange (estimate). **[osquery and Velociraptor for Fleet Visibility]**

Artifact analysis functions (6.3) — Media or surface analysis, reverse engineering, run-time (dynamic) analysis, comparative analysis. **[SOC 2 Trust Services Criteria, COBIT 2019, CSIRT Services]**

Artifact (PO.3.3) — Evidence a tool produces that a practice is performed: scan reports, SBOMs, signed provenance, review records. The attestation (M-22-18) rests on these. **[SSDF v1.1: the 42 Tasks]**

AS and RS — OAuth authorization server issues tokens; the resource server (API) validates them and enforces scopes. **[Identity Protocols: OAuth, OIDC, SAML, FIDO2]**

AS_PATH — fewest AS numbers in the path; prepending (repeating your own ASN) lengthens it to push inbound traffic away **[Routing II: EIGRP, BGP at the Enterprise Edge, Redistribution]**

AS-REP roasting — Same offline cracking against accounts without Kerberos pre-authentication. **[ANSSI Active Directory Recommendation Catalogue]**

ASG — application security group: label NICs by role and use the label as source/destination in NSG rules; no IP maintenance when VMs scale. **[Azure and Entra ID Security Essentials]**

ASLR (Address Space Layout Randomization) — Loading images, stack and heap at random addresses so exploit code cannot hard-code them; needs position-independent code (PIE on Linux, DYNAMIC_BASE on Windows). **[Executable Formats: ELF and PE]**

ASPA — Autonomous System Provider Authorisation: RPKI object listing a customer AS's providers so path checks can catch leaks and some forged paths (IETF draft, early implementations). **[BGP, 802.1X & VPN]**

ASR rules — Microsoft Defender Attack Surface Reduction rules blocking risky behaviours such as Office spawning child processes or credential theft from LSASS. **[ANSSI Endpoint Security: Overview and Windows]**

Assertion — Signed statement from an IdP to an RP carrying the authentication result and attributes (OIDC ID token, SAML assertion). **[Digital Identity Guidelines SP 800-63-4]**

Assertion (SAML) — Signed XML statement by an IdP about a subject: authentication event, attributes, audience and validity. **[Multi-Cloud Identity Federation]**

Assessment objects — Specifications, mechanisms, activities, individuals. Depth and coverage (basic, focused, comprehensive) rise with the impact level. **[SP 800-53 Rev. 5 Security and Privacy Controls]**

Assessment objects (2.4.1) — Specifications (documents: policies, plans, designs), **mechanisms** (hardware, software, firmware, plus physical devices such as locks and cameras), **activities** (actions by people: backups, monitoring, exercising a plan), **individuals**. **[SP 800-53A and 800-53B in Practice]**

Asset — Anything of value to the organization: data, systems, people, reputation. **[CEH v13: Core Concepts, Phases and Legal Framework]**

Asset (A.x) — what the risk damages, e.g. A1 company reputation, A7 personal data (critical). *[ENISA Cloud Computing Risk Register (2009)]*

Asset / resource — people, process, infrastructure, information, applications affected *[CRISC Domain 2: IT Risk Assessment]*

Asset tag — Physical label (barcode, RFID) linking a device to its inventory record and owner. *[CISSP Domain 2: Asset Security]*

Asset valuation — Estimating an asset's worth to the business (replacement cost, revenue dependency, legal exposure) so that impact can be sized. *[CRISC Domain 1: Governance]*

Associated data (AAD) — Bytes that are authenticated but not encrypted, such as a record id or tenant id, binding a ciphertext to its context so it cannot be pasted into another row. *[Cryptography in Code]*

Assume a hostile environment — users, devices and networks inside and outside are untrusted *[DoD Zero Trust Reference Architecture v1.0]*

Assume one device stays compromised — The window of opportunity can be reduced, never closed (business exchanges, reused passwords, one exposed flaw in any large perimeter). Rather than hunting the initial entry point: fix known flaws, reinstall compromised equipment, disable compromised accounts, and define a **reintegration procedure** (update, add to... *[Managing Cyber Remediation]*

Assumed breach — Scenario that starts from given low-privilege domain credentials, as after a phishing compromise. *[OSCP / OSCP+: Exam Format and Rules]*

ASTAD / COMCYBER-MI — Atteintes aux systemes de traitement automatise de donnees (the French offence of hacking) / the Interior Ministry cyber command that counts these cases. *[Start-ups, Municipalities, Telassistance, Open Source]*

ASV (Approved Scanning Vendor) — Company certified to run the quarterly external vulnerability scans (Req. 11.3.2). *[PCI DSS v4.0.1, CVSS and FIRST]*

ASVS — Application Security Verification Standard: OWASP list of testable security requirements for web apps and APIs. *[OWASP ASVS 5.0 - Application Security Verification Standard]*

AT (Attack Requirements) — New in 4.0: conditions beyond the attacker's control (a race window, a specific config) that must hold. *[Report Templates and Severity Rating]*

ATA security freeze — State set by many BIOSes at boot that blocks ATA Secure Erase until a suspend/resume or OEM tool

unfreezes the drive. *[Multi-Environment Workstation and Refurbishing]*

ATO — Authority to Operate: formal approval to run a system after risk review; continuous ATO keeps it valid through ongoing monitoring. *[DoD Zero Trust and NSA Hardening Guidance]*

ATO (Authorization to Operate) — Formal decision by the Authorizing Official that residual risk is acceptable; valid while continuous monitoring shows no drift. *[NIST SP 800-53r5 Controls in Practice]*

Atomic indicator — Cannot be broken down further: IP address, email address, vulnerability id. *[Pentest Methodologies]*

Atomic test — Small, scripted, benign procedure that reproduces one ATT&CK technique (e.g. creating a scheduled task) so its telemetry and detection can be checked; cleanup included. *[Detection Validation and Purple Teaming]*

ATS — App Transport Security: iOS setting that forces HTTPS with modern TLS for app network calls. *[OWASP Mobile - Top 10 2024, MASVS v2.1, MASTG]*

ATS (Applicant Tracking System) — software that stores applications and lets recruiters filter and rank CVs by keywords, titles and dates; exotic layouts and text in images are often parsed badly *[CV, Portfolio and Job Interviews in Security]*

ATT&CK — MITRE catalogue of attacker tactics and techniques with ids such as T1003 (OS Credential Dumping); Navigator = web tool to colour technique matrices. *[Threat Hunting Playbooks]*

ATT&CK group ID — MITRE catalogue id for a tracked group, G + 4 digits (APT28 = G0007); its page lists the techniques (Txxxx) the group was seen using. *[Threat Actor Profiles]*

Attachments and links — Hash and detonate; macro-enabled Office, ISO/IMG disk images (bypassed Mark-of-the-Web until patched in 2022), LNK shortcuts, HTML smuggling (JavaScript assembles the payload inside the browser), password-protected ZIP (password in the body defeats gateway scanning). Hover to compare anchor text vs href. *[Security Tools and Techniques]*

Attack Complexity — L low, H high *[Vulnerability Management and Security Testing]*

Attack graph — network of states and exploits generated from real configurations and vulnerabilities, showing multi-step paths (BloodHound for Active Directory is one). *[Threat Modeling Methods]*

Attack Requirements (4.0) — N none, P present *[Vulnerability Management and Security Testing]*

Attack surface — The sum of all exposed entry points of a system or organization. *[CEH v13: Core Concepts, Phases and Legal Framework; Vulnerabilities +2]*

Attack surface / friction surface — external interfaces a use exposes (R7) / actions a domain can perform on the global system (R9). *[System Partitioning: ANSSI PG-040]*

Attack tree — root = attacker goal, children = ways to reach it; OR nodes need one child, AND nodes need all; leaves annotated with cost, skill or likelihood to find the cheapest path. *[Threat Modeling Methods]*

Attack vector — The path or channel an attacker uses to reach the target. *[CEH v13: Core Concepts, Phases and Legal Framework; Vulnerability Management and Security Testing]*

Attacker access — network, local code, admin, minutes of physical access, lab *[Hardware Security: Self-Assessment]*

Attacker capabilities — training data control, model control, testing data control, label limit, source code control, query access (black box), resource control (indirect injection via web pages, documents, emails). *[AI Security Engineering]*

Attacker objectives (PredAI) — **availability breakdown, integrity violation, privacy compromise**; GenAI adds **misuse enablement** (using the model to harm others). *[AI Security Engineering]*

Attacker of the function — assumed to control one or more domains; wins when an action forbidden by the policy succeeds. Reading a secret the policy already exposes is a policy flaw, not a partitioning break. *[System Partitioning: ANSSI PG-040]*

Attestation — Auditor's formal opinion that management's assertions about controls are fairly stated. *[CISSP Domain 6: Security Assessment and Testing; Software Supply Chain Security +3]*

Attestation and acknowledgement — Attestation: a formal statement that controls exist and work (management letter, SOC report, PCI AOC). Acknowledgement: users and staff sign that they read and accept policy (AUP, training completion). *[Compliance, Audits and Security Awareness]*

Attestation key — Restricted TPM signing key used only to sign quotes of PCR values. *[Hardware Roots of Trust and the TPM 2.0]*

Attestation report / quote — structure signed by a key rooted in the CPU vendor that carries measurements, TCB version,

policy flags and 64 bytes of caller-chosen data (nonce, public key hash) *[Confidential Computing and Remote Attestation]*

Attestations (2.4) — Device attestation (TPM-signed boot and health measurements), access attestation (periodic certification by owners), authenticator attestation (FIDO metadata proves which security-key model created the credential). *[Security Architecture - SDLC, IAM Design, Cloud]*

Attribute sampling — Estimates the rate of deviation from a control (occurs or not); used in compliance testing. *[CISA Domain 1: Information System Auditing Process]*

Attribution — Assessing which actor is behind activity; stated with a confidence level, rarely needed for defence decisions. *[Cyber Threat Intelligence Lifecycle]*

ATX 3.0 / 3.1 — Intel PSU spec (2022/2023): tolerates short power excursions up to 2x rated load from modern GPUs and adds the 16-pin connector. ATX 3.1 adopts **12V-2x6** (shorter sense pins) after 12VHPWR melting cases (2022): fully seat the plug, no sharp bend near it. *[Power, Displays, Peripherals and Printers]*

Audience (aud) and subject (sub) — aud says which RP the token is for, sub which identity it represents; the two claims every trust policy must pin, plus iss. *[Multi-Cloud Identity Federation]*

Audit (175B 5.4.9) — Three kinds: compliance audit of policy adherence, audit of the protective mechanisms (algorithms, key lengths still adequate), audit of human actions in the key-management system. *[Crypto Mechanisms, Key Policy and AES Internals]*

Audit charter — Document approved by the board or audit committee that defines the audit function's purpose, authority, responsibility and reporting line (ITAF 1001). *[CISA Domain 1: Information System Auditing Process]*

Audit log — Records who, what, when, where and the outcome; forwarded to a write-once store or a SIEM (security information and event management platform) so the actor cannot erase it. Windows event 1102 'audit log cleared' is itself an indicator of tampering. *[Fundamental Security Concepts]*

Audit trail — Chronological record that lets a reviewer reconstruct who did what and when. *[CISA Domain 3: IS Acquisition, Development and Implementation; CISSP Domain 6: Security Assessment and Testing]*

Audit universe — Inventory of all auditable entities (processes, systems, sites, vendors) from which the plan is built. *[CISA Domain 1: Information System Auditing Process]*

Auditable policy — the policy in force can be read and audited at any time (R20.3) *[System Partitioning: ANSSI PG-040]*

auditd — user-space daemon of the Linux Audit framework: the kernel matches system calls and file accesses against rules and auditd writes the records to /var/log/audit/audit.log. *[Linux and Cloud Logging]*

auS libraries — reuse functions, classes, modules *[Enumeration and Scripting]*

Aut(IT) — source check against an allow-list of legitimate data sources (source IP, optionally authentication). *[ANSSI ICS Detailed Measures v2 (2/2): technical measures]*

Aut(IT) / Aut(OT) — allow-list of legitimate sources (IP + optional authentication) / allow-list of destination tuples checked by DPI: e.g. Modbus function 6 write single register + register address; OPC UA write (ids 673, 676); IEC 60870-5-104 type P_ME_NA_1 (id 110). *[ANSSI ICS/SCADA Security]*

Aut(OT) — destination check against allow-listed tuples by deep packet inspection, e.g. Modbus function 6 write single register at one register address, OPC UA write, IEC 104 type P_ME_NA_1 (id 110). *[ANSSI ICS Detailed Measures v2 (2/2): technical measures]*

Authenticated variable — PK (platform key, owner of the platform), KEK (key exchange keys, may update db/dbx), db (signature database: allowed certs and hashes), dbx (forbidden database: revoked) are time-based authenticated variables (EFI_VARIABLE_AUTHENTICATION_2): an update must be signed by the key one level up (db/dbx by a KEK, KEK by... *[UEFI, Secure Boot and Bootkits]*

Authentication — Proving the claimed identity with one or more factors (password, token, fingerprint). *[Fundamental Security Concepts]*

Authentication (AAL) — you control the authenticator, 63B *[Digital Identity Guidelines SP 800-63-4]*

Authentication factor — Proof of identity from one category: knowledge (password, PIN), possession (smart card, FIDO key, phone app) or inherence (biometrics). *[ANSSI Identity: MFA, AD Tiering, OpenID Connect]*

Authentication intent — A deliberate user action (touch, button) proving a human is present; blocks silent malware use of a connected authenticator. *[Digital Identity Guidelines SP 800-63-4]*

Authentication package / SSP — DLL loaded by LSASS for a protocol (Security Support Provider): msv1_0 (NTLM, local SAM), kerberos, wdigest, tspkg (CredSSP for RDP), cloudap

(Microsoft Entra ID, Primary Refresh Token), schannel (TLS). *[Windows Internals for Defenders]*

Authentication-Results — Header (RFC 8601) in which the receiving server records its SPF, DKIM, DMARC, ARC and composite verdicts; only the one added by your own boundary server is meaningful. *[Phishing Analysis and E-mail Header Forensics]*

Authentication vs authorization — Authentication: is this really Scott's process? Authorization: may Scott delete cookbook.old? The first is the hard part; the second is a table lookup. *[Network Security II - Authentication, Email, Web]*

Authenticator — Something the claimant possesses and controls (password, OTP device, security key, smart card) used to prove control of the account. *[Passkeys and Passwordless Authentication; Digital Identity Guidelines SP 800-63-4]*

Authenticator (client in PA-043) — Switch or access point that keeps the port closed until the server accepts the supplicant; PA-043 calls it the RADIUS *client*. *[BGP, 802.1X & VPN]*

Authenticity — Assurance that data or a subject is genuine and from the claimed source. *[CISSP Domain 1: Security and Risk Management]*

Authenticode — Microsoft code-signing format; a valid signature proves who published a file and that it was not modified, not that it is harmless. *[Sysinternals Suite for Windows Administrators]*

Authentication forte / Strong authentication — At least two distinct factors (knowledge, possession, inherence). Required by ANSSI for administration and remote access. *[ANSSI CyberDico FR/EN Glossary]*

Authn/authz enforced — dynamic, before access, re-checked during session *[Zero Trust Architecture SP 800-207]*

Authorisation — Written permission from the person who legally controls the system (owner or delegated manager) to perform named actions on named assets during a named period. *[Law and Ethics for Security Practitioners]*

Authoritative server — Answers for its own zones without recursion. The primary holds the editable zone; secondaries get a copy by zone transfer (AXFR full, IXFR incremental). *[DNS, Wi-Fi & DDoS Architectures]*

Authorization — Deciding what the authenticated identity may access, according to an access control model and least privilege. *[Fundamental Security Concepts]*

Authorization (accreditation) — Management decision to accept the residual risk and operate the system, after certification

(technical evaluation). *[CISSP Domain 3: Security Architecture and Engineering]*

Authorization (ATO) — Authority To Operate: a government risk acceptance to use a cloud service (FedRAMP) *[Compliance Frameworks Crosswalk]*

Authorization decision (R-4) — **ATO** authorization to operate; **ATU** authorization to use (leveraging another AO's package, e.g. a FedRAMP CSP); **common control authorization**; **denial of authorization**. Type authorization and facility authorization are ATO variants. *[Risk Management Framework (RMF)]*

Authorization federation — middleware that takes consumer AC requirements and handles local and remote attributes/roles, shifting policy management from the SaaS provider to the consumer and lowering required trust in the provider. *[Cloud Reference Architecture and Access Control]*

Authorization letter — Signed 'permission to test' - the get-out-of-jail letter, carried on-site. *[Engagement Management; Engagement Methodology and Reporting]*

Authorization package (R-1) — Executive summary, System Security Plan (plus privacy plan), Security and Privacy Assessment Reports (SAR/PAR), Plan of Action and Milestones (POA&M). Increasingly delivered in OSCAL for automation. *[Risk Management Framework (RMF)]*

Authorization termination date — Set by the AO (commonly 3 years); may be removed when the system is under ongoing authorization with an effective ISCM program. *[Risk Management Framework (RMF)]*

Auto-escaping (html/template) — html/template escapes each value for where it lands (HTML body, attribute, JavaScript, URL), preventing XSS; text/template does none of this. *[Go for Security Tooling and Safe Code]*

Automated attack generation — vector discovery, payloads, malware, honeypot lures, DDoS (distributed denial of service) *[AI-Assisted Security]*

Automation — A script or tool performs one task without a human (create an account, add a firewall rule). *[Incident Response, Forensics, Automation; Compliance, Audits and Security Awareness]*

Automation bias — Human tendency to accept a machine's output without enough scrutiny, strongest when the output is fluent and the analyst is tired. *[AI Assistants for Defenders]*

Autonomous System — Network under one routing policy, identified by an ASN (16- or 32-bit number) assigned by a Regional Internet Registry. *[BGP and Internet Routing in Practice]*

Autonomous System (AS) — A network under one routing policy with its own AS number; IGP (interior gateway protocols: OSPF, EIGRP, IS-IS) route inside it, BGP between them. *[Networking Fundamentals II - Routing, L2, IPv6, Wi-Fi, Tools; Routing I: Routing Table, Static Routes, OSPF]*

AVA_VAN.3 / .5 — Common Criteria vulnerability analysis levels: resistance to attackers with enhanced-basic (3) or high (5) attack potential. *[Physical Access Control and CCTV (ANSSI PA-72)]*

Availability — Authorized users get timely, reliable access; countered by destruction or denial. *[CISSP Domain 1: Security and Risk Management]*

AVB — Android Verified Boot: each boot stage checks the next and a rollback index blocks downgrade to vulnerable versions. *[Mobile Device Security and MDM]*

AVC denial — Access Vector Cache message logged when SELinux blocks an action (type=AVC in the audit log); the primary evidence both of misconfiguration and of an attack being contained. *[Linux Hardening in Practice]*

Awareness — The moment the organisation has reasonable certainty that an incident occurred (not the first log line of the intrusion); every legal deadline counts from it, so record it in the crisis log. *[Cyber Incident Reporting Obligations]*

B

B2BUA — Back-to-back user agent: the SBC ends each call leg and opens a new one, so no direct flow crosses between inside and outside. *[ToIP and Virtualization Security]*

Backpressure — Signal from a slow downstream that makes upstream components slow down, buffer or drop; the point where silent data loss happens. *[Observability and Security Telemetry Pipelines]*

Backtracking — Engine strategy that, when a match attempt fails, returns to an earlier choice point and tries the next alternative; flexible but can explode in time. *[Defender Scripting Toolkit]*

Backup agent — software on each protected server that reads data and sends it to the backup server; runs with high privileges. *[IT Backup - ANSSI BP-100 R1-R32]*

Backup catalogue — index telling what was backed up, when and on which medium; without it, media cannot be restored quickly. *[IT Backup - ANSSI BP-100 R1-R32]*

Backup chain — A full backup plus the incrementals or differential that depend on it; losing one link makes every later point in that chain unrestorable. *[Backup and Recovery Engineering]*

Backup-less architecture — Protection by storage snapshots only, without backup software: fine against a disk failure, useless against ransomware that encrypts every server (guide warning). *[Ransomware: Anatomy, Detection, Prevention]*

Badge cloning — Copy 125 kHz HID cards with Proxmark3; 13.56 MHz with crypto is harder. *[Vulnerability Discovery and Analysis]*

Balanced scorecard — Measures IT through four perspectives: financial/business contribution, customer, internal process, learning and growth. *[CISA Domain 2: Governance and Management of IT]*

Bandwidth vs throughput vs goodput — Bandwidth = nominal link rate; throughput = what is actually carried; goodput = useful application data after headers and retransmissions. *[Network Models, Performance and the Physical Layer]*

Banner grabbing — Reading the greeting a service sends on connect (product, version, OS). Active when you connect yourself, passive when read from Shodan/Censys. *[Reconnaissance and OSINT]*

Bare-metal recovery (BMR) — full restoration of a physical server, operating system included, onto empty hardware. *[IT Backup - ANSSI BP-100 R1-R32]*

Barrier (barrière) — A security objective answering one stage of a risk scenario; made of a set of measures. *[Defence in Depth & Secure Internet Gateway]*

BAS — Breach and Attack Simulation: commercial platform that runs safe attack scenarios continuously from agents and reports which were blocked, detected or missed. *[Detection Validation and Purple Teaming]*

Base / complementary indicator — built from key points and parameters / synthesis created for a recipient level *[SSI Maturity and Security Dashboards]*

Base control — Outcome statement with lettered parts (a., b., ...). Written without the word "organization" as subject so it works for any implementer. *[SP 800-53 Rev. 5 Security and Privacy Controls]*

Base platform (socle) — Hardware and software running the domains; contains the TCB (Trusted Computing Base) plus

components whose compromise must not sink the whole system. Only strictly necessary tasks run in the base; everything else lives in a domain. *[Multi-Environment Workstation and Refurbishing]*

Baseline — Snapshot of existing findings; later scans report only what is new relative to it, so old debt does not block every pull request. *[Static Analysis and Code Scanning in Practice]*

Baseline configuration — (SP 800-53 control CM-2) Documented, approved set of specifications for a system or component at a point in time; changed only through change control. *[Patch, Configuration and Continuous Monitoring]*

Basic server security steps (sec. 2.3) — Plan deployment, install and configure the OS securely, install and configure server software securely, apply additional controls, test, maintain (patch, log, backup, test). *[Security Operations: Logs, Malware, Servers, Media]*

Battle rhythm — Fixed cadence of situation updates and decision meetings between crisis units (e.g. every 2-4 h at first, then daily). *[Cyber Crisis Management & Communication]*

BC/DR — Business Continuity / Disaster Recovery: keep critical functions running, then restore IT after a major outage. *[CompTIA CySA+ CS0-003]*

BCP (Best Current Practice) — An IETF document series for operational rules. BCP 38 (RFC 2827) = ingress filtering against spoofed sources; BCP 84 (RFC 3704) = the same for multihomed networks. *[IPv4 Addressing, Subnetting, VLSM and NAT]*

BCP (business continuity plan) — Keeps critical business functions running during and after a disruption; owned by the business. *[CISSP Domain 7: Security Operations]*

BCP (PCA) — Business Continuity Plan (plan de continuité d'activité): procedures to keep critical activities running at a pre-defined level during a disruption; in a cyber crisis it must work with no IT at all. *[Cyber Crisis Management & Communication]*

BCRs — Binding corporate rules: regulator-approved internal rules allowing transfers inside a multinational group. *[CISSP Domain 1: Security and Risk Management]*

Beaconing — Periodic check-in of implanted malware to its command-and-control (C2) server to fetch instructions; mapped to T1071 Application Layer Protocol. *[Indicators of Malicious Activity; SANS Incident Handler Checklists and Enterprise IR]*

Bearer assertion — Whoever holds it can use it (SAML POST, OIDC ID token). Mitigate: short life, audience, TLS, nonce. *[Digital Identity Guidelines SP 800-63-4]*

BEC — Business e-mail compromise: fraud using a hijacked or spoofed business mailbox to redirect payments or data, usually without malware. *[Social Engineering and Deepfakes; Email Security: SPF, DKIM, DMARC]*

BeEF — Browser Exploitation Framework: hook browsers via XSS, run JS, steal cookies. *[Cloud, Wireless, Social Eng and Specialized Attacks]*

Behavior baselines and analytics (UEBA) — Network (bytes per host per hour), systems (process trees, new services), users (logon hours, geography, volume), applications/services (API call rates) - deviation scores feed prioritization. *[Security Operations]*

Behavioral indicator — Collections of atomic and computed indicators with qualifiers, describing a TTP (tactic, technique, procedure). *[Pentest Methodologies]*

Bell-LaPadula — Confidentiality model: no read up (simple security), no write down (star property). *[CISSP Domain 5: Identity and Access Management]*

Benign true positive — The rule fired correctly on real activity that is authorised (admin tool, pentest); closes without incident but may justify a tuning exception. *[SOC Operations and SOAR]*

Benign true positive (BTP) — the rule fired correctly on activity that was authorised (admin, scanner, red team). Tune with an exclusion, not by deleting the rule. *[SIEM and Detection Engineering]*

Best available information — past, present, future, with limitations stated *[CRISC Domain 1: Governance]*

Best evidence rule — Original documents are preferred over copies; forensic images with verified hashes are accepted. *[CISSP Domain 7: Security Operations]*

BFLA — Broken Function Level Authorization: a lower-privileged caller can invoke an admin or privileged operation. *[OWASP API Security Top 10 - 2023]*

BFU / AFU — Before First Unlock / After First Unlock: after a reboot an iPhone holds most data keys locked until the passcode is entered; AFU devices expose far more data. *[macOS and iOS Forensics for Defenders]*

BGP — Border Gateway Protocol: the routing protocol between autonomous systems (AS, networks under one routing policy

with a public AS number); it trusts what neighbours announce by default. *[BGP, 802.1X & VPN]*

BGP roles and OTC (RFC 9234) — Peers declare provider, customer, peer or route-server roles; the Only-To-Customer attribute stops routes learned from a peer or provider being re-announced upward. *[BGP, 802.1X & VPN]*

BIA — Business impact analysis: identifies critical functions, dependencies and the cost of their outage over time. *[CISSP Domain 1: Security and Risk Management]*

BIA (business impact analysis) — Identifies critical processes, their dependencies and MTD/RTO/RPO; the first analytical step of BCP. *[CISM Domain 4: Incident Management; CISSP Domain 7: Security Operations +1]*

BIA first — priorities and time objectives come from business impact *[Business Continuity and ISO 22301]*

Biba — Integrity model: no read down (simple integrity), no write up (star integrity). *[CISSP Domain 5: Identity and Access Management]*

BIMI / VMC — Brand Indicators for Message Identification (logo next to authenticated mail) / Verified Mark Certificate proving the logo is a registered trademark. *[Email Security: SPF, DKIM, DMARC]*

Binder — Android's kernel inter-process communication driver; every intent, service call and content-provider query travels through it, and the receiver learns the caller's UID. *[Android Application Internals and Security]*

BISO (Business Information Security Officer) — security lead embedded in a business unit, dotted line to the CISO; translates the central policy into the unit's priorities *[Building a Security Program]*

Bit-stream image — Sector-by-sector copy including unallocated space and slack. Formats: raw dd, EWF E01 (compressed, hashed segments), AFF4. *[Digital Forensics in Incident Response]*

Black-box test — Tester has only the URL and maybe accounts; no source or design documents. *[OWASP Web Security Testing Guide v4.2]*

Black hat — Attacker acting without authorization for gain or harm. *[CEH v13: Exam Blueprint and Module Map]*

Blackholing / RTBH — Asking the upstream operator to drop all traffic to an attacked address (remotely triggered black hole, BGP community 65535:666): saves the link and neighbours, sacrifices the target. *[DDoS: Protection Options, Response, Non-Participation]*

Blackmail — Threat to publish stolen data or intimate images unless paid (sextortion, leak sites). *[Threat Actors and Threat Vectors]*

Blast radius — How far one failure or compromise propagates; segmentation and least privilege shrink it. *[Cloud Reference Architectures; Landmark Incidents and Lessons +1]*

Bloatware — Pre-installed unwanted software (PUP, potentially unwanted program): not malicious but widens the attack surface and consumes resources; remove it during hardening (objective 2.5, mitigation techniques). *[Malware, Attacks and Indicators]*

Blob — Object holding the raw bytes of one file version; no name, no permissions. *[Git Internals and Repository Security]*

Blockchain / open public ledger — Append-only chain of blocks where each block contains the hash of the previous one; changing an old record changes its hash and breaks every later link, so tampering is evident. An open public ledger is replicated to many participants and readable by anyone; consensus among them decides which blocks are added. Uses:... *[Cryptography]*

Blue team — The defenders (SOC, incident response, IT operations) who are not told about the exercise so their real reaction can be measured. *[Red Team Programme and Rules of Engagement]*

Bluejacking / bluesnarfing / bluebugging — Unsolicited messages / data theft / remote control over Bluetooth; keep devices non-discoverable. *[CISSP Domain 4: Communication and Network Security]*

BLUF — Bottom Line Up Front: military writing rule, put the conclusion and the ask in the first two lines, details after. *[Writing for Security Work]*

BMC — Baseboard management controller: always-on server management computer controlling power, console and firmware. *[Platform Firmware, BMC, DMA and USB Attacks]*

BMC (baseboard management controller) — Small computer soldered on every server board (Dell iDRAC, HPE iLO, Lenovo XCC, AMI MegaRAC firmware on many brands). It runs even when the server is off and controls power, console, virtual media and firmware flashing. Protocols: **IPMI** (Intelligent Platform Management Interface, 1998, UDP 623 via RMCP = Remote... *[Platform Firmware, BMC, DMA and USB Attacks]*

Bodyfile — Pipe-separated file list with MACB times (Modified, Accessed, Changed = inode change, Born) produced by Sleuth

Kit f1s and read by mactime to build a timeline. *[Linux DFIR and Live Response]*

Bogon — Source address that should never appear on the internet (unallocated or reserved ranges). *[VPN and Firewall Security; Firewall Policy and IDPS Deployment]*

Bogon / martian — A source address that must never appear on the public Internet: private, reserved, unallocated or loopback space. 'Martian' is the router term for such packets. *[IPv4 Addressing, Subnetting, VLSM and NAT]*

BOLA — Broken Object Level Authorization - API #1 risk; per-object access not enforced. *[Web Application Assessment; OWASP API Security Top 10 - 2023]*

BOOT LED — no boot device: drive, cable, boot order, ESP *[Hardware Troubleshooting Playbook]*

Bootkit — Malware that runs before the OS kernel by replacing or patching boot components. *[Hardware Security: Self-Assessment]*

Bootstrap token — secret escrowed by the Mac to MDM; lets MDM grant SecureToken (the right to unlock FileVault) to new accounts and authorize kernel extensions and updates on Apple silicon. *[macOS Security for Defenders]*

Botnet / booter — Networks of compromised machines; 'booter' or 'stresser' services rent attacks cheaply, some with free trial minutes (the secure gateway guide PA-066 cites less than about 100 euros). *[DDoS: Protection Options, Response, Non-Participation]*

Bottom-up team (3.5.2) — Built from Competencies when the Tasks are not yet known. The guide's notional red team: **Engagement Planning, Rules of Engagement, Pen Testing, Data Collection, Vulnerability Exploitation**. Members may hold no matching Work Role at all. *[NICE Workforce Framework for Cybersecurity]*

Bound authenticator — FAL3 alternative: an authenticator bound to the RP account, presented together with the assertion (RP-provided or subscriber-provided binding ceremony). *[Digital Identity Guidelines SP 800-63-4]*

Bounding set (CapBnd) — Hard ceiling for the process and descendants; can only shrink. *[Linux Isolation Primitives and Sandboxes]*

BPDU — Bridge Protocol Data Unit: Spanning Tree Protocol (STP) control frame that elects the root bridge and blocks loops. *[Access Switch Audit Grid: DAT-NT-025 R1-R71]*

Branch protection — Repository rules on the main branch: required reviews, status checks (SAST, tests) must pass, no

force-push (history rewrite), signed commits, CODEOWNERS file forcing review by named owners for security-sensitive paths. *[Security Architecture - SDLC, IAM Design, Cloud]*

Breadcrumb (lure) — planted pointer that leads an intruder to a decoy: saved RDP file, cached credential, config file, bookmark. *[Deception: Honeypots, Honeytokens, Canaries]*

Break-glass account — Emergency administrator account kept sealed, monitored and tested, used only when normal access fails. *[CISSP Domain 5: Identity and Access Management; AWS Security Essentials +1]*

Break-glass account (compte bris de glace) — Privileged account whose very complex password sits sealed in a safe, used only for exceptional incidents, then changed and sealed again (R78). Example given: DSRM passwords (Directory Services Restore Mode of Active Directory domain controllers). *[ANSSI ICS Detailed Measures v2 (1/2): organisation and accounts]*

Break-glass identity (bris de glace) — Emergency super-administrator account (AD RID 500, hypervisor root, cloud super-admin) stored offline and used only when normal admin access is lost. *[Preparing Cyber Remediation]*

Breakout time — Time from an intruder's initial access to its first lateral movement to another host (CrowdStrike metric). *[Security Outlook 2026; Breach and Threat Landscape 2024 +1]*

Brewer-Nash — Chinese Wall: access rights change dynamically to avoid conflicts of interest. *[CISSP Domain 5: Identity and Access Management]*

Brewer-Nash (Chinese Wall) — Access changes dynamically with history to prevent conflicts of interest between competing clients. *[CISSP Domain 3: Security Architecture and Engineering]*

Bridge — system that locks assets on one chain and mints a representation on another; the lock contract becomes a large honeypot *[Blockchain and Smart-Contract Security]*

Bridge anti-spoofing — In bridge (transparent) mode the SNS keeps a per-port host table and alerts when an IP address appears on another port; it learns only after the first packet, so a silent host is not protected. *[Stormshield SNS 3.7.17 Hardening by Chapter]*

Bridge ID — 8 bytes: 2-byte priority (4-bit priority + 12-bit extended system ID = VLAN) + 6-byte MAC. Lowest wins the root election. *[Switching: VLANs, Trunks, Spanning Tree, EtherChannel]*

Broad network access — available over the network through standard mechanisms (thin/thick clients, mobile) *[Cloud Computing Security]*

Broadcast domain — The set of hosts reached by a broadcast frame: one VLAN. Only a router (or L3 switch) separates broadcast domains. *[Ethernet, MAC Tables and ARP]*

Browser extension — add-on package (JavaScript, manifest) that can read and change pages, intercept requests and call browser APIs within the permissions it declares *[Browser and Extension Security]*

BSIMM — Building Security In Maturity Model: descriptive model built from observing what real firms do. *[CISSP Domain 8: Software Development Security]*

BSSID — Basic Service Set Identifier: MAC address of one access-point radio for one SSID; several BSSIDs can share one SSID. *[Wi-Fi Security Internals]*

btime — File birth (creation) time stored by ext4, XFS and Btrfs inodes and exposed by statx (stat %w); absent from classic ls output. *[Linux DFIR and Live Response]*

Buffer over-read — Code reads past the end of a buffer and returns adjacent memory (keys, session tokens): Heartbleed, Citrix Bleed. *[Famous Vulnerabilities Explained]*

Bulk encryption — AES-GCM, AES-CCM, (CBC legacy) *[NIST Cryptography, TLS and PKI]*

BUM traffic — Broadcast, unknown unicast, multicast: replicated by underlay multicast or by head-end (ingress) replication. *[Wireless, Data-Center Fabrics and Cloud Networking; Overlay, Data-Centre and Cloud Network Internals]*

Burnout — Occupational phenomenon (WHO ICD-11 code QD85, 2019) resulting from chronic workplace stress that has not been managed: exhaustion, mental distance or cynicism, reduced professional efficacy. *[Working Life in Security]*

Bus / payload — The bus keeps the satellite alive (power, thermal, attitude, propulsion); the payload delivers the mission (communications, imaging, navigation). *[Space and Satellite Security]*

Business alignment — IT serves business objectives; business owners own data and risks *[CISA Exam Strategy]*

Business associate (HIPAA) — vendor that creates, receives or processes PHI for a covered entity (cloud host, billing firm, MSSP); directly liable since 2013 *[Global Security and Privacy Regulations]*

Business case — Justification of a project by benefits, costs, risks and options; revisited at each stage gate. *[CISA Domain 3: IS Acquisition, Development and Implementation]*

Business continuity — (c) backup, DR, crisis *[NIS2 Directive: EU-wide Obligations]*

Business email compromise (BEC) — Invoice or payroll fraud from a spoofed or hijacked mailbox; no malware needed. *[Social Engineering and Phishing Simulation]*

Business first — choose the option tied to objectives and value *[CRISC Exam Strategy]*

Business impact analysis — Translating a technical finding into business terms: which process, data or revenue is affected and how badly. *[Engagement Management]*

Business value (valeur metier) — service, support function, project step, information or know-how needed for the mission; ISO 27005 'primary asset', EBIOS 2010 'bien essentiel' *[EBIOS Risk Manager]*

BYOD — Bring your own device: personal equipment used for work, low trust by default for ANSSI. *[ANSSI Zero Trust Model]*

BYOD (bring your own device) — Personally owned laptops or phones that reach enterprise data; the enterprise cannot fully configure them. *[Zero Trust Architecture SP 800-207]*

BYOVD — Bring Your Own Vulnerable Driver: loading a legitimately signed but vulnerable kernel driver to kill EDR or gain kernel access. *[Windows Application Control and Endpoint Monitoring; Windows Endpoint Telemetry and Sysmon]*

BYOVD (Bring Your Own Vulnerable Driver) — Attack where an intruder with admin rights loads a legitimately signed but vulnerable driver to run code in the kernel and disable EDR; Windows blocks known ones with the vulnerable driver blacklist. *[Operating System Concepts for Beginners]*

Bypass measure — Temporary non-application of a normal operating rule so that a business line works in degraded mode (e.g. paper orders, a stand-alone PC); recorded in the register of exemptions. *[Cyber Crisis Management & Communication]*

C

C2 — Command and Control: the channel an implant uses to receive orders from the attacker (HTTPS beacons, DNS, named pipes internally). *[Windows Endpoint Telemetry and Sysmon]*

C3PAO / DIBCAC / Cyber AB — C3PAO = accredited third-party assessor (Level 2); DIBCAC = DoD's Defense Industrial Base Cybersecurity Assessment Center (Level 3); Cyber AB = accreditation body for C3PAOs. *[SP 800-171 Rev. 3, CUI and CMMC 2.0]*

C5 — Cloud Computing Compliance Criteria Catalogue (2020): attestation criteria for cloud providers (basic and additional criteria), reported like an ISAE 3000 Type 1 (design) or Type 2 (operating effectiveness over a period) audit; required for German federal cloud use. *[NCSC, BSI and Allied Cyber Authorities]*

CAA record — DNS record (Certification Authority Authorization) naming the CAs allowed to issue for a domain; public CAs must check it before issuing. *[PKI Operations and Key Management]*

CAA record (RFC 8659) — example.com. CAA 0 issue "letsencrypt.org" restricts which CAs may issue; iodef gets violation reports. *[TLS and Certificates in Practice]*

CAA (RFC 8659) — Certification Authority Authorization: DNS record naming the CAs allowed to issue for a domain; checked before a domain enters an ACME account (BP-106 R7), published by the domain owner (R89). *[PKI and ACME Certificate Automation]*

Cache — L1 (per core, split I/D, ~32-64 KB), L2 (per core, 1-3 MB), L3 (shared, tens of MB). AMD X3D parts stack extra L3 (3D V-Cache). *[CPUs, Memory, Motherboards and Buses]*

Cache poisoning — A low-trust job writes a build cache entry that a later privileged job restores and executes (Ultralytics, Dec 2024). *[CI/CD Pipeline Security]*

CAF profile — The subset of contributing outcomes a regulator (cyber oversight body) sets as the target, some at achieved, some at partially achieved, some not applicable, often calibrated to resist attackers of basic or moderate capability. The NCSC itself is not a regulator and sets no targets. *[NCSC CAF 4.0, CCCS Readiness Goals, BSI 2024]*

CAIQ — Consensus Assessments Initiative Questionnaire: yes/no questions derived from the CCM that a provider answers to describe its controls. *[CCSP and CCSK: Cloud Security Certifications]*

CAIQ (Consensus Assessments Initiative Questionnaire) — one yes/no question per CCM control (261 in v4). Providers publish it as STAR Level 1; customers use it in vendor due diligence instead of bespoke questionnaires. *[CSA Cloud Controls Matrix and Guidance]*

Calibrated estimate — 90 % confidence interval from an expert trained to be right 90 % of the time (Hubbard); min / most likely / max feeds a PERT (smoothed triangular) or lognormal distribution *[Risk Quantification and Cyber Insurance]*

Callback phishing (TOAD) — e-mail with no link, only a phone number for a fake invoice or subscription; the call leads to remote-access tool installation. Mitigate: block unapproved remote monitoring and management (RMM) tools, train finance and support staff. *[Social Engineering and Deepfakes]*

Campaign — Time-bound activity (C0024 SolarWinds Compromise) attributed to a group, with its own technique set and first/last seen dates. *[MITRE ATT&CK]*

Canal caché / Covert channel — Concealed transfer of information through a mechanism not meant for communication. *[ANSSI CyberDico FR/EN Glossary]*

Canary and regression testing — Canary = release to a small slice of traffic with automatic rollback on error budget; regression = re-run the previous test suite so a fix does not reopen an old bug. *[Security Architecture - SDLC, IAM Design, Cloud]*

Canary token — Unique fake secret planted in a context; any appearance outside proves a leak with no false positives. *[Deception: Honeypots, Honeytokens, Canaries; LLM Application Security Testing]*

Canonicalisation — Turning a path or URL into its single absolute form (resolve . . . , symlinks, encodings) before checking it. *[OWASP Secure Coding Practices and Developer Guide; Secure Coding Patterns by Vulnerability Class]*

Capabilities — root's powers split into ~40 units (cap_net_bind_service, cap_sys_admin...) that can be given to one binary instead of full root. *[Linux Security Command Line]*

Capability — One slice of root's power (e.g. CAP_NET_ADMIN) that can be granted or dropped per process. *[Docker Container Security; Linux Isolation Primitives and Sandboxes]*

Capacity management — Monitoring utilisation and forecasting demand so performance meets SLAs without over-buying. *[CISA Domain 4: IS Operations and Business Resilience]*

CAPEC — Common Attack Pattern Enumeration and Classification (MITRE): catalog of attack patterns used to populate trees and PASTA stage 6. *[Compliance, Threat Modeling and AI Security; Threat Modeling Methods]*

CapEx / OpEx — Capital expenditure (buy hardware up front) versus operating expenditure (pay per use, as with cloud). *[Security Architecture Models]*

Capsule update — Signed firmware update package handed to UEFI with UpdateCapsule() and applied at reboot. *[UEFI, Secure Boot and Bootkits]*

Captive portal — Web login page imposed by hotel, airport or train Wi-Fi before Internet access; it forces the device to talk to an untrusted network outside the VPN. *[Business Travel and SME Cybersecurity]*

Capture group — Parenthesised part of a pattern whose matched text is kept (\1, \$1, m.group(1)) for extraction or replacement. *[Defender Scripting Toolkit]*

Cardinality — Number of distinct time series a metric produces, the product of the distinct values of each label. *[Observability and Security Telemetry Pipelines]*

Carpet bombing — Spreading attack traffic over every address of a prefix so no single destination crosses per-IP detection thresholds. *[DDoS and Edge Protection]*

CASB — Cloud Access Security Broker: visibility and policy control over SaaS use (shadow IT, data sharing, DLP). *[CompTIA CySA+ CS0-003; NIST Cloud, Virtualization, and Container Security]*

CASB (Cloud Access Security Broker) — Proxy or API service between users and cloud apps that discovers shadow IT from traffic logs and applies DLP and session controls. *[SaaS Security and Google Workspace]*

CAT — Computerized adaptive testing: each answer sets the difficulty of the next item and the exam stops once the candidate's ability is estimated with confidence. *[Security Certification Landscape]*

CAT (Computerized Adaptive Testing) — Exam that picks each next item from your ability estimate so far; stops once a pass/fail decision is statistically confident. *[CISSP Exam Strategy]*

Category — Group of related outcomes inside a Function (GV.SC = Govern / Cybersecurity Supply Chain Risk Management). *[NIST Cybersecurity Framework 2.0]*

CBOM (Cryptographic Bill of Materials) — Machine-readable inventory of cryptographic assets: algorithms, key sizes, protocols, certificates, libraries and where they are used. Standardised in **CycloneDX 1.6** (April 2024) as an extension of the SBOM. Tools: IBM sonar-cryptography (SonarQube plugin), CBOMkit, vendor discovery scanners. The CBOM is

what. . . *[Post-Quantum Migration Playbook; Quantum-Safe Network Protocols: Status]*

cBPF (classic BPF) — 1992 packet-filter virtual machine (2 registers) used by tcpdump and seccomp; the kernel translates it to eBPF internally. *[eBPF in Depth]*

CBRN information or capabilities — easier access to or synthesis of knowledge that helps design chemical, biological, radiological or nuclear weapons. *[AI Risk Management Program Design]*

CBT (Changed Block Tracking) — Hypervisor or storage feature that records which blocks changed since the last backup, so an incremental reads only those blocks. *[Backup and Recovery Engineering]*

CC / EAL — Common Criteria (ISO/IEC 15408) and its Evaluation Assurance Level, the depth of the lab analysis (EAL1 to EAL7). *[Firewall Policy: Design, Cleanup, Exposed Zone]*

CCAG-TIC — General administrative clauses for IT and communication contracts, the default contract terms the CCAP adapts. *[PPST Research Protection and Buying Qualified Security]*

CCI — Control Correlation Identifier: links each STIG rule to a NIST SP 800-53 control, so a checklist becomes evidence for the RMF (Risk Management Framework, SP 800-37) authorisation. *[DISA STIG Viewer 3 and STIG Checklists]*

CCI (Configurable Code Integrity) — Allow-list policy for drivers and applications, today Windows Defender Application Control (App Control for Business). *[Windows Privacy GPOs and VBS Deployment]*

CCM — Cloud Controls Matrix: CSA control framework for cloud; version 4 has 197 control objectives in 17 domains, each mapped to ISO/IEC 27001, NIST and other standards. *[CCSP and CCSK: Cloud Security Certifications]*

CCM (Cloud Controls Matrix) — cloud-specific control framework: each control has an id (domain letters + number, e.g. IAM-14), a one-sentence requirement, implementation and auditing guidelines, and mappings to ISO 27001/27017/27018, NIST SP 800-53 r5, PCI DSS, CIS Controls, the AICPA Trust Services Criteria behind SOC 2, and others, plus the. . . *[CSA Cloud Controls Matrix and Guidance]*

CCMP / GCMP — AES counter mode with CBC-MAC (WPA2) or Galois counter mode (WPA3-Enterprise 192-bit): encryption plus integrity. *[Wireless Security and IDS/IPS]*

CCTP / CCAP — Cahier des clauses techniques particulières (technical specification) / administratives particulières

(contract-specific administrative clauses). *[PPST Research Protection and Buying Qualified Security]*

CDE — Cardholder data environment (PCI DSS): systems that store, process or transmit card data. *[Network and Infrastructure Assessment]*

CDI / UDI — Constrained data item protected by the model / unconstrained data item such as raw input. *[CISSP Domain 3: Security Architecture and Engineering]*

CDM — Continuous Diagnostics and Mitigation: CISA programme giving agencies asset, identity and vulnerability visibility tools and dashboards. *[CISA Zero Trust Maturity Model v2.0]*

CDM (Continuous Diagnostics and Mitigation) — US DHS program and tooling that inventories assets and reports their patch and vulnerability state; generically, any continuous asset-posture system. *[Zero Trust Architecture SP 800-207]*

CDR — Call detail record: per-call billing log (caller, callee, time, duration) used to spot fraud. *[ToIP and Virtualization Security]*

CDR / statification — Content Disarm and Reconstruction: rebuilding a file (image, office document) from its allowed structures only, dropping macros and active content. *[Removable Media Airlock and White Station]*

CEER — The four remediation stages in ANSSI's vocabulary: Containment (endiguement: stop the spread), Eviction (remove the attacker's accesses in one coordinated operation), Eradication (remove every persistence and malicious artefact), Reconstruction (rebuild trusted systems). *[Incident Qualification & Remediation Decision Keys]*

CEIP — Customer Experience Improvement Program: optional usage statistics sent to Microsoft (CEIPEnable=0 turns it off). *[Windows Privacy GPOs and VBS Deployment]*

CEL variables — In an admission expression: object (the incoming object), oldObject (for updates), request (the AdmissionRequest), params (bound parameter), namespaceObject, authorizer. *[Kubernetes Admission Control and Policy as Code]*

Central gateway — ECU routing between vehicle domains; applies whitelists of allowed CAN IDs per direction, rate limits and blocks diagnostic services outside authorised sessions. *[Automotive and Embedded Security]*

CER / EER — Crossover (equal) error rate where FAR equals FRR; the lower, the more accurate the device. *[CISA Domain 5: Protection of Information Assets]*

CERT / CSIRT sharing — Indicators shared with sectoral CSIRTs, circles of trust and CERT-FR; competent authorities can offer support. *[Cyber Crisis Management & Communication]*

CERT-FR — The French government CERT, operated by ANSSI: publishes alerts and threat reports, receives incident reports and supports major victims. *[Cyber Crisis Management & Communication]*

Cert SAN — Subject Alternative Name field of a TLS certificate: lists other host names served, useful to find hidden vhosts. *[WSTG v4.2 - Complete Test Catalogue]*

CERTA / CERT-FR — The French government CERT, named CERTA until 2014 and CERT-FR since; issues alerts that trigger the 24 h patch clause. *[IT Usage Charter and Outsourcing Security]*

Certificate authority — Trusted party that binds a public key to an identity by signing a certificate. *[CISA Domain 5: Protection of Information Assets]*

Certificate Authority (CA) — Entity that issues and signs certificates, binding a public key to an identity. Root CAs anchor trust; issuing CAs do the day-to-day signing. *[PKI and Certificate Architecture]*

Certificate-based persistence — A stolen or misissued certificate keeps working until it expires or is revoked; remediation includes revocation and, for a CA key compromise, re-keying the CA. *[Identity and Active Directory Assessment]*

Certificate inventory (9.2.2) — Every certificate SHALL be inventoried upon creation; the tool monitors validity periods, flags weak algorithms, and drives response to a CA compromise. Unrecorded certificates cause outages at expiry. *[Crypto Mechanisms, Key Policy and AES Internals]*

Certificate pinning — App accepts only a known server certificate or public key, not any certificate trusted by the device. *[NIST Cryptography, TLS and PKI; OWASP Mobile - Top 10 2024, MASVS v2.1, MASTG]*

Certificate Transparency (CT) — Public append-only logs where public CAs must record every TLS certificate; browsers require SCTs (Signed Certificate Timestamps) and owners monitor logs for rogue issuance. *[PKI Operations and Key Management]*

Certificate Transparency (RFC 6962) — Public append-only logs of every issued certificate; browsers require SCTs (Signed Certificate Timestamps, proof of logging). Monitor crt.sh for

certificates issued for your domains. *[TLS and Certificates in Practice]*

Certification — accredited body declares conformity to a standard for a 3-year cycle (ISO 27001, CMMC Level 2 third-party) *[Compliance Frameworks Crosswalk]*

Certification and accreditation — Technical evaluation of a system (certification) followed by management's formal approval to operate (accreditation). *[CISSP Domain 8: Software Development Security]*

Certify / Seatbelt — AD CS template abuse (ESC1-ESC8); host situational awareness. *[Host and Web Application Attacks]*

CESTI — Centre d'évaluation de la sécurité des technologies de l'information: independent evaluation lab licensed by ANSSI. *[Firewall Policy: Design, Cleanup, Exposed Zone]*

CFAA — US Computer Fraud and Abuse Act (1986): federal law criminalising unauthorised access to computers. *[Engagement Methodology and Reporting]*

CGNAT (Carrier-Grade NAT) — NAT run by the ISP for many subscribers at once, using the shared 100.64.0.0/10 space between the customer router and the ISP (RFC 6598). Customer + ISP NAT = NAT444. *[IPv4 Addressing, Subnetting, VLSM and NAT]*

CGO_ENABLED — When 0, the build uses no C code, producing a static binary with no libc dependency; when 1 (default with a C toolchain) some packages link against libc and lose portability. *[Go for Security Tooling and Safe Code]*

cgroup — Control group: kernel mechanism that limits and accounts CPU, memory, PIDs and I/O of a process group. *[Docker Container Security]*

cgroup (control group) — Kernel hierarchy that accounts for and limits CPU, memory, I/O and process count; v2 is one unified tree under /sys/fs/cgroup. *[Linux Isolation Primitives and Sandboxes]*

Chain — leaf → one or more intermediates → root; the server must send leaf + intermediates, the client already holds the root in its trust store. *[OpenSSL and Certificate Tooling]*

Chain of custody — Documented record of who handled evidence, when and how, preserving its admissibility. *[Digital Evidence and Chain of Custody; CISA Domain 5: Protection of Information Assets +7]*

Chain of custody (chaîne de traçabilité) — Documented record of who collected the evidence, when, where, how, and who handled it since; tamper-evident bags, signed hand-over log. A

broken chain makes evidence inadmissible. *[Incident Response and Management]*

Challenge-response — One side sends a random **nonce** R; the other proves knowledge of the shared key K_AB by returning K_AB(R). Nonces give freshness, so replay fails (Fig. 8-32). *[Network Security II - Authentication, Email, Web]*

Change management — Formal process to request, assess, approve, test, implement, verify and document every modification to systems, applications or configurations, so that changes are deliberate, reversible and traceable. Security cares because unplanned or unreviewed changes open ports, weaken configurations, break controls and cause... *[CRISC Domain 4: Information Technology and Security; Change Management]*

Change vs configuration management — Change management approves and schedules modifications (CAB = change advisory board; emergency changes are approved after the fact); configuration management keeps the authoritative baseline (SP 800-53 CM-2 baseline configuration) and detects drift from it (CM-3 change control, CM-6 configuration settings). *[Governance and Risk Management]*

Chart — A versioned package: templates, default values and metadata (Chart.yaml). The unit you install and share. *[Helm, operators and the CRD ecosystem (with security)]*

ChatML — Chat Markup Language: message format that tags each turn with a role (system, user, assistant), used to separate trusted from untrusted text. *[OWASP LLM Top 10 v1.1 (2023) and the 2025 Shift]*

CHD / SAD — Cardholder Data (card number, name, expiry); Sensitive Authentication Data (CVV, PIN, track data), never stored after authorization under PCI DSS. *[CompTIA CySA+ CS0-003]*

Chiffrement / Encryption — Cryptographic transformation of data producing a cryptogram. 'Chiffrement symétrique' (one shared key) vs 'asymétrique' (public/private key pair). Never 'cryptage'. *[ANSSI CyberDico FR/EN Glossary]*

CIAT (DICT) — Confidentiality, Integrity, Availability, Traceability: the four security requirements PA-046 records for each piece of information and asset (French DICT: Disponibilité, Intégrité, Confidentialité, Tracabilité). *[Segmentation and IS Mapping]*

Cible de sécurité — Security target: the client's statement of security objectives derived from its risk analysis, which the PAS must cover. *[IT Usage Charter and Outsourcing Security]*

CIDR — Classless Inter-Domain Routing notation: /24 = the first 24 bits are the network part, 8 bits left for hosts. *[IP Addressing, ICMP, DHCP and Network Triage]*

CIDR (Classless Inter-Domain Routing) — Addressing and routing with prefixes of any length instead of fixed classes A/B/C (RFC 4632, 2006; first RFC 1519, 1993). Makes aggregation and VLSM possible. *[IPv4 Addressing, Subnetting, VLSM and NAT]*

CIDR range — Block of IP addresses written as prefix/length (10.0.0.0/24 = 256 addresses). *[Network and Infrastructure Assessment]*

CIDR (RFC 4632) — Classless prefixes replace classes A/B/C; routers use longest-prefix match (Tanenbaum Fig. 5-52). Aggregation shrinks BGP tables. *[Networking Fundamentals I - Models, IP, TCP, Ports]*

Cipher — The algorithm that encrypts and decrypts (AES, ChaCha20, RSA). *[Cryptography]*

Cipher suite — The set of algorithms for one TLS connection: key exchange, authentication, bulk encryption and hash. *[TLS, IPsec and SSH Hardening; Web Server and TLS Configuration]*

Circuit vs packet switching — Circuit switching reserves a path and bandwidth for the whole call (old telephone network); packet switching shares links packet by packet, efficient but with queueing delay (the Internet). *[Network Models, Performance and the Physical Layer]*

CIS benchmark — Center for Internet Security hardening guide per OS; its auditd section is the usual baseline (Neo23x0 = Florian Roth's public auditd rule set). *[Linux and Cloud Logging]*

CIS Benchmarks — Center for Internet Security consensus hardening guides per OS (Level 1 = safe baseline, Level 2 = defence in depth); Linux+ XK0-005 = CompTIA Linux+ exam. *[Linux Security Command Line]*

CIS Controls v8.1 — Center for Internet Security prioritised list of 18 defensive controls with three implementation groups (IG1 = essential hygiene). *[CompTIA Security+ SY0-701]*

CISA KEV — Known Exploited Vulnerabilities catalog - patch these first; weaponized in the wild. *[Vulnerability Tools, CVSS and Prioritisation; Vulnerability Discovery and Analysis]*

CISA KEV (Nov 2021) — Known Exploited Vulnerabilities catalog: CVE id, evidence of active exploitation, vendor fix or mitigation available, due date. Binding for US federal agencies through CISA Binding Operational Directive BOD 22-01

(fix within 2 weeks for new entries), replaced on 10 June 2026 by BOD 26-04 (risk tiers from 3 days to... *[Vulnerability Management and Security Testing]*

CISO (Chief Information Security Officer) — executive accountable for the security program; owns the strategy, the policy set and risk reporting, not every control *[Building a Security Program]*

Clark-Wilson — Integrity via well-formed transactions: subject-program-object triple, separation of duties, CDIs and TPs. *[CISSP Domain 3: Security Architecture and Engineering; CISSP Domain 5: Identity and Access Management]*

Class 0 network — II 901 term: a public network, or any network connected to one without qualified filtering and flow-break devices (the Internet). *[Firewall Policy: Design, Cleanup, Exposed Zone]*

Classful legacy — A 1-126 (/8), B 128-191 (/16), C 192-223 (/24), D 224-239 multicast, E 240-255 reserved; 127 loopback. Still asked in exams. *[Networking Fundamentals I - Models, IP, TCP, Ports]*

Classification vs categorization — Classification labels data by sensitivity (who may see it); categorization (FIPS 199) rates the impact on C, I and A (low, moderate, high) to choose a control baseline. *[CISSP Domain 2: Asset Security]*

Clean room — Isolated recovery environment where restored systems are scanned and rebuilt before being reconnected to production. *[Backup and Recovery Engineering]*

Clean room (isolated recovery environment) — pre-built, network-isolated environment where backups are scanned, restored and verified before reconnecting to production *[Business Continuity and ISO 22301]*

Clear — Logical techniques (overwrite, reset) that defeat simple, non-invasive recovery. Not enough for high-confidentiality data leaving control. *[NIST Security Operations Guides; Security Operations: Logs, Malware, Servers, Media]*

Clear vs Purge vs Destroy — NIST SP 800-88 sanitization levels: Clear = overwrite (defeats simple tools), Purge = firmware or crypto erase (defeats labs), Destroy = physical destruction. *[Hardware: Self-Assessment]*

Clickjacking — Your page is framed invisibly so the user clicks on it while believing they click elsewhere. *[Browser-Side Web Security Standards]*

Client impact — prefer the least disruptive option that still answers the test objective *[PenTest+ Practice Scenarios]*

Client-server vs peer-to-peer — Sybex: central server with accounts and resources vs every host shares its own; Windows workgroup = P2P, domain = client-server. **[CompTIA A+ Core 1 - Networking, SOHO, Network Troubleshooting]**

Clipping level — Threshold of repeated events (e.g. failed logons) below which activity is not reported, to reduce noise. **[CISSP Domain 7: Security Operations]**

CLM — PowerShell Constrained Language Mode: blocks .NET, COM and Win32 API calls in scripts not allowed by the WDAC policy. **[Windows Application Control and Endpoint Monitoring]**

Clock skew — Difference between a device clock and true time. A 7-minute skew on a firewall can make an outbound connection appear to precede the process that created it: measure skew per source and correct it before drawing causal conclusions. **[Forensics by Data Type]**

Cloisonnement (partitioning) — separating systems so they share no physical means (network, server, storage) and no logical means (processing, flows) beyond what is strictly needed. **[Protecting Essential IS - PA-085 R1 to R62]**

Clos fabric — Leaf-spine topology (after Charles Clos's 1953 telephone switch design): every leaf links to every spine, so any two servers are leaf-spine-leaf apart. **[Overlay, Data-Centre and Cloud Network Internals]**

Cloud access keys — AWS keys (prefix AKIA), Azure tokens, GCP service-account JSON in repos, .env, CI/CD vars. Hunt with TruffleHog / Gitleaks. **[Enumeration and Scripting]**

Cloud Auditor — independent assessment of services, operations, performance and security; **security audit, privacy impact audit, performance audit** against SLA and controls (SP 800-53). **[Cloud Reference Architecture and Access Control]**

Cloud Broker — manages use, performance and delivery; negotiates between consumers and providers. **Service intermediation** (adds identity, security, reporting), **service aggregation** (combines several services, secure data movement), **service arbitrage** (aggregation with dynamic provider choice, e.g. by score). **[Cloud Reference Architecture and Access Control]**

Cloud Carrier — intermediary providing connectivity and transport (network, telecom, access devices); provider may require dedicated, encrypted links and SLAs from the carrier to meet consumer SLAs. **[Cloud Reference Architecture and Access Control]**

Cloud Consumer — person or organisation that maintains a business relationship with, and uses services from, providers;

browses the service catalogue, signs the SLA, is billed per use. **[Cloud Reference Architecture and Access Control]**

Cloud jump kit — the tools, access and know-how prepared in advance to investigate remotely: collect platform logs and metadata, snapshot running VMs, reach disk and memory. **[CSA Security Guidance v4: the 14 Domains]**

Cloud Provider — entity responsible for making a service available; five major activities: **service deployment, service orchestration, cloud service management, security, privacy**. **[Cloud Reference Architecture and Access Control]**

Cloud / text sites — Upload to attacker S3/Blob/GCS/Mega or paste sites via legit APIs (may bypass DLP). **[Post-Exploitation and Lateral Movement]**

ClusterServiceVersion (CSV) — The operator's manifest OLM reads: it declares the CRDs owned, the install strategy and - crucially - the RBAC granted. **[Helm, operators and the CRD ecosystem (with security)]**

CM.AW-P7 breach notification — Impacted individuals and organizations are notified; maps to GDPR Art. 33-34 (72 h to the authority, without undue delay to individuals when high risk). **[NIST Privacy Framework 1.0]**

CMDB — Configuration management database: records configuration items and their relationships, the basis for change and impact analysis. **[CISSP Domain 2: Asset Security; Governance and Risk Management]**

Cmdlet — Verb-Noun command (Get-Process). Discover with `Get-Command -Verb Get -Noun *Net*` and read help with `Get-Help <cmdlet> -Examples`. **[PowerShell for Defenders]**

CMK — Customer-managed key in the cloud KMS, so the customer controls rotation, access and deletion. **[Cloud Configuration Review]**

CMMS (GMAO) — Computerised Maintenance Management System: maintenance planning server, often fed from supervision. **[OT Detection Doctrine, Integrators and Training]**

CMP / CCP — Code des marchés publics (2006) / Code de la commande publique, which replaced it on 1 April 2019. **[PPST Research Protection and Buying Qualified Security]**

CMR vs SMR — Conventional vs **Shingled** Magnetic Recording: SMR overlaps tracks for density but rewrites slowly; unsuitable for RAID/ZFS rebuilds (undisclosed SMR in NAS drives caused a 2020 controversy). **[Storage: Interfaces, SSD Internals, RAID, SMART]**

CMRS — Continuous Monitoring and Risk Scoring: DoD reporting feed of compliance results. **[DISA STIG Viewer 3 and STIG Checklists]**

CMVP / CAVP — Cryptographic Module Validation Program / Cryptographic Algorithm Validation Program: NIST and Canada's CCCS (Canadian Centre for Cyber Security) validate modules (CMVP) and algorithm implementations (CAVP, tested through the automated ACVP protocol). A product 'using FIPS algorithms' is not a validated module: check... **[HSMs, Supply Chain, Physical Security, Decommissioning]**

CN — Common Name: legacy subject field that once held the hostname; browsers now use only the SAN. **[TLS and Certificates in Practice]**

CNA — CVE Numbering Authority: vendor, CERT or researcher body allowed to assign CVE ids in its scope **[Vulnerability Management Programme]**

CNAME / PTR / MX — DNS records: alias (dangling CNAME to a deleted cloud resource = subdomain takeover), reverse lookup (mail servers need matching PTR), mail exchanger (target of SPF/DMARC questions). **[CompTIA SecurityX CAS-005 - Exam Overview]**

CNI — Container Network Interface: specification and binaries (/opt/cni/bin, config in /etc/cni/net.d) that the container runtime calls to wire a pod into the network. **[Kubernetes and Container Networking Explained]**

CNIL — Commission nationale de l'informatique et des libertés: French data protection authority, to be notified of personal data breaches within 72 h. **[Business Travel and SME Cybersecurity; Internet Voting for Non-Political Elections]**

Co-channel interference (CCI) — APs on the same channel hearing each other share airtime (CSMA/CA defers). The dominant capacity killer; solved with more channels and lower power, not more APs. **[Wireless, Data-Center Fabrics and Cloud Networking]**

Code 22 / 28 — Device disabled / drivers not installed. **[Hardware Troubleshooting Playbook]**

Code 43 — Driver stopped the device after it reported problems: typical of failing USB devices and GPUs. **[Hardware Troubleshooting Playbook]**

Code 45 / 52 — Device not currently connected / driver signature cannot be verified (Secure Boot, unsigned driver). **[Hardware Troubleshooting Playbook]**

Code / paste search — Searching public repositories and paste sites for a company's domain or key formats uncovers leaked secrets and internal URLs. *[Reconnaissance and OSINT]*

Code signing — Digital signature proving publisher identity and integrity of released code. *[CISSP Domain 8: Software Development Security]*

Coercion / Compromise — blackmail, threats to family, compromising material *[Insider Threat Program]*

COFRAC — Comite francais d'accreditation: accredits the bodies that certify HDS hosts. *[Local Authorities: the Regulatory Security Framework]*

Cohesion and coupling — Good modules have high cohesion (one purpose) and low coupling (few dependencies). *[CISSP Domain 8: Software Development Security]*

Cold start — First invocation in a new environment: extensions, runtime and init code outside the handler run once before the handler. *[Serverless and Runtime Security]*

Collector / forwarder — Agent or service that reads events at the source, buffers them, and ships them onward over an authenticated channel (Splunk UF, Elastic Agent/Beats, Fluent Bit, Vector, NXLog, rsyslog). *[Security Operations Architecture]*

Collision domain — The set of ports whose frames can collide: all ports of a hub, a single port of a switch. *[Ethernet, MAC Tables and ARP]*

Collusive insider — recruited or bribed by an outsider (criminal group, competitor, foreign service). *[Insider Threat Program]*

COM-B — Capability (knows how), Opportunity (tools, time, social norm) and Motivation (wants to) jointly produce Behaviour (Michie et al., 2011); diagnose which one is missing before designing content *[Security Awareness and Culture Programme]*

Command and Control — outbound beacon, interactive access *[Pentest Methodologies]*

Commanditaire — legal entity consuming the cloud service; its admins use the **public APIs** to manage VMs, volumes, images, secrets of their domain/projects. *[OpenStack and Virtualisation Security]*

Commit — Object pointing to one root tree, zero or more parent commits, author and committer (name, e-mail, timestamp) and a message; optionally a signature. *[Git Internals and Repository Security]*

Common control — Control implemented once by a common control provider (CCP) and inherited by many systems, such as physical security of a data centre. *[Risk Management Framework (RMF)]*

Common control framework (CCF) — an organisation's own single list of controls, each mapped to all applicable external requirements *[Compliance Frameworks Crosswalk]*

Common Criteria — ISO/IEC 15408 evaluation framework; replaced TCSEC (US Orange Book) and ITSEC (Europe). *[CISSP Domain 3: Security Architecture and Engineering]*

Common Criteria EAL4+ / qualification — ISO/IEC 15408; EAL4 augmented (AVA_VAN.5) is the usual level for smart cards and HSMs. ANSSI **qualification** (standard/renforcé/élevé) adds the state's recommendation of the product for regulated uses (RGS, II 901). *[OpenSSH Hardening and Hardware Security]*

Communication categories — RS.CO N1: incident coordination (parties with IR roles), incident notification (customers, regulators), public communication (media), information sharing (voluntary, e.g. ISAC). *[Incident Handling and Response]*

Communication channel — medium that moves data between primitives (wired, wireless, USB, protocol) *[Networks of Things SP 800-183]*

Community Profile — Baseline of CSF outcomes created and published for a group with shared interests: a sector (water, health, elections), a technology (cloud, AI, PNT: positioning, navigation and timing), a threat (ransomware), a regulation. An organization uses it as the starting point for its own Target Profile. NIST publishes them... *[NIST Cybersecurity Framework 2.0; Incident Handling and Response]*

Comparative — ENISA's column saying whether a risk is higher, equal or lower in the cloud than on premises. *[ENISA Cloud Computing Risk Register (2009)]*

Compartmentalize — Isolate components so a breach stays contained *[OWASP Developer Guide v4.2 - Chapter by Chapter]*

Compensating control — Alternative control that reduces a risk to an acceptable level when the required control cannot be implemented. *[Attack Mitigation and Vulnerability Response; CompTIA SecAI+ CY0-001 +2]*

Compensating controls — WAF (web application firewall) virtual patch, IPS signature, disable the feature, extra monitoring *[Vulnerability Management and Monitoring]*

Competency Area — A cluster of related TKS statements used to assess a learner or team on a topic (Cloud Security, AI Secu-

ity, Cryptography). Rev. 1 introduced them as **Competencies** (name, description, assessment method, group of TKS statements); the 2024 Components call them Competency Areas. *[NICE Workforce Framework for Cybersecurity]*

Complain mode — AppArmor mode where violations are logged but allowed, used to build a profile; the SELinux equivalent is permissive. *[Linux Hardening in Practice]*

Complementary user entity controls — Controls a service organisation's SOC report assumes the customer operates (e.g. reviewing its own users' access); the customer's auditor must test them. *[CISA Practice Scenarios]*

Complete mediation — Check authorization on every access, not only the first one *[System Partitioning: ANSSI PG-040; Security Operations: Logs, Malware, Servers, Media +1]*

Compliance inheritance — the provider's certified infrastructure is out of scope of the customer's audit, but the customer must still make everything it builds on top compliant. *[CSA Security Guidance v4: the 14 Domains]*

Compliance report — Findings mapped to a requirement set (PCI DSS 11.3 quarterly scans, ISO 27001 Annex A 8.8 technical vulnerability management, HIPAA risk analysis) with pass/fail, exceptions and evidence for auditors. *[Reporting and Communication]*

Composite signature / certificate — one key and signature object containing a classical and a PQ component, both verified; alternative to dual certificate chains *[Quantum-Safe Network Protocols: Status]*

Compromise recording — SP 800-123 principle: record breaches (logs, integrity alerts) when preventing them is not feasible. *[Security Operations: Logs, Malware, Servers, Media]*

Compromised insider — legitimate account used by an outside attacker after phishing or token theft; looks like an insider in the logs. *[Insider Threat Program]*

CompTIA — Vendor-neutral IT association; Security+, CySA+, PenTest+, SecurityX (ex-CASP+) and SecAI+. *[Security Certification Landscape]*

Computed indicator — Derived from incident data: hash values, regular expressions. *[Pentest Methodologies]*

Concentration risk — Dependence on one provider, region or technology whose failure hits many processes at once. *[CISM Domain 2: Information Security Risk Management; Third-Party Risk Management (TPRM)]*

Conditional access — Policy at the IdP combining user risk, sign-in risk, device compliance, location, application sensitivity

→ allow, require MFA, block, limit session. *[Security Architecture - SDLC, IAM Design, Cloud]*

Conditional access failures — User-to-device binding (token bound to a device key so a stolen token fails elsewhere), geographic location (impossible travel = two sign-ins too far apart for the elapsed time), time-based windows, configuration (compliant device required) - troubleshoot with the sign-in log's policy evaluation detail. *[Security Engineering - IAM, Endpoints, Network, Hardware, OT, Automation]*

Conditional certification — Level 2: score of at least **80 %** (88 of 110) with only POA&M-eligible items open (no 3- or 5-point items except listed exceptions); close-out assessment within **180 days** or the certification lapses. *[SP 800-171 Rev. 3, CUI and CMMC 2.0]*

Conditional forwarder — Resolver rule that sends queries for one domain to a chosen server instead of the normal recursion. *[ICMP, Path MTU, DHCP and DNS Operations]*

Conditional UI — Passkeys offered in the browser's autofill list on the username field (mediation: 'conditional', autocomplete="username webauthn"), so users need no separate button. *[Passkeys and Passwordless Authentication]*

Conduit — Logical grouping of the communication channels between two or more zones; a conduit inherits the highest SL of the zones it connects. *[ANSSI ICS/SCADA Security; OT/ICS Network Security]*

Confabulation — NIST term for a model confidently producing false or fabricated content (hallucination). *[LLM Application Security Testing; AI Risk Management Program Design]*

Confidence coefficient — Probability the sample represents the population (e.g. 95 %); higher confidence needs a larger sample. *[CISA Domain 1: Information System Auditing Process]*

Confidence level — **Confidence level** - a score built independently for the user and for the non-person entity (device, process) from attributes such as identity, location, time and device posture, then aggregated where appropriate. Above a measured threshold the request is authorized; every enforcement point logs to the SIEM, which... *[DoD Zero Trust Reference Architecture v1.0]*

Confidentiality — Only authorized subjects can read the data; countered by disclosure. *[CISSP Domain 1: Security and Risk Management]*

ConfigMap — Non-secret configuration (key/values, files) injected as env vars or mounted files, kept out of the image. *[Kubernetes hands-on: learn it in your own lab]*

Configuration Control Board (CCB) — Group that approves or rejects changes after a security impact analysis (control CM-4); emergency changes reviewed after the fact. *[Patch, Configuration and Continuous Monitoring]*

Configuration drift — Difference between the intended configuration (from the source of truth) and what actually runs on the device, usually from manual out-of-band changes. *[CIS Controls v8.1 and NIST SP 800-171r3; Network Operations: Documentation, Monitoring, Resilience +1]*

Configuration management — Approved baseline + change control + drift detection (SCAP scans, GPO = Windows Group Policy, Ansible). Most misconfiguration findings are configuration-management failures. *[Attack Mitigation and Vulnerability Response]*

Configuration management database (CMDB) — Repository of configuration items and their relationships; accuracy drives impact analysis for changes and incidents. *[CRISC Domain 4: Information Technology and Security]*

Configuration profile — signed XML file (.mobileconfig) holding payloads: Wi-Fi, certificates, PPC, FileVault, firewall, restrictions, system extension allow-lists. *[macOS Security for Defenders]*

Confirm safe calls — html/template, ?-params, crypto/rand *[Go for Security Tooling and Safe Code]*

Conflict of interest — Relationship between people choosing a vendor and the bidders that could bias the choice; disclose it, rotate evaluators, document the scoring. *[Governance, Risk and Third-Party Management]*

Confused deputy — A privileged service tricked into using its own rights on behalf of a less-privileged caller (for example a vendor role assumed by another customer of the same vendor). *[AWS Security Essentials; Agentic AI and MCP Security +2]*

Confusion matrix — true/false positives and negatives of the automated stage; false positives overload analysts but are visible, false negatives are the silent failure. *[Security Supervision: ANSSI GP-112 and PG-113]*

ConMon (continuous monitoring) — Ongoing scanning, reporting and reassessment after the ATO (control CA-7, guide SP 800-137). *[NIST SP 800-53r5 Controls in Practice]*

Connect scan (-sT) — Full TCP connect; no root needed but always logged by the target service. *[Reconnaissance and OSINT]*

Connection ID — QUIC identifier chosen by each endpoint and carried in packet headers; lets a connection survive a change of

IP address or port (connection migration). *[Protocol Walk-Throughs at Packet Level]*

Connection-oriented vs connectionless — Connection-oriented services set up state first (TCP, telephone call); connectionless services send each unit independently (UDP, IP, postal letter). *[Network Models, Performance and the Physical Layer]*

Connectivity — Redundant uplinks and ISPs, out-of-band (OOB) management network, cellular backup; never manage devices over the production data path. *[Securing Enterprise Infrastructure]*

Console web malveillante / Webshell — Malicious file executed by a web server giving remote command execution on it. *[ANSSI CyberDico FR/EN Glossary]*

Constant-time code — Implementation whose timing and memory-access pattern do not depend on secret values. *[CPU Side Channels and Memory Attacks]*

Constant-time compare — subtle.ConstantTimeCompare(a, b) takes the same time regardless of where the bytes differ, so an attacker cannot learn a secret from response timing; == returns early. *[Go for Security Tooling and Safe Code]*

Constant-time comparison — Equality check whose duration does not depend on where the first differing byte is, so response timing leaks nothing about a secret. *[Cryptography in Code]*

Consumer lag — Number of messages (or time) between the newest record in a Kafka partition and the consumer group's committed offset. *[Observability and Security Telemetry Pipelines]*

Container — Process isolated by the host kernel (namespaces, cgroups) and started from an image; shares the host kernel, unlike a VM. *[Docker and Containers Hands-On; Container and Virtualization Security]*

Container escape — Breaking out of container isolation to the host, typically via privileged mode, host mounts, kernel or runtime bugs. *[Kubernetes Security]*

Container key — Random symmetric key that encrypts the content of one .zed container. *[ANSSI Encryption Tools: Zed! and Cryhod (1/2, Zed!)]*

Container runtime — seccomp, non-root, capabilities *[NIST Cloud, Virtualization, and Container Security]*

Content discovery (forced browsing) — Requesting many candidate paths from a wordlist to find pages not linked anywhere (old backups, admin panels, API routes). *[Web and API Testing Toolkit for Your Own Apps]*

Context — A named (cluster, user, namespace) tuple in kube-config; `kubectl config use-context` switches which cluster and identity every command targets. *[kubectl and Cluster Operations Mastery]*

Context window — Maximum amount of text (measured in tokens, about 3/4 of a word each) the model considers at once; data beyond it is silently ignored or truncated. *[AI Assistants for Defenders]*

Context window (LLM04) — Maximum text the model handles, input plus output, fixed by the architecture. v1.1 lists continuous input overflow, repeated long inputs, recursive context expansion and variable-length floods as DoS patterns. *[OWASP LLM Top 10 v1.1 (2023) and the 2025 Shift]*

Contextual information (4.1) — Five areas: user attributes, device health and risk, real-time context (time, geolocation), the IT service accessed, and the security of its hosting environment. Must be real time, prioritized, proportional to risk. *[Secure Enterprise Network Landscape SP 800-215]*

Contextual trust algorithm — Takes the subject's recent history into account, so it can flag an attacker using stolen credentials in an atypical pattern. *[Zero Trust Architecture SP 800-207]*

Continual improvement — learning and experience *[CRISC Domain 1: Governance]*

Continuity kit (mallette) — Documents and means needed in a major incident (contacts, procedures, credentials, media), with a copy outside the IS. *[Preparing Cyber Remediation]*

Continuous Access Evaluation (CAE) — Near-real-time revocation of access tokens by resource providers when a user is disabled, changes password or moves location. *[Azure and Entra ID Security Essentials]*

Continuous auditing — Auditor-owned automated testing performed close to real time to provide ongoing assurance. *[CISA Domain 1: Information System Auditing Process]*

Continuous monitoring — Management-owned automated oversight of controls and risks; the auditor may rely on it after testing it. *[CISA Domain 1: Information System Auditing Process]*

Continuously reconciled — agents compare live vs desired on a loop and correct drift, not only on deploy *[GitOps and Continuous Delivery Security]*

Contractual obligations — Duties created by contracts rather than law (PCI DSS via card brands, SLAs, DPAs, right to audit) - breaching them costs fines, termination or loss of card acceptance. *[Compliance, Threat Modeling and AI Security]*

Control deficiency — Gap between a control objective and what a control actually achieves, in design or in operation. *[CISM Domain 2: Information Security Risk Management; CRISC Domain 2: IT Risk Assessment]*

Control enhancement — Numbered addition in parentheses that strengthens a base control, such as **IA-2(1)** multi-factor authentication to privileged accounts on top of **IA-2** identification and authentication of users. An enhancement is never selected without its base control. *[SP 800-53r5 Key Controls Explained]*

Control gap — Objective with no effective control, found by a gap analysis (objective 1.2: compare the current state with a target framework) against NIST CSF 2.0 (US National Institute of Standards and Technology Cybersecurity Framework), CIS (Center for Internet Security) Controls v8.1 or ISO/IEC 27001:2022 (international. . . *[Security Controls]*

Control objective — Statement of the result a control must achieve, derived from a risk or requirement. *[CISM Domain 3: Information Security Program; Security Controls]*

Control of media (4.4) — Maintenance under contract with confidentiality clauses, or on site under supervision, stays **under organization control**; warranty swaps and rebates where the drive is not returned are **external control** (sanitize to Purge or keep the drive). *[Malware, Servers and Media in Depth]*

Control path — Set of direct control relationships, each showing how one entity controls another through a property; reveals deviations, validates the perimeter around Tier 0 and exposes persistence left after an intrusion. *[Active Directory Tier 0 Remediation]*

Control path (chemin de contrôle) — Chain of AD permissions (ACL, group membership, GPO rights) through which one object can take control of another. *[ANSSI Active Directory Recommendation Catalogue]*

Control plane / data plane — management components (admin and workload vCenters, NSX Manager, NSX Controllers, ESXi admin interfaces) vs hosted VMs and business storage. Separating them protects the platform from the VMs it hosts (R3). *[VMware vSphere and ESXi Security]*

Control risk — Risk that a material error is not prevented or detected by internal controls. *[CISA Domain 1: Information System Auditing Process]*

Control self-assessment — Workshops where process owners assess their own controls; complements but never replaces audit. *[CISA Domain 1: Information System Auditing Process]*

Control self-assessment (CSA) — Business owners evaluate their own controls in structured workshops; cheap and engaging, but not independent. *[CISM Domain 2: Information Security Risk Management]*

Control total — Sum of a financial field or record count compared before and after processing. *[CISA Domain 3: IS Acquisition, Development and Implementation]*

Controlled Unclassified Information (CUI) — Information the US government creates or possesses, or that an entity creates for the government, that a law, regulation or government-wide policy requires to be safeguarded (32 CFR Part 2002, managed by NARA, the US National Archives and Records Administration, in its CUI Registry). Not classified, but not public. . . *[SP 800-171 Rev. 3, CUI and CMMC 2.0]*

Cookie tossing — A compromised or attacker-controlled subdomain (evil.example.com) sets a cookie with `Domain=example.com` that the main application then reads, fixing a session or overriding a CSRF token. The `__Host-` prefix makes the browser reject such cookies for the protected name. *[HTTP Security Headers and Browser Policies]*

COOP — Continuity of operations plan: keeps essential functions running during a disruption (US federal term). *[IR Exercises and Threat Information Sharing]*

COOP (R46) — same-origin breaks `window.opener` links: protects against tab-nabbing and cross-window XS-leaks. R45: open windows with `rel="noopener noreferrer"`. *[Browser-Side Web Security Standards]*

COPE / BYOD — Corporate-Owned, Personally Enabled device versus Bring Your Own Device (personal phone used for work). *[Mobile Device Security and MDM]*

Copy-on-write (CoW) — Never overwrite in place: write new blocks, then switch pointers (APFS, Btrfs, ZFS); makes snapshots cheap and old versions linger. *[Storage and Filesystems for Defenders]*

Coraza — OWASP WAF engine written in Go, compatible with the ModSecurity rule language (SecLang) and the CRS; embeds in Caddy, Envoy (proxy-wasm) and Go services. *[WAF and API Gateway Configuration]*

Core scheduling / SMT off — Only mutually trusting tasks share a physical core (Linux core scheduling, Hyper-V core scheduler, VMware side-channel aware scheduler) or SMT is disabled: DAT-24 **R4** asks to dedicate hardware to distinct security contexts (disable Hyper-Threading, dedicated machine, CPU pinning), because two threads of one core. . . *[CPU Side Channels and Memory Attacks]*

Core tier — A small number of very fast routers/switches that only forward between distribution blocks. Kept policy-free so it never becomes a bottleneck. *[Classic Enterprise Network Architecture]*

Core vs thread — A core is a physical execution unit; SMT (simultaneous multithreading: Intel **Hyper-Threading**, AMD SMT) exposes 2 logical threads per core. 8 cores / 16 threads = 16 logical processors in Task Manager. *[CPUs, Memory, Motherboards and Buses]*

CORS (Cross-Origin Resource Sharing) — Headers by which a server allows chosen other origins to read its responses. *[Browser-Side Web Security Standards]*

CORS preflight (R39) — OPTIONS with Access-Control-Request-Method; server answers allowed origin, methods, headers, Max-Age. Avoid *simple requests* that skip it (R35, R36: prefer POST/PUT with JSON content type). *[Browser-Side Web Security Standards]*

COSO — Committee of Sponsoring Organizations of the Treadway Commission - Internal Control Integrated Framework (2013) and ERM framework (2017); the SOX internal-control reference, 5 components: control environment, risk assessment, control activities, information and communication, monitoring. *[CompTIA SecurityX CAS-005 - Exam Overview]*

Cost — Time and money of the unmitigated reliability and security risks plus the cost of each primitive; drives design decisions. *[Routing I: Routing Table, Static Routes, OSPF; Networks of Things SP 800-183]*

Cost per record — average cost divided by records lost: USD 169 in 2024; customer PII was the most common type stolen (46 % of breaches). *[IBM Breach Cost and X-Force Index 2024]*

Count-to-infinity — After a link fails, two distance-vector routers keep learning the dead route from each other, raising the metric by one per exchange until the 'infinity' value (16 in RIP). *[Routing I: Routing Table, Static Routes, OSPF]*

Coverage — share of ATT&CK techniques with at least one tested detection on the perimeter; the guide's effectiveness metric. *[ANSSI Logging and Security Supervision]*

Coverage-guided fuzzing — Automated testing that mutates inputs and keeps those that reach new code edges, steering towards deep, rarely-run paths. *[Memory Safety and Fuzzing]*

Coverage matrix — ATT&CK technique grid coloured by how well you detect each technique (none, partial, tested); built

in ATT&CK Navigator. *[Detection Rules: Sigma and YARA Catalogue]*

Coverage (section 2.1) — Covering every technique is unrealistic and not the goal. Some behaviours (ipconfig.exe, Valid Accounts) warrant collected telemetry, not alerts. Anyone mapping to ATT&CK must be able to explain which procedures they cover; one analytic rarely covers a whole technique (Get-NetIPConfiguration bypasses an ipconfig rule). *[ATT&CK Design Philosophy, ATT&CK for ICS, CISO View]*

Covered cyber incident (CIRCIA) — substantial cyber incident at a covered critical-infrastructure entity, as defined in CISA's final rule *[Global Security and Privacy Regulations]*

Covered entity (HIPAA) — health-care provider transmitting health information electronically, health plan or clearinghouse; directly regulated by HHS Office for Civil Rights *[Global Security and Privacy Regulations]*

Covert channels — DNS tunneling (iodine, dnscat2), ICMP (icmsh), HTTPS blend, steganography. *[Post-Exploitation and Lateral Movement]*

Covert channels and marking (R13, R14) — Every downward design leaks through covert channels. R13: the designer characterises and documents each one (inherent, configuration-dependent, residual after added measures), its exploitation conditions and maximum rate; e.g. an attacker encoding data in sequences of individually allowed messages, detected by... *[Multilevel Interconnections & Trusted Core]*

Covert testing — Black hat: only upper management knows; tests detection and response of IT staff. *[PTES Phase Tasks, SP 800-115, Kill Chain Analysis]*

CPE / CEU — Continuing professional education credits (ISC2, ISACA) or continuing education units (CompTIA) needed to keep a certification active. *[Security Certification Landscape]*

CPG — **CPG** - a prioritized subset of IT and OT practices that every critical infrastructure organization, from large to small, should implement: a floor, not a ceiling. Each goal is mapped to NIST CSF 2.0 subcategories and to SP 800-53 r5 / SP 800-82 r3 controls, and rated for **Cost**, **Impact** and **Ease of...** *[CISA Cybersecurity Performance Goals 2.0]*

CPME — Confederation des petites et moyennes entreprises: French SME employers' federation, co-author of the TPE/PME guide. *[Business Travel and SME Cybersecurity]*

CPU LED — CPU seating, EPS 8-pin, BIOS support for the CPU *[Hardware Troubleshooting Playbook]*

CRA — EU Cyber Resilience Act (Regulation 2024/2847): security requirements and vulnerability reporting for products with digital elements; reporting from September 2026, full application December 2027. *[Start-ups, Municipalities, Teleassistance, Open Source]*

CRA (Cyber Resilience Act) — EU Regulation 2024/2847: security-by-design and vulnerability handling duties for products with digital elements. *[ENISA ETL 2024, DoD Zero Trust, ATT&CK for ICS]*

CRC / input errors — Frames failing the FCS check: physical layer (cable, EMI, optic) or the full-duplex side of a duplex mismatch. *[Network Troubleshooting: Method, Layers, Tools, Symptoms]*

Credential — Binding of an authenticator to an identity (password record, certificate, passkey). *[CISSP Domain 5: Identity and Access Management]*

Credential Guard — virtualization-based security moves NTLM hashes and Kerberos TGT keys into LSALso.exe in VTL1 (virtual trust level 1), unreadable even by a kernel-level attacker; on by default on eligible Windows 11 22H2+ Enterprise devices (verify for your build). *[Windows Internals for Defenders; Windows Hardening Baseline]*

Credential stuffing — Automated reuse of username-password pairs leaked from other sites. *[CISSP Domain 5: Identity and Access Management; Authentication and Session Design]*

CREST — Council of Registered Ethical Security Testers - accreditation body. *[CompTIA PenTest+ PT0-003]*

crictl — The CRI (Container Runtime Interface) debugging CLI; talks straight to containerd/CRI-O on a node, bypassing kubelet and the API server. *[kubectrl and Cluster Operations Mastery]*

Crisis cell — small decision body activated when an incident threatens the organisation's operations, reputation or legal position; separate from the technical response team *[Crisis Communication and Tabletop Exercises]*

Crisis logbook — timestamped record of facts, decisions, owners and messages sent (main courante in French); evidence for regulators, insurers and the after-action review *[Crisis Communication and Tabletop Exercises]*

Crisis management exercise — Simulation of a **scenario** (a chain of fictitious but credible events) over a limited period, in a context designed for the occasion, where players manage the crisis as it unfolds. The guide covers **decision-level** exercises training the crisis unit, not purely technical simulations (cy-

ber range). Method based on... *[Organising a Cyber Crisis Management Exercise]*

Criteria — Benchmark against which the subject matter is evaluated: policy, law, standard, contract, framework. *[CISA Domain 1: Information System Auditing Process]*

Criteria-based trust algorithm — Every configured attribute must be met (for example: managed device AND MFA AND role = finance) or access is denied. *[Zero Trust Architecture SP 800-207]*

Critical or important function — DORA Art. 3(22): a function whose disruption would materially impair financial performance, soundness or continuity of services, or compliance with licence conditions. *[DORA: Digital Operational Resilience]*

Critical path — Longest sequence of dependent activities; zero slack, determines the project end date. *[CISA Domain 3: IS Acquisition, Development and Implementation]*

CRL — Certificate Revocation List: CA-signed list of revoked certificate serial numbers. *[Stormshield SNS 3.7.17 Hardening by Chapter]*

CRL / delta CRL (RFC 5280) — Signed list of revoked serials with reason codes, published at the CRL Distribution Point; issuing CAs publish at least daily, root CRL at each ceremony. *[PKI and ACME Certificate Automation]*

CRL / OCSP — Revocation list published periodically versus a real-time status query. *[CISA Domain 5: Protection of Information Assets]*

CRLDP / AIA — CRL Distribution Point and Authority Information Access: certificate fields giving where to fetch revocation lists and the OCSP responder. *[ANSSI TLS and IPsec Guides: Full R Index]*

Cross-account resources — Stage to another cloud account/tenant the attacker controls (assumed role, shared bucket) so exfil stays inside provider traffic. *[Post-Exploitation and Lateral Movement]*

Cross-origin isolation — State (window.crossOriginIsolated = true) reached with COOP same-origin plus COEP require-corp or credentialless; unlocks SharedArrayBuffer and precise timers safely against Spectre-class leaks. *[HTTP Security Headers and Browser Policies]*

Cross-restore — restoring on one backup instance data stored by another instance; mixes sensitivity levels, disabled by default (R19). *[IT Backup - ANSSI BP-100 R1-R32]*

Cross-sectoral profile — Profile for models or activities common across sectors, such as large language models, cloud services

or acquisition; AI 600-1 is one. *[AI Risk Management Framework]*

Crosswalk — table mapping one control or requirement to its equivalents in other frameworks; the basis of a common control framework *[Compliance Frameworks Crosswalk]*

Crown jewels — The client's most valuable assets (customer database, payment system, domain admin) used as test objectives. *[Engagement Methodology and Reporting; Red Team Programme and Rules of Engagement]*

CRQC — Cryptographically relevant quantum computer: one large enough to run Shor against real key sizes. *[ANSSI Cryptographic Mechanisms and PQC; Post-Quantum Migration Playbook +1]*

CRS — OWASP Core Rule Set: generic attack-detection rules for ModSecurity or Coraza web application firewalls. *[OWASP Secure Coding Practices and Developer Guide]*

CRTM — Core Root of Trust for Measurement: first immutable firmware code that measures the rest of the boot chain into the TPM. *[OpenSSH Hardening and Hardware Security]*

Crypto agility — Ability to change algorithms, key sizes and CAs by configuration and automation, without code rewrites: algorithm ids carried in the data, a CBOM (Cryptographic Bill of Materials, e.g. CycloneDX 1.6) listing every use, and short certificate lifetimes so a new algorithm reaches the fleet in weeks. *[Post-Quantum Migration Playbook; Quantum-Safe Network Protocols: Status +1]*

Crypto-agility (ANSSI views, 2025) — Ability to extend and/or replace cryptographic components of an IT system without affecting its functionality, while minimising service downtime during the update. Two levels: **parameterisation** (AES-128 to AES-256, ML-DSA-65 to ML-DSA-87, RSA-2048 to RSA-4096) and **algorithmic** (SHA-2 to SHA-3, ML-KEM to HQC,...) *[ANSSI Cryptographic Mechanisms and PQC]*

Crypto-erase — Sanitisation by destroying every copy of the key that encrypts the media, leaving only unreadable ciphertext. *[Storage and Filesystems for Defenders]*

Crypto-period — Validity window of a key, as a date or a usage count, after which it must be replaced. *[ANSSI Crypto Rules Catalogue (PG-083 v3.00)]*

crypto/rand — The cryptographically secure random source; use it (not math/rand) for keys, salts, nonces and tokens. *[Go for Security Tooling and Safe Code]*

Crypto regime — Use of cryptology is free in France (LCEN, the 2004 law on confidence in the digital economy, art. 30); sup-

ply, import and export are declared to or authorised by ANSSI. *[HTTPS Flow Inspection: Proxy and Reverse Proxy]*

Crypto Sheriff — No More Ransom tool that identifies a ransomware family from an encrypted file and the note, and points to a free decryptor if one exists. *[Ransomware: Respond and Recover]*

Crypto-shredding — Making data unreadable by destroying or disabling its encryption key instead of deleting every copy. *[CCSP and CCSK: Cloud Security Certifications; GCP Security Essentials +1]*

Cryptographic erase — Sanitization by destroying the media encryption key, leaving only unreadable ciphertext. *[Multi-Environment Workstation and Refurbishing; Storage: Interfaces, SSD Internals, RAID, SMART]*

Cryptographic erase (CE) — Purge technique that destroys the media encryption key so the stored ciphertext can no longer be decrypted; takes seconds on self-encrypting drives. *[NIST Security Operations Guides; Malware, Servers and Media in Depth]*

Cryptographic erase (sec. 2.6, App. D) — Sanitize by destroying the media encryption key. Valid only if all data was encrypted before storage, the key was never exposed, and the algorithm is strong (FIPS 140 validated modules). *[Security Operations: Logs, Malware, Servers, Media]*

Cryptographic flaws (OSINT) — Weak TLS versions and ciphers, expired or self-signed certificates and reused keys visible in public scan databases (Censys, Shodan) without touching the target. *[Reconnaissance and OSINT]*

Cryptoperiod — How long a key is allowed to be used before rotation; limits the damage of an undetected key compromise. *[Cryptography; NIST Cryptographic Standards]*

Cryptoperiod (SP 800-57 Pt 1) — Private signing key 1-3 years; symmetric data key ≤ 2 years for the originator; root CA 10-20 years; session keys per connection. Rotate = new key material, never reuse. *[NIST Cryptography, TLS and PKI]*

CSA CCM (Cloud Controls Matrix) — Cloud Security Alliance catalog of cloud controls (v4: 197 controls in 17 domains) mapped to ISO 27001, NIST and others. *[Cloud Computing Security]*

CSE — Comite social et economique: elected staff representative body, consulted before rules are added to the internal rules. *[IT Usage Charter and Outsourcing Security]*

CSF 2.0 — NIST Cybersecurity Framework 2.0 (Feb 2024): 6 Functions, 22 Categories, 106 Subcategories describing security outcomes, not controls. *[Incident Handling and Response]*

CSIRT — Computer Security Incident Response Team; the national one receives NIS2 and CRA reports. *[EU Governance and Regulation: Self-Assessment; IR Teams, Playbooks and Lessons Learned]*

CSIRT / CERT — Computer Security Incident Response Team: in-house or sector team that receives alerts, analyses and responds to attacks. *[Cyber Crisis Management & Communication]*

CSIRT vs PSIRT — A CSIRT protects a constituency (organisation, sector, country) against incidents; a PSIRT handles vulnerabilities in the products an organisation ships (FIRST PSIRT Services Framework v1.1). Many vendors run both. *[SOC 2 Trust Services Criteria, COBIT 2019, CSIRT Services]*

CSK — Combined Signing Key: one DNSSEC key that plays both the key-signing (KSK) and zone-signing (ZSK) roles. *[DNS Infrastructure Operations]*

CSMA/CD — Carrier Sense Multiple Access with Collision Detection: listen before sending, detect a collision while sending, jam, then wait a random binary exponential backoff. Needed only on half-duplex shared media; a full-duplex switched link has no collisions. *[Ethernet, MAC Tables and ARP]*

CSP — Cloud service provider (AWS, Microsoft Azure, Google Cloud) that runs the shared infrastructure. *[Security Architecture Models; Digital Identity Guidelines SP 800-63-4]*

CSP (Content Security Policy) — Header listing the sources from which a page may load scripts, styles, frames and connections. *[Browser-Side Web Security Standards]*

CSPM — Cloud Security Posture Management: tool that continuously compares cloud configuration with a benchmark. *[Cloud Configuration Review]*

CSPM / CWPP / CNAPP — Cloud security posture management (finds misconfiguration), cloud workload protection platform (VM/container runtime), cloud-native application protection platform (both combined). CIEM = cloud infrastructure entitlement management (excess permissions). *[NIST Cloud, Virtualization, and Container Security]*

CSPN — Certification de securite de premier niveau: ANSSI fixed-time, fixed-budget product evaluation, lighter than Common Criteria. *[Local Authorities: the Regulatory Security Framework; Multi-Environment Workstation and Refurbishing +2]*

CSPRNG — Cryptographically secure pseudo-random number generator (e.g. SecureRandom, secrets, /dev/urandom). *[Cryptography Primer; Cryptography in Code +1]*

CSR — Certificate Signing Request (PKCS#10): subject, public key and requested extensions, signed with the private key to prove possession; the CA never sees the private key. *[OpenSSL and Certificate Tooling]*

CSRF — Cross-Site Request Forgery: a malicious site makes the victim's browser send an authenticated request to another site. *[OWASP Top 10 2017 and Risk Rating]*

CSRF (cross-site request forgery) — Another site makes the victim's browser send an authenticated request to your site. *[Browser-Side Web Security Standards]*

CT (Certificate Transparency) — Public append-only logs of issued certificates; an SCT is the log's signed receipt embedded in the certificate. *[TLS, IPsec and SSH Hardening]*

CT.DP-P5 attribute references — Share a claim ("over 18", "resident of X") instead of the value (date of birth, address): the basis of selective disclosure credentials and the EU Digital Identity Wallet. *[NIST Privacy Framework 1.0]*

CT / SCT — Certificate Transparency public logs; a Signed Certificate Timestamp is the log's receipt embedded in the certificate. *[ANSSI TLS and IPsec Guides: Full R Index]*

CTI — Cyber threat intelligence: information on threat actors, their TTPs (tactics, techniques, procedures) and IoCs (indicators of compromise: hashes, IPs, domains). *[Incident Handling and Response]*

CTI (cyber threat intelligence) — collected knowledge on attackers, leaks and campaigns, used to anticipate and detect. *[Data Protection: Classification, Leaks, GDPR]*

CTPP — Critical ICT third-party service provider designated by the ESAs (Art. 31) and overseen directly by a Lead Overseer. *[DORA: Digital Operational Resilience]*

CTY / VTY — Console line (physical serial port) and virtual terminal lines (usually 16, numbered 0-15, used by SSH sessions). *[Access Switch Audit Grid: DAT-NT-025 R1-R71]*

CUI (Controlled Unclassified Information) — Government information that is not classified but still needs safeguarding by law or policy: export-controlled technical data, defence program drawings, personal data held for an agency. Any contractor or university whose own systems store CUI must implement SP 800-171. **FCI** (Federal Contract Information) is the ... *[CIS Controls v8.1 and NIST SP 800-171r3]*

Current profile / target profile — Temporal profiles: how AI risk is managed today versus the outcomes wanted; the gap drives an action plan. *[AI Risk Management Framework]*

Current risk — Actual risk at a point in time, reflecting controls as they really operate today (may be higher than planned residual). *[CRISC Domain 2: IT Risk Assessment]*

Custom Resource Definition (CRD) — An object that teaches the Kubernetes API server a new resource kind, enabling custom resources handled by an operator. *[Helm, operators and the CRD ecosystem (with security)]*

Customer-managed key — customer controls the key, provider runs the engine; if the key lives in the provider's KMS it is still potentially reachable by the provider. *[CSA Security Guidance v4: the 14 Domains]*

Customized approach — PCI DSS 4.x option to meet a requirement's stated objective with your own control, backed by a targeted risk analysis *[Compliance Frameworks Crosswalk]*

Customized approach objective — Printed under each eligible requirement; the outcome to meet another way. Needs a targeted risk analysis (12.3.2), a controls matrix and assessor-designed tests. Not available to SAQ filers. *[PCI DSS v4.0.1 Requirement by Requirement]*

CVD (Coordinated Vulnerability Disclosure) — Process in which a finder, the vendor and often a coordinator agree on fixing a flaw before it is published. *[Law and Ethics for Security Practitioners]*

CVE — Common Vulnerabilities and Exposures: unique public identifier for one known vulnerability (CVE-2021-44228 = Log4Shell). *[Famous Vulnerabilities Explained; CISSP Domain 6: Security Assessment and Testing +4]*

CVM (Confidential Virtual Machine) — VM-level TEE (AMD SEV-SNP, Intel TDX, Arm CCA Realm): the whole guest OS runs encrypted, the host is outside the trust boundary *[Confidential Computing and Remote Attestation]*

cVM (confidential VM) — a virtual machine whose whole memory is encrypted by the CPU with a per-VM key, so the hypervisor cannot read it. *[Confidential Computing]*

CVSS — Common Vulnerability Scoring System (FIRST): 0.0-10.0 severity score; 9.0+ critical, 7.0-8.9 high, 4.0-6.9 medium. *[Famous Vulnerabilities Explained; CISSP Domain 6: Security Assessment and Testing +3]*

CVSS 4.0 — 2023 revision: Base/Threat/Environmental/Supplemental, adds attack requirements (AT). *[Vulnerability Discovery and Analysis]*

CVSS 4.0 (Nov 2023) — Common Vulnerability Scoring System, score 0-10 (0.1-3.9 low, 4.0-6.9 medium, 7.0-8.9 high, 9.0-10 critical). Metric groups Base, Threat (replaces Temporal), Environmental, Supplemental; label says which groups were used: CVSS-B, CVSS-BT, CVSS-BE, CVSS-BTE; new Attack Requirements (AT) and impact split into. . . *[Security Operations]*

CWE — Common Weakness Enumeration: MITRE catalogue of software weakness types, each with a number and a name. *[CISSP Domain 6: Security Assessment and Testing; OWASP Top 10 - Web (2021 and 2025)]*

CWR — Congestion Window Reduced: sender has reacted to an ECN echo *[TCP and UDP Deep Dive]*

Cyber crisis (ANSSI definition) — Immediate and major destabilisation of the day-to-day operation of an organisation (halt to activities, inability to provide services, heavy financial losses, major loss of integrity) caused by one or more **malicious** actions on its digital services and tools, which **cannot be handled through usual processes**. . . . *[Cyber Crisis Management & Communication]*

Cyber device — FDA term (section 524B): device that includes software, can connect to the internet, and could be vulnerable to cyber threats *[IoT and Medical Device Security]*

Cyber Kill Chain — Lockheed Martin model of seven intrusion stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, actions on objectives. *[CEH v13: Exam Blueprint and Module Map]*

Cyber maturity / trust — the stakeholder's security capability / your confidence in its intentions and interests; high values raise reliability. *[EBIOS Risk Manager]*

Cyber 'teams' — Employees without activity are mobilised as project teams to meet several objectives in a short time. *[Cyber Crisis Management & Communication]*

Cyber vault — air-gapped or logically isolated immutable backup copy, managed with separate credentials outside the production identity domain *[Business Continuity and ISO 22301]*

Cybermalveillance.gouv.fr — Public victim-assistance platform (GIP ACYMA) for citizens, SMEs and municipalities: diagnostics, alerts, labelled providers. *[Business Travel and SME Cybersecurity]*

Cybersecurity Act — Regulation (EU) 2019/881: gives ENISA (created 2004 by Reg. 460/2004, seat Athens, office in Heraklion) a permanent mandate and sets up the EU cybersecurity certification framework; ENISA drafts candidate schemes, the

Commission adopts them. *[ENISA, NIS2 and the EU Threat Landscape]*

Cybersecurity incident — An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity or availability of information or systems, or violates security policy. *[Incident Handling and Response]*

Cybersecurity incident (FISMA 2014) — An occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality or availability of information or a system, or violates (or imminently threatens to violate) law, security policies, procedures or acceptable use policies. *[SP 800-61r3 Community Profile in Detail]*

Cybersecurity supply chain risk — Risk that a product, service or component is compromised, counterfeit, tampered with, contains malicious functionality or unpatched vulnerabilities, or that a supplier's practices expose the acquirer. Sources: suppliers, developers, system integrators, external system service providers, other ICT/OT-related service. . . . *[Cybersecurity Supply Chain Risk Management]*

Cybersecurity workforce gap — ISC2 estimate of additional professionals organisations say they need, not a count of open job adverts. *[Industry and Workforce Reports]*

.cymap / .zaf — Files holding a workstation's encryption map and an access list; sensitive, readable only by owner and security admins (R28). *[ANSSI Encryption Tools: Zed! and Cryhod (2/2, Cryhod)]*

D

DAAS — **DAAS** - Data, Applications, Assets, Services: what zero trust protects. DoD's RA defines ZT as *never trust, always verify* applied per request, with the **Policy Decision Point / Policy Enforcement Point** pattern of NIST SP 800-207 at the core. *[DoD Zero Trust and NSA Hardening Guidance]*

DAC / MAC — Discretionary Access Control (owners set file rights) / Mandatory Access Control (a system policy the process cannot change: SELinux, AppArmor, Windows MIC integrity levels). *[System Partitioning: ANSSI PG-040]*

DAC / RBAC — Discretionary access control (owner grants rights) and role-based access control (rights attached to roles). *[ANSSI Zero Trust Model]*

dACL (downloadable ACL) — Access list sent by the RADIUS server at authentication time and applied to that port only. *[First-Hop Security and Gateway Redundancy]*

DAD (Duplicate Address Detection) — Before using an address the host sends NS from :: to the solicited-node group; any NA answer = duplicate. An attacker answering every DAD is a DoS (address never assigned). *[IPv6 in Depth: Addressing, NDP, SLAAC, Security]*

DAD triad — Disclosure, Alteration, Destruction: the attacks that defeat C, I and A. *[CISSP Domain 1: Security and Risk Management]*

DAI — Dynamic ARP Inspection: the switch drops ARP packets whose IP/MAC pair does not match the DHCP snooping table. *[ToIP and Virtualization Security]*

Daisy chaining — Gaining access to one system and using it to reach the next. *[CEH v13: Core Concepts, Phases and Legal Framework]*

DAM (Database Activity Monitoring) — Independent capture and analysis of database logins and statements to detect misuse, including by administrators. *[Database Security]*

DANE / TLSA — DNS-based Authentication of Named Entities: a TLSA record, protected by DNSSEC, pins the certificate a server must present. *[Email Security: SPF, DKIM, DMARC]*

Dark site — pre-built, unpublished web page or status page activated during a crisis to host updates, hosted outside the possibly compromised infrastructure *[Crisis Communication and Tabletop Exercises]*

DAS / NAS / SAN — Direct-attached storage (disk inside or cabled to one host); network-attached storage (file shares over SMB 445 or NFS 2049); storage area network (block storage over a dedicated fabric: Fibre Channel, **iSCSI 3260**, NVMe-oF = NVMe over Fabrics). *[Storage: Interfaces, SSD Internals, RAID, SMART]*

Data access — training sets, vector store chunks, prompt logs, weights *[Securing AI Systems]*

Data action — A system operation that processes data (collect, retain, log, generate, transform, disclose, transfer, dispose). The unit of privacy risk analysis. *[NIST Privacy Framework 1.0]*

Data altruism organisation (DGA) — not-for-profit entity registered to collect data made available voluntarily for general-interest purposes; uses the European data altruism consent form *[Data Act, Data Governance Act and EHDS]*

Data augmentation — Rotation, cropping, noise (images); paraphrase, back-translation (text); synthetic generation. Raises robustness but can amplify existing bias. *[AI Data Security and Lifecycle]*

Data balancing — Oversampling minority classes (e.g. SMOTE, which synthesises new minority samples), undersampling majority, class weights. Prevents the model from ignoring rare attacks. *[AI Data Security and Lifecycle]*

Data classification — Labelling data by sensitivity and criticality so controls are proportional; starts with the owner. *[CISA Domain 2: Governance and Management of IT]*

Data classification labels — Public / internal / confidential / restricted tags on datasets and documents, propagated to chunks and prompt logs; drive which model tier may see the data. *[Securing AI Systems]*

Data cleansing — Remove errors, duplicates, inconsistencies, noise. Garbage in = garbage out; also where obviously poisoned records are caught. *[AI Data Security and Lifecycle]*

Data controller — GDPR term: decides the purposes and means of processing personal data. *[CISSP Domain 2: Asset Security]*

Data custodian — Role (often IT) that stores and protects data according to the owner's requirements. *[CISA Domain 2: Governance and Management of IT; CISM Domain 3: Information Security Program +2]*

Data diode — Network device that physically allows traffic in one direction only. *[ANSSI ICS Detailed Measures v2 (2/2): technical measures; Removable Media Airlock and White Station +1]*

Data diode (unidirectional gateway) — Hardware that physically allows traffic in one direction only, e.g. historian data out of the control network, nothing back in. *[OT Architecture and the SP 800-82r3 OT Overlay]*

Data disclosure — excessive collection, storage, processing or sharing *[Privacy Engineering and PETs; Threat Modeling Methods +1]*

Data dispersion — bit splitting across physical storage for durability; a file is never on a single disk. *[CSA Security Guidance v4: the 14 Domains]*

Data exfiltration — Stealing data to sell, leak or exploit; precedes double-extortion ransomware (encrypt the data and also threaten to publish it). *[Threat Actors and Threat Vectors]*

Data extortion — theft of data followed by a payment demand under threat of publication, with or without encryption. *[CISA #StopRansomware Guide]*

Data holder and user — the holder controls access to readily available product data; the user (owner, renter, lessee) has the right to access it and to have it shared with a third party of

its choice (Art. 4-5) *[Data Act, Data Governance Act and EHDS]*

Data integrity — Data has not been altered without authorisation: hashes, signatures, immutable storage, access logs on buckets. *[AI Data Security and Lifecycle]*

Data intermediation service (DGA) — neutral service establishing commercial relationships for data sharing between holders and users; must notify, keep data use separate from its own business, and ensure a high level of security (Art. 10-12) *[Data Act, Data Governance Act and EHDS]*

Data-leak-site unreliability — After Operation Cronos many LockBit postings were duplicates or misattributed; do not count leak-site victims as confirmed breaches. *[Breach and Threat Landscape 2024]*

Data lineage — The **path**: every transformation from raw source to training set, who did it, when (data catalog, ETL = extract-transform-load job logs). Needed for audits and rollback. *[AI Data Security and Lifecycle]*

Data link — 2, frame: 'Do' *[Networking Ports and Protocols]*

Data localization — Legal obligation to keep certain data inside a country (e.g. some health, telecom or government data). *[Compliance, Threat Modeling and AI Security]*

Data minimisation — Art. 5(1)(c): adequate, relevant, limited to what is necessary *[GDPR for Security Teams]*

Data owner — Business role accountable for a data set's classification, access approval and retention. *[CISA Domain 2: Governance and Management of IT; CISM Domain 3: Information Security Program +2]*

Data-per-service — Each service owns its database; others reach that data only through the service's API, never by direct DB access. *[Web Application and Microservices Architecture]*

Data perimeter — Set of SCP, RCP and endpoint policies ensuring only trusted identities reach trusted resources from expected networks. *[AWS Security Essentials]*

Data permit — EHDS authorisation stating which health data a user may process, for what purpose and for how long, inside a secure processing environment. *[Data Act, Data Governance Act and EHDS]*

Data poisoning — Altering training data so the model learns a hidden behaviour triggered later by a chosen input. *[ANSSI Generative AI Security]*

Data privacy — leakage, unauthorised use or de-anonymisation of personal data (biometric, health, location), e.g. training

data regurgitated in outputs. *[AI Risk Management Program Design]*

Data processor — Processes personal data on the controller's behalf under contract (GDPR Art. 28). *[CISSP Domain 2: Asset Security]*

Data provenance — The **origin**: where the data came from and whether it is authentic and untampered (signed manifests, C2PA = Coalition for Content Provenance and Authenticity content credentials, chain of custody). *[AI Data Security and Lifecycle]*

Data residency — Requirement that data be stored and processed in a given geography. *[Data Security Posture in the Cloud; Compliance, Threat Modeling and AI Security]*

Data source / component — DS0009 Process has components Process Creation, Process Access, OS API Execution; a component lists the techniques it can detect. Build a coverage map by intersecting your telemetry with components, not technique names. *[MITRE ATT&CK]*

Data sovereignty — Data subject to the laws of the country where it is stored, and protected from foreign legal access; stronger than residency. *[Data Security Posture in the Cloud; Compliance, Threat Modeling and AI Security]*

Data steward — Ensures data quality, metadata and business meaning; governance, not security enforcement. *[CISSP Domain 2: Asset Security]*

Data subject — The identified or identifiable natural person the personal data describes. *[CISSP Domain 2: Asset Security]*

Data tier — Storage class for data of a given age: hot (fast disks, being written), warm, cold, frozen (object storage or archive). *[SIEM Architecture and Sizing]*

Data verification — Confirm accuracy and completeness against trusted sources; checksums per dataset version (data version control tools such as DVC and lakeFS, Hugging Face dataset hashes). *[AI Data Security and Lifecycle]*

Datastore (NMDA) — Named copy of configuration or state (RFC 8342 Network Management Datastore Architecture): running, candidate, startup, intended, and operational (what the device is really doing). *[Network Automation and Observability]*

DBIR — Verizon's yearly study of incidents and confirmed breaches contributed by dozens of partners (IR firms, CERTs, law enforcement), coded with VERIS (Vocabulary for Event Recording and Incident Sharing). *[Breach and Threat Landscape 2024]*

DBSC — Device Bound Session Credentials: sessions tied to a private key kept in the device TPM, so copied cookies stop working quickly *[Browser and Extension Security]*

dbx — UEFI forbidden-signature database: hashes and certificates that must never boot. *[UEFI, Secure Boot and Bootkits]*

DC — Domain controller: server holding the AD database (NTDS.dit) and issuing Kerberos tickets. *[Active Directory Tier 0 Remediation; Identity and Active Directory Assessment]*

DCS (Distributed Control System) — Integrated control for a single large plant (refinery, power station); many controllers under one supervisory system. *[Industrial (OT/ICS) Architecture]*

DCSync — Abusing directory replication rights to ask a DC for any account's password hash, krbtgt included. *[Active Directory Security; Windows Audit Policy and Event ID Reference +1]*

DDM (Declarative Device Management) — newer Apple management model (macOS 13+): the device holds declarations and reports status changes itself; now the supported way to enforce software update deadlines. *[macOS Security for Defenders]*

Dead-box vs live — dead: system powered off, disk imaged offline (no volatile data). Live: system running, memory and volatile state captured first. *[DFIR Artifacts and Tools]*

Débridage / Jailbreak — Bypassing a system's protections to remove the manufacturer's usage restrictions. *[ANSSI CyberDico FR/EN Glossary]*

Deception platform — product that deploys, rotates and monitors decoys at scale (Thinkst Canary, Zscaler Deception, SentinelOne Singularity Hologram, Acalvio). *[Deception: Honey-pots, Honeytokens, Canaries]*

Decision trigger — conditional expression that produces the NoT's final result and may drive an actuator *[Networks of Things SP 800-183]*

Declarative vs imperative — Declarative: describe the desired state ("VLAN 20 exists on these ports") and let the tool compute the commands. Imperative: send the commands yourself, in order. *[Network Automation and Observability]*

Deconfliction — Confirming with the client whether an observed event is your testing or a real incident, so a genuine breach is never mistaken for the test (and vice versa). *[CEH v13: Practice Scenarios; PenTest+ Practice Scenarios +2]*

Decoy account — directory account that no person or service uses; any authentication or query against it is an alert. *[Deception: Honey-pots, Honeytokens, Canaries]*

Decryption (déchiffrement) — The proxy terminates the client's TLS session with its own certificate and opens a second TLS session to the real server: clear HTTP exists on the proxy in between. *[HTTPS Flow Inspection: Proxy and Reverse Proxy]*

Decryptor — Program that reverses the encryption with the key; the attacker's own tools are often slow and corrupt files being written during encryption (databases). *[Ransomware: Respond and Recover]*

DECT — Digital Enhanced Cordless Telecommunications: cordless handset radio standard, advised against by R48. *[ToIP and Virtualization Security]*

Deepfake — AI-generated or AI-altered audio, image or video that imitates a real person. *[Social Engineering and Deepfakes]*

Deepfake content — impersonation, misinformation (false), disinformation (deliberately false) *[AI-Assisted Security]*

Defacement — Replacement of a website's pages by the attacker's message; very visible, usually low technical impact. *[Cyber Crisis Communication]*

Defanging — making an indicator non-clickable when sharing it: `hxxp://evil[.]com, sample.exe_`. *[Malware Triage and Analysis]*

Default — switchport port-security alone = maximum 1 MAC, violation shutdown, no aging. Only on static access or trunk ports, never on a dynamic port. *[First-Hop Security and Gateway Redundancy]*

Default SAs — Compute Engine default SA (PROJECT_NUMBER-compute@developer...) is granted **Editor** on project creation unless the org policy `iam.automaticIamGrantsForDefaultServiceAccounts` is enforced; App Engine default SA likewise. Replace with dedicated, least-privilege SAs. *[GCP Security Essentials]*

Default VLAN (VLAN 1) — Never used for anything (R28); all ports moved out of it, control protocols still use it internally. *[Network Equipment Hardening]*

Defence in depth — Stacking complementary, independent security barriers so that the failure of one does not let an attacker reach the objective. *[ANSSI Secure Architecture: sensitive and RD systems; Defence in Depth & Secure Internet Gateway]*

Defense-in-depth — Layered controls so that one failure does not expose the asset. *[CEH v13: Core Concepts, Phases and Legal Framework; Secure Architecture Patterns +1]*

Defense in depth (layered security) — Several controls of different categories and types protect one asset, so a single failure is not a breach. Exam answer when 'one control failed': add a complementary layer, not a bigger version of the same control. *[Security Controls]*

defer — Schedules a call for when the surrounding function returns; deferred calls run last-in first-out, ideal for `Close()`, `Unlock()`, and `recover()`. *[Go Programming from Zero (Part 1: language basics)]*

Defined approach requirement — The numbered requirement (e.g. 8.3.6) plus its testing procedures (8.3.6.a/b) and guidance. What a ROC or SAQ tests by default. *[PCI DSS v4.0.1 Requirement by Requirement]*

Defined support period — the minimum time the manufacturer commits to shipping security updates, stated at the point of sale *[IoT and Medical Device Security]*

DEFR (Digital Evidence First Responder) — ISO/IEC 27037 role authorised and trained to act first at the scene to identify, collect and preserve digital evidence *[Digital Evidence and Chain of Custody]*

Degaussing — Exposing magnetic media to a strong magnetic field to erase it; useless on flash, and renders a modern HDD unusable. *[Malware, Servers and Media in Depth]*

Degraded recommendations (Rx-) — A recommendation suffixed with a dash (R7-, R8-, R9-, R10-, R18-, R21-) is a **tolerated fallback** used only when the nominal one cannot be met, typically for **uncontrolled clients** (public web browsers you cannot upgrade). R1 requires a documented client profile before applying any Rx-: e.g. a public website may... *[ANSSI TLS and IPsec Guides: Full R Index]*

Delegation (Kerberos) — Letting a service act on behalf of users: unconstrained, constrained, or resource-based (RBCD); any delegation towards DC services is a path to Tier 0. *[Active Directory Tier 0 Remediation]*

Deleted-but-open file — File unlinked from the directory tree but still held open by a process; its content stays readable through `/proc/<pid>/fd` until the process exits. *[Linux DFIR and Live Response]*

Deleted files (4.1.3) — Deleting marks the clusters as free; content stays until overwritten. Recoverable from the file system metadata or by carving. *[Forensics by Data Type]*

Denial of service — availability *[DevSecOps and Supply-Chain Security; CISSP Domain 1: Security and Risk Management +6]*

Denial of service → **availability** — rate limiting at gateway, DDoS protection, autoscaling *[Secure Architecture Patterns]*

Dependence / penetration — how much you rely on the stakeholder for your missions / how deeply it accesses your IS (accounts, links, data); high values raise exposure. *[EBIOS Risk Manager]*

Deployer — entity using an AI system under its authority in a professional context (AI Act term for the user organisation) *[Cyber Resilience Act and AI Act; AI Governance Programme]*

Deployment — Declares N identical replica Pods and manages rolling updates and rollbacks; the object you use for stateless apps. *[Kubernetes hands-on: learn it in your own lab]*

Deprecated — May be used to apply protection, but the user accepts a growing risk. *[NIST Cryptographic Standards]*

DER — Distinguished Encoding Rules: the raw binary ASN.1 (Abstract Syntax Notation One) form; one object per file, starts with byte 0x30. *[OpenSSL and Certificate Tooling]*

DES (Digital Evidence Specialist) — ISO/IEC 27037 role with deeper skills (analysis, specific technologies) who supports or takes over from the DEFR *[Digital Evidence and Chain of Custody]*

Deserialization — Rebuilding an object from bytes (Java, .NET, PHP, Python pickle); dangerous when the bytes come from the user. *[OWASP Top 10 2017 and Risk Rating]*

Design mitigations (4.2) — Least privilege, fail secure (deny on error) vs fail safe (life-safety: doors unlock), least functionality, defense-in-depth, code signing, encryption, indexing (tokenize/index sensitive fields instead of storing them in clear), allow listing, security design patterns. *[Security Operations]*

Design targets (voice/real-time) — Primary cell edge -67 dBm received signal (dBm = decibels relative to 1 mW; closer to 0 is stronger), SNR (signal-to-noise ratio) ≥ 25 dB, 15-20 % overlap for roaming, retries < 15 %, AP power no more than the weakest client can return (power symmetry). *[Wireless, Data-Center Fabrics and Cloud Networking]*

Desktop virtualization (4.4) — Users may create, copy and delete images, so policy compliance is hard. Managed images for teleworkers, clean image per remote session, or boot a hypervisor from removable media to bypass the host OS. Treat

images as appliances that expire. *[Cloud Outsourcing and Virtualization Lifecycle]*

Destroy — Media cannot be reused: shredding, disintegration, pulverizing, incineration, melting. *[NIST Security Operations Guides; Security Operations: Logs, Malware, Servers, Media]*

Detached HEAD — HEAD points straight at a commit instead of a branch; new commits are not on any branch and are easy to lose. Create a branch (git switch -c fix) to keep them. *[Essential Git Commands: a Working Reference]*

Detect 4625 — SIEM alert on failed-logon spikes *[Network and Authentication Attacks]*

Detecting cyber security events — monitoring, threat hunting *[NCSC, BSI and Allied Cyber Authorities]*

Detection — a rule plus its documentation, test data, response playbook and owner; a query alone is not a detection. *[SIEM and Detection Engineering]*

Detection & Analysis — precursors, indicators, triage, prioritization *[Incident Handling and Response]*

Detection-as-code — Rules stored in git with peer review, automated tests on sample events and CI deployment to the SIEM or EDR. *[Detection Rules: Sigma and YARA Catalogue; Detection Validation and Purple Teaming]*

Detection gap — an ATT&CK technique relevant to the threat model with no rule or no telemetry; tracked in the coverage matrix. *[SIEM and Detection Engineering]*

Detection risk — Risk that the auditor's own procedures fail to detect a material error. *[CISA Domain 1: Information System Auditing Process]*

Determination statement — Each control part is turned into assessable statements: AC-17a.[01] "usage restrictions are established and documented for each type of remote access"; each gets **satisfied (S)** or **other than satisfied (O)**. *[SP 800-53 Rev. 5 Security and Privacy Controls]*

Deterministic encryption — same plaintext and key always give the same ciphertext: allows equality search and joins, leaks frequency *[Privacy Engineering and PETs]*

Device-bound passkey — Private key generated in and never leaving one piece of hardware (security key, TPM, Microsoft Authenticator); lost device = lost credential. *[Passkeys and Passwordless Authentication]*

Device code phishing — attacker starts an OAuth device authorisation flow and sends the user the code with a pretext (Teams meeting invite); the user signs in and hands over tokens. Detect: sign-ins with authenticationProtocol = deviceCode;

mitigate: Conditional Access *authentication flows* policy blocking device code where not needed. *[Social Engineering and Deepfakes]*

Device fingerprinting — Active (-0, -sV, SNMP walk: reading a device's management data) or passive (p0f TCP/IP stack fingerprinting, Zeek, DHCP/OUI, NetFlow) identification of OS, firmware and role; drives which plugins the scanner runs. *[Vulnerability Scanning Methods]*

Device_ID — Unique identifier of a primitive, usually from the manufacturer (RFID for physical ones); can be modified or forged. *[Networks of Things SP 800-183]*

Device Manager Code 10 — Device cannot start: driver or hardware fault; update or roll back driver, reseal. *[Hardware Troubleshooting Playbook]*

Device placement — WAF (web application firewall) in front of the web tier; IPS (intrusion prevention system) inline right behind the edge firewall; IDS (intrusion detection system) on a tap or SPAN mirror port; load balancer in front of the server farm; VPN concentrator terminates in the screened subnet; jump server is the *only* path... *[Securing Enterprise Infrastructure]*

DevSecOps — Development and operations practice where security checks are automated inside the CI/CD (continuous integration / continuous deployment) pipeline instead of a gate at the end. *[Security Architecture - SDLC, IAM Design, Cloud]*

DFD (Data-Flow Diagram) — model of a system with four element types: external entities, processes, data stores and data flows, plus trust boundaries. *[Threat Modeling Methods]*

DFSR / NTFRS — Replication engines of SYSVOL (the share holding GPOs and logon scripts): DFSR is current, NTFRS is deprecated and must be retired. *[Active Directory Tier 0 Remediation]*

DGE — Direction generale des entreprises: ministry of economy directorate, co-author of the TPE/PME guide. *[Business Travel and SME Cybersecurity]*

DH (Diffie-Hellman) group — Numbered set of parameters for the key exchange that creates a shared secret over an open network. *[VPN and Firewall Security]*

DHCP — Dynamic Host Configuration Protocol: leases an IP address, mask, gateway and DNS servers to a client (UDP 67 server, 68 client). *[IP Addressing, ICMP, DHCP and Network Triage]*

DHCP relay — Router function (ip helper-address) that forwards client broadcasts as unicast to a DHCP server on another subnet. *[ICMP, Path MTU, DHCP and DNS Operations]*

DHCP snooping — Switch feature that drops DHCP server replies on untrusted ports and records MAC/IP/port bindings. *[Network Equipment Hardening]*

DiagTrack — Connected User Experiences and Telemetry service (Diagnostic Tracking Service) that uploads Windows diagnostic data to Microsoft. *[Windows Privacy GPOs and VBS Deployment]*

Diamond Model — Intrusion analysis model linking adversary, capability, infrastructure and victim for each event. *[CEH v13: Exam Blueprint and Module Map]*

DIC — French acronym for Disponibilit , Int grit , Confidentialit : the availability, integrity and confidentiality needs of a resource (CIA). *[ANSSI Zero Trust Model]*

DICE — TCG Device Identifier Composition Engine: for chips too small for a TPM; a Unique Device Secret mixed with the hash of the first mutable code gives a per-firmware identity (CDI = Compound Device Identifier). Changed firmware = changed key. *[Hardware Roots of Trust and the TPM 2.0]*

Differential privacy — A randomised algorithm M is **epsilon-differentially private** if, for any two datasets that differ in one person's data, the probability of any output changes by at most a factor e^{ϵ} . Whatever an attacker already knows, the output reveals almost the same about you whether or not you are in the data. Introduced... *[Privacy Engineering and PETs]*

Differential result — osquery logs only rows that were *added* or *removed* since the previous run of a scheduled query, which keeps log volume small. *[osquery and Velociraptor for Fleet Visibility]*

DiffServ (Differentiated Services) — Scalable QoS model (RFC 2474/2475): packets are marked with a DSCP class at the edge; each router applies a per-hop behaviour (PHB) to the class, with no per-flow state. *[QoS, Multicast and WAN Services]*

Diffusion Restreinte (DR) — French protective marking for sensitive but unclassified information (roughly 'restricted'); DR systems need a homologation and qualified products. *[ANSSI Encryption Tools: Zed! and Cryhod (1/2, Zed!)]*

Digest — SHA-256 hash of an image manifest; the only immutable way to name an image. *[Container Image and Registry Security]*

Digital certificate — An X.509 document binding a subject name (e.g. www.example.com) to a public key, with a validity period, a serial number and the issuer's digital signature. Anyone who trusts the issuer can trust the binding. *[PKI and Certificates]*

Digital evidence — information stored or transmitted in binary form that may be relied on in a legal, disciplinary, regulatory or insurance proceeding *[Digital Evidence and Chain of Custody]*

Digital forensics — Application of science to identify, collect, examine and analyse data while preserving its integrity and a strict chain of custody (SP 800-86 definition). *[Digital Forensics in Incident Response]*

Digital risk — any risk to the organisation's missions arising from its use of digital technology, from cyberattack to IT failure; treated as a business risk. *[Digital Risk Governance - ANSSI-AMRAE 15 Steps]*

Digital signature — Hash signed with the sender's private key; gives integrity, authentication and non-repudiation. *[CISA Domain 5: Protection of Information Assets; Fundamental Security Concepts +1]*

DINUM — interministerial digital directorate that implements the *cloud au centre* doctrine for State IS. *[Cloud Hosting for Sensitive Systems]*

Diode — Device physically able to pass data in one direction only (e.g. fibre with a single transmitter), so nothing can flow back. *[Multi-Environment Workstation and Refurbishing; Multilevel Interconnections & Trusted Core]*

Direct / indirect — Direct = network link through security devices. Indirect = removable media carried between a data extraction point (PED, point d'extraction de donn es) and a data insertion point (PID, point d'insertion de donn es). *[Multi-level Interconnections & Trusted Core]*

Direct PPE (D-PPE) — The attacker modifies the pipeline definition file itself (workflow YAML, .gitlab-ci.yml) in a branch or pull request that the CI then runs. *[CI/CD Pipeline Security]*

Direct prompt injection — The user types instructions that override the system prompt (jailbreak). *[OWASP LLM Top 10 v1.1 (2023) and the 2025 Shift]*

DIREX — Director of the exercise: validates the guidelines and every stage of preparation; may lead the exercise. *[Organising a Cyber Crisis Management Exercise]*

DISA — Direct inward system access: an outside caller reaches internal features (e.g. outgoing lines) of the PBX, a classic toll-fraud path. *[ToIP and Virtualization Security]*

Disallowed — No longer allowed to apply cryptographic protection. *[NIST Cryptographic Standards]*

Disaster — A disruption that exceeds normal incident handling and triggers the BCP or DRP. *[CISM Domain 4: Incident Management]*

Disclosure-deadline extortion — Actors weaponise reporting obligations (SEC 4-business-day rule, NIS2 24 h early warning) to pressure victims before the regulator is told. *[Breach and Threat Landscape 2024]*

Discoverable credential — Credential stored with the user handle on the authenticator, so login needs no username first (formerly 'resident key'). *[Passkeys and Passwordless Authentication]*

Discovery sampling — Attribute variant sized to find at least one instance when the expected rate is very low, e.g. fraud. *[CISA Domain 1: Information System Auditing Process]*

Discretion posture — Level of secrecy chosen for the response (low, medium, high) to limit what the attacker can learn from it. *[Preparing Cyber Remediation]*

Disruption / chaos — Attack for the thrill or notoriety, no strategic objective. *[Threat Actors and Threat Vectors]*

Dissector — decoder for one protocol; Decode As forces a dissector on a non-standard port (HTTP on 8081, TLS on 8443). *[Wireshark and tshark for Troubleshooting and Analysis]*

distinct media — disk + tape, or on-prem + object storage *[IT Backup - ANSSI BP-100 R1-R32]*

Distractor — A wrong option written to look plausible, often a true statement that does not answer the qualifier. *[CISA Practice Scenarios]*

Distributed anycast gateway — Same gateway IP and MAC on every leaf, so a VM keeps its gateway after moving; symmetric IRB (integrated routing and bridging) routes between VNIs (VXLAN network identifiers) through an L3VNI per VRF. *[Wireless, Data-Center Fabrics and Cloud Networking]*

Distribution tier — Aggregates access switches, performs inter-VLAN routing, applies ACLs and QoS, and hosts the default gateway via a First-Hop Redundancy Protocol (FHRP: HSRP/VRRP). This is where Layer 2 becomes Layer 3. *[Classic Enterprise Network Architecture]*

Diverse data sources — Third-party reports and logs, threat intelligence feeds, vulnerability scans, CVE details, bounty pro-

- grams, DLP data, endpoint logs, infrastructure device logs, application logs, CSPM data. **[Security Operations]**
- DKIM** — DomainKeys Identified Mail: the sending server signs each message; the public key is in DNS. **[CISSP Domain 4: Communication and Network Security; Social Engineering and Deepfakes +2]**
- DLP** — Tools that discover, monitor and block sensitive data in use, in motion and at rest. **[CISA Domain 5: Protection of Information Assets; CompTIA CySA+ CS0-003]**
- DLP (Data Loss Prevention)** — controls that detect or block sensitive data leaving through email, web, USB, print or cloud apps. **[Data Protection: Classification, Leaks, GDPR; Insider Threat Program]**
- DLP policy** — Rule that detects sensitive information types (card numbers, national IDs) in content and warns, blocks or audits sharing. **[Microsoft 365 Hardening]**
- DMA attack** — A bus-mastering device (Thunderbolt, PCIe, FireWire) reads or writes RAM directly, bypassing the CPU and OS. **[Platform Firmware, BMC, DMA and USB Attacks]**
- DMARC** — Domain policy telling receivers what to do when SPF/DKIM fail and align (none, quarantine, reject), with aggregate reports (rua). **[CISSP Domain 4: Communication and Network Security; Social Engineering and Deepfakes +2]**
- DMZ** — Demilitarised zone: network segment between the external and internal firewalls hosting exposed servers and relays. **[Firewall Policy: Design, Cleanup, Exposed Zone]**
- DMZ (demilitarised zone)** — A screened subnet between the Internet and the internal network that holds services reachable from outside; a compromise there does not directly reach the LAN. **[Classic Enterprise Network Architecture]**
- DMZ (demilitarized zone)** — Screened subnet between internet and internal network that hosts the public-facing servers. **[VPN and Firewall Security]**
- DMZ (screened subnet)** — Enterprise: separate segment for public servers between two firewalls. SOHO 'DMZ host' forwards every unsolicited port to one device: exposes it completely. **[CompTIA A+ Core 1 - Networking, SOHO, Network Troubleshooting]**
- DNP3 / Modbus** — Multilayer ICS protocols without native authentication; DNP3 Secure Authentication adds it. **[CISSP Domain 4: Communication and Network Security]**
- DNS-PRIV / DNS-PUB / DNS-HEB** — The guide's three services: resolution of internal names, resolution of Internet names for internal systems, hosting of the entity's Internet domains. **[DNS, Wi-Fi & DDoS Architectures]**
- DNS sinkhole** — Resolver answer that points a malicious domain to an internal address, blocking the connection and revealing which hosts asked. **[SecurityX Discriminator Pairs and Gap Closers]**
- DNSSEC** — DNS security extensions: zones are signed (RRSIG records) so a validating resolver can check integrity and origin of answers along a chain of trust from the root. **[DNS, Wi-Fi & DDoS Architectures]**
- DNSSEC services (8.9.2)** — 1. proof of origin, 2. public key distribution, 3. transaction and request authentication. Each RRSet is signed (RRSIG, formerly SIG); keys published as DNSKEY (formerly KEY); DS links parent and child. **[Network Security II - Authentication, Email, Web]**
- dnstap** — Structured binary log format (protocol buffers over Frame Streams) for DNS messages, emitted by the server without parsing text logs. **[DNS Infrastructure Operations]**
- DOC / SMC** — Document of Compliance (company) and Safety Management Certificate (ship), issued after ISM audits; the DOC audit is where cyber risk is checked. **[Cyber Security On Board Ships]**
- Docker daemon (dockerd)** — Root service that builds images and starts containers; the docker CLI only sends it API calls over `/var/run/docker.sock`. **[Docker and Containers Hands-On]**
- DoD 8140** — US Department of Defense cyber workforce qualification framework that replaced DoD 8570; lists accepted certifications per work role. **[Security Certification Landscape]**
- DoD Assessment Methodology (SPRS score)** — Start at 110; subtract 5, 3 or 1 point per unmet Rev. 2 requirement (MFA and FIPS crypto are 5-point items); range -**203 to 110**. Score, date and POA&M completion date go into SPRS (DFARS 7019/7020). **[SP 800-171 Rev. 3, CUI and CMMC 2.0]**
- DoH / DoT** — DNS over HTTPS / DNS over TLS: encrypts name lookups against eavesdropping and tampering. **[CISA Zero Trust Maturity Model v2.0]**
- DoIP (ISO 13400)** — Diagnostics over IP: UDS carried over automotive Ethernet, port 13400 TCP/UDP; enables fast flashing and remote diagnostics. **[Automotive and Embedded Security]**
- Domain** — A replication and policy boundary inside a forest, with its own accounts and domain controllers; it is NOT a security boundary against a forest-wide attacker. **[On-Prem Active Directory Architecture; Windows Administration and Active Directory Basics]**
- Domain controller (DC)** — Server running AD DS: stores the directory, answers LDAP and Kerberos, applies replication; tier 0, protect it like the crown jewels. **[Windows Administration and Active Directory Basics]**
- Domain / project** — Keystone domain = one client and its users/groups; project (ex-tenant, since Grizzly 2013) = a resource container inside a domain. **[OpenStack and Virtualisation Security]**
- Domain restricted sharing** — Org policy `iam.allowedPolicyMemberDomains` limiting IAM members to your own Cloud Identity customer IDs. **[GCP Security Essentials]**
- Domain transition** — Change of SELinux process type when a confined program is executed, e.g. `systemd (init_t)` starts `/usr/sbin/httpd` which then runs as `httpd_t`. **[Linux Hardening in Practice]**
- DORA** — Discover, Offer, Request, Acknowledge: the four DHCP messages by which a client leases an IPv4 address. **[IT Usage Charter and Outsourcing Security; Protocol Walk-Throughs at Packet Level]**
- DORA (Digital Operational Resilience Act)** — EU Regulation 2022/2554: ICT risk, incident reporting, resilience testing and third-party oversight for financial entities. **[ENISA ETL 2024, DoD Zero Trust, ATT&CK for ICS]**
- DORA exit plan** — EU Digital Operational Resilience Act (applies from 17 Jan 2025): financial entities must keep documented, tested exit strategies for critical ICT providers. **[Cloud Outsourcing and Virtualization Lifecycle]**
- Dossier d'homologation** — accreditation dossier: the evidence file (risk analysis, architecture, gaps, compensating measures) the authority reads before deciding. **[Protecting Essential IS - PA-085 R1 to R62]**
- Double extortion** — Data exfiltrated before encryption; publication threatened even if backups allow recovery. **[Ransomware: Anatomy, Detection, Prevention; Threat Actor Profiles +1]**
- Downward interconnection (descendante)** — Data goes high → low. Essential service: **transfer authorisation control** (R12). Risk: confidentiality; unidirectionality alone does not prevent exfiltration. **[Multilevel Interconnections & Trusted Core]**
- Doxing** — Collecting and publishing personal information about an individual. **[CEH v13: Core Concepts, Phases and Legal Framework]**

DPA — Data Protection Authority: the national GDPR regulator (CNIL in France, ICO in the UK) that receives Art. 33 notifications. *[Reporting and Communication]*

DPA (authority) — Data protection authority (CNIL in France) receiving GDPR Art. 33 breach notifications; not to be confused with a data processing agreement. *[EU Governance and Regulation: Self-Assessment]*

DPD — Dead Peer Detection: periodic encrypted probes that close an IKE tunnel whose peer stopped answering. *[Stormshield SNS 3.7.17 Hardening by Chapter]*

DPD (dead peer detection) — IKE liveness probe: if the peer stops answering, its SAs are deleted and the tunnel is rebuilt. *[VPN Planning, Design and Operations]*

DPI (deep packet inspection) — Inspection of the payload, not only headers, to identify applications and attacks. *[VPN and Firewall Security]*

DPIA — Data protection impact assessment required before high-risk processing of personal data (GDPR Art. 35). *[CRISC Domain 4: Information Technology and Security]*

DPO — Data protection officer: GDPR role that monitors compliance and advises, independent of instructions. *[CISSP Domain 2: Asset Security]*

DPO / DPIA — Data protection officer / data protection impact assessment (GDPR Art. 37 and 35). *[Local Authorities: the Regulatory Security Framework]*

DPoP / mTLS binding — Demonstrating Proof of Possession (RFC 9449) / mutual-TLS certificate binding (RFC 8705): a stolen token is useless without the client's private key. *[Identity Protocols: OAuth, OIDC, SAML, FIDO2]*

DR / BDR — Designated Router / Backup DR, elected on broadcast and NBMA segments to cut adjacencies from $n(n-1)/2$ to about $2n$. Highest `ip ospf priority` (default 1, 0 = never) then highest RID. **Non-preemptive**: a better router joining later does not take over until the DR fails or `clear ip ospf process`. *[Routing I: Routing Table, Static Routes, OSPF]*

DR (Diffusion Restreinte) — French 'restricted distribution' marking, the level just below classified information; NP (non protégé) = unmarked. *[Multi-Environment Workstation and Refurbishing; Firewall Policy: Design, Cleanup, Exposed Zone]*

DRAM LED — seating, slot order, training, XMP/EXPO off *[Hardware Troubleshooting Playbook]*

DRBG — Deterministic random bit generator: the algorithmic post-processing that expands seeded entropy into random output. *[ANSSI Cryptographic Mechanisms and PQC]*

DRBG / RBG — (Deterministic) random bit generator: algorithm that expands a seed from an entropy source into unpredictable bits for keys, IVs and nonces (SP 800-90A/B/C). *[Crypto Mechanisms, Key Policy and AES Internals]*

Drift — Difference between the deployed cloud configuration and what the IaC code declares, caused by manual or external changes. *[Infrastructure as Code and Secrets; GitOps and Continuous Delivery Security]*

Driver — Kernel code that knows how to talk to one kind of device; it runs with full kernel privileges. *[Operating System Concepts for Beginners]*

DRP (disaster recovery plan) — Restores IT systems and data after a disruption; a subset of continuity. *[CISSP Domain 7: Security Operations]*

DRP (PRA) — Disaster Recovery Plan (plan de reprise d'activité): procedures to restore IT and resume activity after the incident, relying on healthy (offline, tested) backups. *[Cyber Crisis Management & Communication]*

DRTM — Dynamic Root of Trust for Measurement: CPU instruction (Intel TXT, AMD SKINIT) that restarts measurement from a clean state after firmware, so firmware is less trusted. *[OpenSSH Hardening and Hardware Security; Hardware Roots of Trust and the TPM 2.0]*

Dry run — mode that prints what a command would do without changing anything (`rsync -n`, `apt-get -s`, `kubectl --dry-run`, `PowerShell -WhatIf`). *[Master Any Command-Line Program Fast, on Every OS]*

DSA = ML-DSA (FIPS 204) — lattice signatures - replaces ECDSA/RSA *[Cryptography Engineering and PQC]*

DSC — Display Stream Compression: visually lossless link compression enabling 4K144+ on DP 1.4. *[Power, Displays, Peripherals and Printers]*

dSHeuristics — Forest-wide attribute of configuration flags (anonymous LDAP, adminSDHolder exclusions); some values weaken the whole directory. *[Active Directory Tier 0 Remediation]*

DSP — Delegation de service public: a public service (water, transport) run by a private delegate under contract. *[Start-ups, Municipalities, Teleassistance, Open Source]*

DSRM — Directory Services Restore Mode: local emergency administrator of each DC, used to repair AD offline; a known

DSRM password is a backdoor. *[Active Directory Tier 0 Remediation]*

DSSE — Dead Simple Signing Envelope: wraps a payload with its type and signatures so the signed bytes are unambiguous. *[Software Supply Chain Security]*

DTO — Data Transfer Object: a class listing exactly the fields an endpoint accepts or returns. *[OWASP API Security Top 10 - 2023]*

DTP — Dynamic Trunking Protocol: Cisco negotiation of trunking; disable with `switchport nonegotiate` or access mode. *[Cisco IOS Configuration Lab]*

Dual-use tool — Software usable both for defence and attack (Nmap, Metasploit, Mimikatz, password crackers); lawful to hold for a legitimate purpose in most EU laws. *[Law and Ethics for Security Practitioners]*

Ductile metals — combustible metals (sodium, magnesium) *[CompTIA A+ Core 2 - Threats, Security Symptoms, Safety]*

Due care — Acting as a prudent person would: implementing reasonable controls. *[CISM Domain 1: Information Security Governance; Compliance, Audits and Security Awareness]*

Due care vs due diligence — **Due diligence** is investigating and planning (know the risk, assess vendors); **due care** is doing the right thing continuously (implement and operate the controls). Negligence is the absence of due care. *[CISSP Exam Strategy]*

Due diligence — Investigating and verifying that controls and third parties actually meet expectations. *[CISM Domain 1: Information Security Governance; Compliance, Audits and Security Awareness]*

Due diligence (vendor selection) — Investigation before signing: financial health, ownership, sanctions screening, security evidence above, references, exit plan. *[Governance, Risk and Third-Party Management]*

Due diligence vs due care — Diligence = investigating and knowing (risk assessment, vendor review); care = acting on it reasonably (implementing controls). Negligence claims target missing due care. *[Compliance, Threat Modeling and AI Security]*

Due professional care — Diligence and skill a prudent, competent auditor would apply; not infallibility. *[CISA Domain 1: Information System Auditing Process]*

Duress code — Silent signal (word, PIN) a person under threat uses to alert security without the attacker noticing. *[CISSP Domain 7: Security Operations]*

Dwell ten days — median 2023 (M-Trends 2024) *[Edge, Readiness and Awareness Reports]*

Dwell time — days between initial compromise and detection; hunting exists to shorten it for what alerts miss. *[Threat Hunting Playbooks; Ransomware Defense End to End +2]*

Dynamic analysis — running the sample in an instrumented, isolated sandbox and recording what it does (processes, files, registry, network). *[Malware Triage and Analysis]*

Dynamic ARP Inspection (DAI) — Drops ARP packets whose MAC/IP pair contradicts the DHCP snooping binding table. *[Network Equipment Hardening]*

Dynamic linker — User-space loader that maps shared libraries and resolves symbols: `ld-linux-x86-64.so.2` on Linux (named in `PT_INTERP`), `ntdll!Ldr*` routines on Windows. *[Executable Formats: ELF and PE]*

Dynamic policy — identity + asset + context *[Zero Trust Architecture SP 800-207]*

E

E-discovery — Identification, collection, review and production of electronically stored information for legal proceedings (Purview eDiscovery, Relativity); driven by counsel, not the SOC (security operations centre). *[Incident Response, Forensics, Automation]*

E-discovery vs forensics — E-discovery = producing relevant records for litigation; forensics = reconstructing events with evidentiary integrity. Legal hold suspends normal retention. *[NIST IR, Forensics, and Exercises]*

EAA / QEAA / PuB-EAA — electronic attestations of attributes (diplomas, driving licence, professional qualifications, account ownership); **qualified** when issued by a QTSP, or issued by or for a public-sector body responsible for an authentic source *[eIDAS 2 and the EU Digital Identity Wallet]*

EAL — Evaluation Assurance Level of the Common Criteria (ISO/IEC 15408), from EAL1 to EAL7; '+' means augmented. *[Local Authorities: the Regulatory Security Framework]*

EAP (Extensible Authentication Protocol) — Framework carrying the actual authentication method (EAP-TLS certificates, PEAP passwords) between supplicant and RADIUS server; the switch only relays it. *[First-Hop Security and Gateway Redundancy]*

EAP-FAST / PEAP — Flexible Authentication via Secure Tunneling (Cisco, PAC-based tunnel) and Protected EAP (TLS tunnel, usually MSCHAPv2 inside) - both need server-

certificate validation to stop evil-twin credential capture. *[CompTIA SecurityX CAS-005 - Exam Overview]*

EAP-TLS — 802.1X method where client and server authenticate each other with X.509 certificates. *[Network Equipment Hardening]*

EAPOL — EAP over LAN (IEEE 802.1X): frame format (Ethernet 0x888E) carrying EAP between client and authenticator, and the EAPOL-Key frames of the 4-way handshake. *[Wi-Fi Security Internals]*

Early warning — NIS2 Art. 23(4)(a) first notice to the CSIRT within 24 h of awareness of a significant incident. *[NIS2 Directive: EU-wide Obligations]*

Earned value — Compares planned value, earned value and actual cost to measure schedule and cost variance. *[CISA Domain 3: IS Acquisition, Development and Implementation]*

EAST — UK Behavioural Insights Team checklist: make it Easy, Attractive, Social (others do it) and Timely (at the moment of risk) *[Security Awareness and Culture Programme]*

East-west traffic — Server-to-server traffic inside the data centre (e.g. app to database); now the dominant volume, unlike north-south (in/out of the DC). *[Data-Centre Architecture; Secure Enterprise Network Landscape SP 800-215]*

EBIOS Risk Manager — EBIOS = Expression des Besoins et Identification des Objectifs de Sécurité (expression of needs and identification of security objectives). ANSSI's digital risk management method (2018, updated v1.5 Sept. 2024, republished in the Jan. 2025 collection). Scenario-based: it studies **intentional** digital risks as... *[EBIOS Risk Manager]*

eBPF — extended Berkeley Packet Filter: sandboxed programs loaded into the Linux kernel to observe syscalls and network events with low overhead. *[Linux and Cloud Logging; Kubernetes and Container Networking Explained]*

eBPF program — Bytecode for a 64-bit virtual machine with 11 registers (R0-R10) and a 512-byte stack, loaded with the `bpf()` system call and attached to a hook. *[eBPF in Depth]*

EC-Council — Commercial training body that issues CEH, CHFI, CPENT and related certifications. *[Security Certification Landscape]*

ECCG — European Cybersecurity Certification Group: the national certification authorities, advising on schemes; the Stakeholder Cybersecurity Certification Group (SCCG) represents industry. *[ENISA, NIS2 and the EU Threat Landscape]*

ECDHE / DHE — Ephemeral Diffie-Hellman on elliptic curves / on finite-field (MODP) groups; the E means a fresh key per session. *[TLS, IPsec and SSH Hardening]*

ECDIS — Electronic Chart Display and Information System: the bridge workstation that replaces paper charts. *[Cyber Security On Board Ships]*

ECDIS malware — Chart updates arrive on USB; an infected update compromises the navigation workstation. Dedicated update station with antivirus, ECDIS isolated from business IT (guide I-3, II-6). *[Cyber Security On Board Ships]*

ECE — ECN-Echo: receiver saw a congestion mark (or ECN capable, in a SYN) *[TCP and UDP Deep Dive]*

ECMP — Equal-Cost Multi-Path: a router installs several next hops for one prefix and picks one per flow by hashing packet header fields, so all links carry traffic. *[Overlay, Data-Centre and Cloud Network Internals]*

ECMP (Equal-Cost Multi-Path) — Routing that spreads flows across all equal-cost leaf-spine links, so nothing is blocked and bandwidth is the sum of the links. *[Data-Centre Architecture]*

Economy of mechanism — Keep designs small and simple enough to review *[OWASP Developer Guide v4.2 - Chapter by Chapter]*

Ecosystem — all stakeholders interacting with the studied object: suppliers, IT providers, partners, subsidiaries, customers, regulators. *[EBIOS Risk Manager]*

eCrime — financially motivated criminal activity (ransomware, data theft for extortion), as opposed to state-nexus espionage. *[Breach and Threat Landscape 2024; Vendor Threat Reports: Identity, Endpoint, IR]*

ECS / OCSF — Elastic Common Schema / Open Cybersecurity Schema Framework: field naming standards used to normalise logs from different sources. *[ANSSI Logging and Security Supervision]*

ECSF (European Cybersecurity Skills Framework) — ENISA framework published in 2022 describing 12 role profiles (mission, tasks, skills, knowledge, deliverables) mapped to the e-CF competence framework; used by EU employers and training programmes *[Career Map of Cyber Security Roles]*

ECU (electronic control unit) — An embedded computer controlling one vehicle function, usually a microcontroller with its own firmware and network interfaces. *[Automotive and Embedded Security]*

Edge device — Internet-facing appliance at the network boundary: VPN concentrator, firewall, load balancer, file-transfer or email gateway; often without EDR (endpoint detection and response) agents. **[Security Outlook 2026]**

eDiscovery — Identifying, preserving and producing electronic records for litigation (EDRM model); starts with a legal hold. **[CISSP Domain 7: Security Operations]**

EDL (elements de langage) — Validated sentences on a topic that every spokesperson reuses word for word, reactive (answers) or proactive (statements). **[Cyber Crisis Communication]**

EDNS0 — Extension Mechanisms for DNS (RFC 6891): an OPT pseudo-record in the additional section that advertises a larger UDP payload size and carries the DO (DNSSEC OK) bit. **[Protocol Walk-Throughs at Packet Level]**

EDR — Endpoint detection and response agent: records process, file, network and registry telemetry on each host and can isolate it. **[ANSSI Endpoint Security: Overview and Windows; Digital Forensics in Incident Response]**

EDR / NDR — Endpoint / Network Detection and Response: sensors that both detect on their own and forward rich telemetry to the SIEM; the SIEM correlates across them. **[Security Operations Architecture]**

EDR / SIEM / SOC — Endpoint detection and response agent; security information and event management platform; security operations centre that runs them. **[ANSSI Zero Trust Model]**

EDR / XDR — Endpoint Detection and Response / Extended Detection and Response (endpoint plus network, identity, cloud telemetry). **[SIEM and Detection Engineering; Security Tools and Techniques +1]**

EEL — Essential Elements of Information: the concrete facts that answer a PIR (initial access vectors used, exploited CVEs, negotiation behaviour). **[Cyber Threat Intelligence Lifecycle]**

Effective permissions — What an identity can really do once every allow, deny, boundary, organisation guardrail and condition is evaluated. **[Cloud Entitlement Management and Least Privilege]**

Effective set (CapEff) — Capabilities the kernel checks now; must be a subset of the permitted set (CapPrm). **[Linux Isolation Primitives and Sandboxes]**

Effective UID (EUID) — The user id the kernel uses for permission checks; differs from the real UID while a setuid program runs. **[Linux Users, Groups, Permissions and ACLs]**

Egress filtering — Filtering of outbound traffic, such as dropping packets whose source address is not the organization's. **[Firewall Policy and IDPS Deployment]**

eIDAS — EU Regulation 910/2014 on electronic identification and trust services (signature, seal, time stamp, registered delivery, website certificates). **[Local Authorities: the Regulatory Security Framework]**

ELAM (Early Launch Anti-Malware) — Signed driver loaded first at boot that classifies later boot drivers and whose certificate lets the vendor's service run as PPL anti-malware. **[EDR Telemetry, Tamper and Evasion Detection]**

Electoral board (bureau electoral) — Body that supervises the election, holds the key shares and must be able to check integrity itself. **[Internet Voting for Non-Political Elections]**

Electronic seal — Signature-like data created by a legal person (a company) to prove origin and integrity of a document, not consent of a human. **[eIDAS 2 and the EU Digital Identity Wallet]**

Elevation of priv — authorization **[CompTIA PenTest+ PT0-003]**

Elevation of privilege — authorisation **[DevSecOps and Supply-Chain Security; CISSP Domain 1: Security and Risk Management +5]**

Elevation of privilege → authorisation — least privilege, PAM, admission control, sandboxing **[Secure Architecture Patterns]**

ELF (Executable and Linkable Format) — Unix object format for executables, shared libraries (.so), object files (.o) and core dumps; starts with bytes 7F 45 4C 46 (\x7fELF). **[Executable Formats: ELF and PE]**

Eliminate extremes — drop options that remove all risk, bypass the owner or buy technology first **[CRISC Practice Scenarios]**

Email still delivers — 88% of malicious files (Check Point) **[Edge, Readiness and Awareness Reports]**

Emargement — Signing the voters' register: the record that a given voter has voted, kept separate from the ballot. **[Internet Voting for Non-Political Elections]**

eMASS — Enterprise Mission Assurance Support Service: DoD system of record where RMF packages, checklists and POA&Ms (plans of action and milestones) are uploaded. **[DISA STIG Viewer 3 and STIG Checklists]**

Embedding — Numeric vector representing a text's meaning, stored in a vector database for retrieval. **[ANSSI Generative AI Security; AI Fundamentals for Cybersecurity +1]**

Emergence (D.2) — Security is an emergent property of the whole system: secure elements can compose into an insecure system, hence Compositional Trustworthiness (E.7). **[Engineering Trustworthy Secure Systems]**

Emerging risk — New or changing risk whose likelihood and impact are not yet well understood (AI adoption, quantum threat to cryptography, new regulation). **[CRISC Domain 3: Risk Response and Reporting]**

Employer liability — Liable for employees' acts with provided tools; decryption is legitimate only if framed (transparency, necessity and proportionality, controlled access to keys). **[HTTPS Flow Inspection: Proxy and Reverse Proxy]**

Encapsulation — Each layer adds its header (and sometimes trailer) around the data from the layer above. **[CISSP Domain 4: Communication and Network Security; Network Models, Performance and the Physical Layer]**

Enclave — process-level TEE (Intel SGX): a protected region inside one application's address space **[Confidential Computing and Remote Attestation]**

Enclave / TEE (Trusted Execution Environment) — a CPU-and-memory-only isolated context whose DRAM is encrypted with keys held in hardware and unavailable to any software, even at the highest privilege. Code confidentiality is **not** guaranteed: the CPU executes the workload unencrypted. **[Confidential Computing]**

Encrypt + compress — 7z AES-256 or GPG before exfil - smaller, evades content inspection; split large files. **[Post-Exploitation and Lateral Movement]**

Encryption — Reversible with the key; protects confidentiality. The work is key management: HSM (hardware security module) or KMS (key management service), rotation, keys stored apart from the data. **[Data Protection and Resilience]**

Encryption at rest — AES-256 with KMS-managed keys for datasets, weights, checkpoints, embeddings, prompt logs; separate keys per tenant or classification. **[Securing AI Systems]**

Encryption in transit — TLS 1.2+ (prefer 1.3) on every hop: client to gateway, gateway to model, model to tools and vector store; mTLS between internal services. **[Securing AI Systems]**

Encryption in use — Confidential computing: TEEs (trusted execution environments: hardware-encrypted memory with attestation) such as AMD SEV-SNP, Intel TDX/SGX, NVIDIA H100 confidential mode; plus homomorphic encryption and se-

cure multi-party computation for narrow cases. *[Securing AI Systems]*

Encryption system components — data, encryption engine, key management; design decides where each sits, starting from a threat model. *[CSA Security Guidance v4: the 14 Domains]*

End-entity (leaf) certificate — The certificate issued to the actual subject (a website, user or device); it cannot sign other certificates (basicConstraints CA:FALSE). *[PKI and Certificate Architecture]*

End-user computing (EUC) — Applications built by business users (spreadsheets, low-code) that may feed critical reports without IT controls. *[CISA Domain 4: IS Operations and Business Resilience]*

Endorsement — ISC2 step after passing: a certified member attests the candidate's experience and ethics before the credential is awarded. *[Security Certification Landscape]*

Endorsement key — Unique, manufacturer-certified TPM key that identifies the chip; decrypt-only. *[Hardware Roots of Trust and the TPM 2.0]*

Enforce lints — go vet, staticcheck, gosec in CI *[Go for Security Tooling and Safe Code]*

Engagement letter — Per-assignment document (often for external audits) confirming scope, objectives, responsibilities and access. *[CISA Domain 1: Information System Auditing Process]*

Engine (PE) — grant/deny/revoke decision via the trust algorithm *[Security Architecture - Resilience, Controls, Zero Trust]*

Engineering security — (e) acquisition, development, vulnerability disclosure *[NIS2 Directive: EU-wide Obligations]*

Engineering Workstation (EWS) — Machine that programs PLCs/DCS; a top-value target because it can rewrite controller logic. Kept in OT, tightly locked down. *[Industrial (OT/ICS) Architecture]*

Enhanced supervision (supervision renforcee) — Incident-dedicated monitoring: extra signatures and configurations, additional sensors, higher vigilance on the compromised perimeter. Some measures are kept after resolution to detect a re-suspension. *[Incident Qualification & Remediation Decision Keys]*

Enhancement — Adds functionality or rigor: IA-2(1) MFA to privileged accounts, IA-2(2) MFA to non-privileged. Never used without its base control. *[SP 800-53 Rev. 5 Security and Privacy Controls]*

Enterprise Access Model — Microsoft's successor to the tier model: it maps privileged access into control, management and data/user planes and is enforced with Privileged Access Workstations (PAWs). *[On-Prem Active Directory Architecture]*

Enterprise architecture — Documented current and target state of business, data, application and technology layers (Zachman, TOGAF) used to steer investment. *[CISA Domain 2: Governance and Management of IT]*

Enterprise browser — browser (or managed profile) with built-in policy, DLP and identity controls, e.g. Island, Prisma Access Browser, Chrome Enterprise Premium, Edge for Business *[Browser and Extension Security]*

Enterprise risk management (ERM) — Enterprise-wide process that identifies, assesses and manages all risk types (strategic, financial, operational, IT, compliance) in one consistent way against objectives. *[CRISC Domain 1: Governance]*

Enticement — Making an attractive target available (honeypot) to an attacker already intent on intruding; legal. *[CISSP Domain 7: Security Operations]*

Entite responsible — the responsible entity: the organisation that owns or operates the industrial system and accepts its risks. *[ANSSI ICS Detailed Measures v2 (1/2): organisation and accounts]*

Entitlement — A permission an identity holds on a resource, directly or through group, role, policy or inheritance. *[Cloud Entitlement Management and Least Privilege; iOS Application Internals and Security]*

Entitlement review — Periodic recertification in which owners confirm or revoke each user's access. *[CISSP Domain 5: Identity and Access Management]*

Entra Connect — The server that synchronises accounts (and optionally password hashes) from AD to Entra ID; protect it as Tier 0 because it bridges both directories. *[On-Prem Active Directory Architecture]*

Entra Connect (AD Connect) — Service synchronising on-premises AD with Microsoft Entra ID (Azure AD); its MSOL service account can read password hashes, hence Tier 0. *[Active Directory Tier 0 Remediation]*

Entra ID (formerly Azure AD) — Microsoft's cloud identity and access service; it is not a cloud domain controller and does not use OUs/GPO, but federates and syncs with on-prem AD. *[On-Prem Active Directory Architecture]*

Entrapment — Inducing someone to commit a crime they did not intend; illegal and makes evidence unusable. *[CISSP Domain 7: Security Operations]*

Entropy — randomness of bytes on a 0-8 scale (bits per byte); plain code sits around 5-6.5, compressed or encrypted data near 8. *[Malware Triage and Analysis]*

Envelope encryption — Encrypting data with a data key, then encrypting that data key with a master key held in a KMS or HSM. *[Storage and Filesystems for Defenders]*

Envelope From (MAIL FROM, Return-Path, RFC5321.MailFrom) — Bounce address seen by MTAs only; SPF checks this domain (and HELO). *[Email Security: SPF, DKIM, DMARC]*

Envelope sender (RFC5321.MailFrom) — Address given in the SMTP MAIL FROM command; bounces go there, SPF checks its domain, and it is copied into the Return-Path: header on delivery. *[Phishing Analysis and E-mail Header Forensics]*

Environment — The universe the primitives operate in: the NoT's operational profile (weather for an aircraft, a specific factory floor); gives context to sensors and aggregators. *[Networks of Things SP 800-183]*

Environmental impacts — high energy, water and compute use for training and running models. *[AI Risk Management Program Design]*

Environmental metrics — Confidentiality, Integrity and Availability Requirements (CR / IR / AR: Low, Medium, High) of YOUR asset plus modified base metrics (e.g. MAV for an isolated host) - this is where context enters the score. *[Vulnerability Tools, CVSS and Prioritisation]*

Environmental variables — Your context: internet-facing or isolated, data sensitivity, existing compensating controls, business criticality. CVSS environmental metrics (confidentiality, integrity and availability requirements, modified base metrics) formalise it. *[Vulnerability Management and Monitoring]*

EOL considerations — No patches after end-of-life - plan replacement in the roadmap, isolate, add compensating controls, record accepted risk with an expiry date. *[Security Architecture - SDLC, IAM Design, Cloud]*

Ephemeral container — A container added to a running pod via kubectl debug for troubleshooting; shares the pod but has no resources/probes and cannot be removed (the pod is recreated to clear it). GA since Kubernetes 1.25. *[kubectl and Cluster Operations Mastery]*

Ephemeral credentials — Short-lived secrets issued on demand: AWS STS (Security Token Service) tokens (15 min-12 h), HashiCorp Vault dynamic database users, SSH certificates valid for minutes, workload identities instead of static API keys. **[Identity and Access Management]**

Ephemeral runner — Build agent recreated for each job; matches ANSSI's regular re-instantiation and no persistent data. **[DevSecOps and Supply-Chain Security]**

EPROCESS — Windows kernel structure for one process; linked in a doubly linked list that `windows.pslist` walks and that rootkits unlink to hide a process. **[Memory Forensics with Volatility 3]**

EPS — Events per second: arrival rate of log records; drives collector and parser capacity, measured as average and peak. **[SIEM Architecture and Sizing]**

EPS / GB per day — sizing units for collectors and SIEM licences; measure on a pilot perimeter before contracting. **[ANSSI Logging and Security Supervision]**

EPSS — Exploit Prediction Scoring System: probability (0-1) that a CVE is exploited in the next 30 days. **[CISSP Domain 6: Security Assessment and Testing; Vulnerability Tools, CVSS and Prioritisation +5]**

EPSS (Exploit Prediction Scoring System) — Daily probability (0-1) that a CVE is exploited in the wild in the next 30 days, with a percentile. Model v3 (March 2023), v4 (March 2025). EPSS measures threat likelihood only; combine with CVSS (severity) and asset exposure. A CVSS 7.5 with EPSS 0.9 outranks a CVSS 9.8 with EPSS 0.01. API:... **[PCI DSS v4.0.1, CVSS and FIRST]**

EPSS (FIRST, 2019; v4 2025) — Exploit Prediction Scoring System: daily ML probability (0-1) that a CVE is exploited in the next 30 days, plus percentile. Use for ordering, not severity. **[Vulnerability Management and Security Testing]**

EPT violation — VM exit raised when a guest touches a guest physical address whose EPT entry is absent or forbids the access; used for lazy allocation, MMIO emulation and introspection. **[Virtualization Internals and VM Isolation]**

EQL (Event Query Language) — Elastic language for event patterns: category where condition and ordered sequence of events sharing a key; used by Elastic Security correlation rules. **[Query Languages: KQL, SPL, EQL, ES|QL, osquery]**

Err-disabled — Port state in which the switch has shut an interface after a violation (port security, BPDU guard); recovered by

`shutdown / no shutdown` or `errdisable recovery`. **[Cisco IOS Configuration Lab]**

Error wrapping — `fmt.Errorf` with `%w` attaches a cause; `errors.Is` tests for a sentinel value, `errors.As` extracts a concrete type, `errors.Join` combines several. **[Go Programming from Zero (Part 1: language basics)]**

ES|QL (Elasticsearch Query Language) — Elastic piped language (GA in 8.14, 2024) starting with `FROM index-pattern`; aggregations, `EVAL`, `DISSECT/GROK`, `ENRICH`. **[Query Languages: KQL, SPL, EQL, ES|QL, osquery]**

Escalate and document — breaches, exceptions and acceptances go on record to the right level **[CRISC Exam Strategy]**

Escalation path — Pre-agreed chain of contacts and thresholds: who is called, how fast, for which event (critical finding, outage, prior breach). **[Engagement Management]**

Escalation vs elevation — RS.MA-04 N1: escalation = more resources or longer time frames; elevation = involving a higher level of management. **[Incident Handling and Response]**

ESD — Electrostatic discharge: static shock that silently damages components; use a wrist strap and antistatic bags. **[CPUs, Memory, Motherboards and Buses]**

ESP — IPsec Encapsulating Security Payload: confidentiality plus integrity of the payload. **[CISSP Domain 4: Communication and Network Security; UEFI, Secure Boot and Bootkits]**

ESP (Encapsulating Security Payload) — IPsec protocol 50: encryption, integrity and anti-replay of the payload. **[VPN and Firewall Security]**

Espionage — Long-term covert collection of state or trade secrets; nation-state and corporate competitors. **[Threat Actors and Threat Vectors]**

Essential entity (EE) — NIS2 category with the heaviest regime: large Annex I entities plus size-independent cases; proactive (ex ante) supervision and EUR 10 M / 2 % fines. **[NIS2 Directive: EU-wide Obligations]**

Essential / important entity — The two NIS2 categories (EE / EI): large organisations in highly critical sectors are essential, others in scope are important; both must report, EE face stricter supervision. **[Cyber Incident Reporting Obligations]**

Essential security device — Device carrying an essential service; must be ANSSI-approved (agr  ) at the high IS level (IGI 1300 s. 6.5.2, R9) and used within its conditions of use (R10). **[Multilevel Interconnections & Trusted Core]**

Establish theory — obvious first **[CompTIA A+ Core 1 - Hardware and Troubleshooting]**

ESXi / vCenter — ESXi is VMware's bare-metal hypervisor; vCenter is the central server (appliance VCSA) that manages many ESXi hosts, clusters and vMotion. **[VMware vSphere and ESXi Security]**

`/etc/group` — `name:x:GID:member1,member2`; the secret-group equivalent `/etc/gshadow` holds group passwords and administrators. **[Linux Users, Groups, Permissions and ACLs]**

etcd — Distributed key-value store holding all cluster state, including Secrets; reading it equals owning the cluster. **[Kubernetes Security]**

Ethical — Authorised testing and bug bounties; 'white hat' with permission, otherwise it is not ethical. **[Threat Actors and Threat Vectors]**

ETL — Extract, transform, load: data pipeline jobs whose logs provide data lineage. **[SecAI+ Discriminators and Practice Scenarios]**

ETM MAC — Encrypt-then-MAC: the integrity tag covers the ciphertext, avoiding the padding-oracle weaknesses of the original SSH MAC-then-encrypt order. **[OpenSSH Hardening and Hardware Security]**

ETW — Event Tracing for Windows: kernel and user providers (Kernel-Process, DNS-Client, DotNETRuntime; Threat-Intelligence is reserved for PPL/EDR). Evasion patches `EtwEventWrite` to blind .NET tracing; EDRs detect the patch or the silence. **[Windows Endpoint Telemetry and Sysmon]**

ETW (Event Tracing for Windows) — Built-in high-speed event system: providers (kernel components, DLLs) emit events, sessions buffer them, consumers such as an EDR read them. **[EDR Telemetry, Tamper and Evasion Detection]**

etype (encryption type) — Algorithm id of a Kerberos key or ticket: 0x12 AES256-CTS-HMAC-SHA1-96, 0x11 AES128, 0x17 RC4-HMAC (key = NT hash), 0x1 / 0x3 DES (removed). **[Active Directory Tiering and Kerberos in Depth]**

EU-CyCLONe — Cyber Crisis Liaison Organisation Network: national crisis agencies coordinating large-scale incidents; ENISA is its secretariat, as for the CSIRTs Network (national Computer Security Incident Response Teams). **[ENISA, NIS2 and the EU Threat Landscape]**

EUCC — EU Common Criteria scheme, the first adopted scheme (Implementing Reg. (EU) 2024/482, Jan 2024) for ICT products, built on Common Criteria (ISO/IEC 15408) and the former SOG-IS mutual recognition agreement; levels substantial and high; operational since Feb 2025. **[ENISA, NIS2 and the EU Threat Landscape]**

EUCS and EU5G — candidate schemes for cloud services (levels basic, substantial, high; sovereignty criteria contested, not adopted) and for 5G network equipment. **[ENISA, NIS2 and the EU Threat Landscape]**

EulaAccepted — registry value HKCU\Software\Sysinternals\<Tool>\EulaAccepted = 1 written the first time a user accepts a tool's licence, or silently with -accepteula; a forensic trace of who ran which tool. **[Sysinternals Suite for Windows Administrators]**

eUtility (external utility) — software, hardware, cloud, database or human that executes processes or supplies data **[Networks of Things SP 800-183]**

EUVD — EU Vulnerability Database run by ENISA under NIS2 Art. 12, live since May 2025; complements the US CVE/NVD system. **[ENISA, NIS2 and the EU Threat Landscape]**

EV certificate — Extended Validation certificate, issued after stronger identity checks of the organisation. **[ANSSI TLS and IPsec Guides: Full R Index]**

Evasion — Fragmentation, TTL games, encoding, encryption; mitigated by normalization, TLS inspection, host sensors. **[NIST Network Security Guides; AI Security Engineering]**

Evenement redoute — what is feared on a business value; gives the severity **[EBIOS Risk Manager]**

Event / adverse event — Any observable occurrence involving computing assets (login attempt, update install). An adverse event has a negative consequence whatever the cause (power failure, attack); r3 only covers adverse **cybersecurity** events. **[SP 800-61r3 Community Profile in Detail]**

Event aggregation — Consolidating similar entries into one entry with a count (e.g. 500 identical denies = 1 line x500). **[Log Management and ISCM in Depth]**

Event correlation — Finding relationships between entries, usually with rules (e.g. many failed logons then a success from the same IP). **[Log Management and ISCM in Depth]**

Event filtering — Suppressing entries from analysis, reporting or long-term storage because they carry no useful information; the original log is unchanged. **[Log Management and ISCM in Depth]**

Event injection — Attacker-controlled data in a trigger event (HTTP body, S3 key, queue message) reaching a dangerous sink in the function. **[Serverless and Runtime Security]**

Event vs incident — An event is any observable occurrence (a logon, a blocked packet); an adverse event has negative consequences; an incident violates or imminently threatens security

policy and triggers the IR plan. Most events are never incidents. **[Incident Response and Management]**

Evidence — Data on which to base proof or to establish truth or falsehood; in IR all collected incident data is treated as evidence even if no prosecution follows. **[Digital Forensics in Incident Response]**

Evidence acquisition — Forensic copies in order of volatility (most short-lived data first); write-blocker (hardware that blocks any write to the evidence disk) for disks; memory before power-off; network captures from SPAN/TAP; cloud snapshots and audit logs exported. **[Incident Response and Management]**

Evidence strength — FAIR (e.g. bank or mobile phone account, student or corporate ID), STRONG (government photo ID with security features), SUPERIOR (cryptographically signed, biometric embedded, e.g. passport with chip, PIV card). **[Digital Identity Guidelines SP 800-63-4]**

Evil maid attack — Tampering with an unattended laptop's boot chain to capture the pre-boot password later. **[ANSSI Encryption Tools: Zed! and Cryhod (2/2, Cryhod); Hardware Security: Self-Assessment]**

Evil twin — Rogue access point broadcasting the same SSID (network name) as the legitimate one to capture clients. **[DNS, Wi-Fi & DDoS Architectures]**

Evilginx — Reverse-proxy AitM that captures session cookies AFTER MFA - defeats push/OTP. **[Cloud, Wireless, Social Eng and Specialized Attacks]**

EVM (Ethereum Virtual Machine) — stack machine running contract bytecode on Ethereum and compatible chains (Arbitrum, BNB Chain, Polygon); contracts written mostly in Solidity or Vyper **[Blockchain and Smart-Contract Security]**

EVPN-VXLAN — VXLAN tunnels carry Layer-2 segments across an IP underlay; Ethernet VPN (EVPN, a BGP address family) distributes the MAC/IP reachability as the control plane. **[Data-Centre Architecture]**

EWS (engineering workstation) — PC with vendor software that programs controllers: the crown jewel of an OT network. **[NIST OT and IoT Security]**

Exam guide — OffSec's authoritative document on scoring, allowed tools and report rules; overrides any summary. **[OSCP / OSCP+: Exam Format and Rules]**

Examine — Review documents, configurations and records (policies, SSP, rulesets, logs, tickets). SP 800-53A Rev. 5, Assess-

ing Security and Privacy Controls. **[SP 800-53r5 Key Controls Explained]**

Exception — Approved, time-limited deviation from a policy or standard, backed by a risk assessment and compensating controls. **[CRISC Domain 3: Risk Response and Reporting; Python for Security from Zero]**

Exceptions and exemptions — documented risk acceptance with owner, expiry date and review **[Vulnerability Management and Monitoring]**

Exchange hash (H) — Hash over both banners, both KEXINIT lists, the host key and the key-exchange values; signed by the server, and the first one becomes the session identifier. **[SSH in Depth]**

Exclusive ownership — A signature cannot verify under another public key. Its absence broke an early draft of ACME (Let's Encrypt), fixed by changing the signature scheme. **[ANSSI Crypto Rules Catalogue (PG-083 v3.00)]**

Execution environment — The microVM sandbox that serves many invocations in sequence; memory, /tmp and globals persist between them. **[Serverless and Runtime Security]**

Execution role — IAM role the Lambda service assumes for the function; its temporary credentials sit in the function's environment variables. **[Serverless and Runtime Security]**

Executive summary — Half a page that lets a decision-maker act without reading the rest: situation, impact, what is being done, decision needed. **[Writing for Security Work]**

Exercise — Scenario-driven simulation of an emergency that validates one or more aspects of a plan **without** using the real operational environment. **[IR Exercises and Threat Information Sharing]**

Exercise programme — Multi-year plan of exercises on various topics to train as many people as possible, in line with the exercise strategy. **[Organising a Cyber Crisis Management Exercise]**

Exit code as a signal — grep returns 0 if it matched, 1 if not, 2 on error; scripts test this with `if grep -q ... diff` returns 1 when files differ. See sheet 06 for the full table. **[Text-Processing and Data Toolkit Reference]**

Exit code (exit status) — The number 0-255 a command returns; 0 means success, anything else failure; \$? holds the last one. **[Bash Scripting from Zero]**

Exit status — integer 0-255 a program returns to its parent when it ends; 0 = success, anything else = a failure or a condition

(grep: 1 = no match). Read with `$?` or `$LASTEXITCODE`.
 [Master Any Command-Line Program Fast, on Every OS]

Expansion — What bash does to a line before running it: variables `$x`, commands `$(cmd)`, arithmetic `$(1+2)`, wildcards `*.log`, then word splitting. *[Bash Scripting from Zero]*

Expert Info — Wireshark's own diagnoses (chat, note, warning, error) such as retransmission, zero window or malformed packet; Analyze > Expert Information or `tshark -z expert`.
 [Wireshark and tshark for Troubleshooting and Analysis]

ExpertCyber — Label granted by `Cybermalveillance.gouv.fr` to IT providers able to secure and assist SMEs after an incident.
 [Business Travel and SME Cybersecurity]

Explain / Compare and contrast — Knowledge objectives (1.1, 1.4, 1.5, 2.5, 3.1, 3.3, 4.1, 4.2): expect definition and best-practice questions. *[CompTIA CySA+ CS0-003]*

Explicit TLS (STARTTLS) — Starts in clear, upgrades on the same port (25/587, 21, 143, 110, 389). Downgradable unless enforced (MTA-STTS). *[Networking Ports and Protocols]*

Exploit — Code or technique that takes advantage of a specific vulnerability. *[CEH v13: Core Concepts, Phases and Legal Framework; Vulnerabilities]*

Exploits first — 38% of initial vectors (M-Trends 2024) *[Edge, Readiness and Awareness Reports]*

Export controls — US EAR (Export Administration Regulations: dual-use goods; encryption hardware and software are classified 5A002/5D002) and ITAR (International Traffic in Arms Regulations: defense items); Wassenaar Arrangement internationally - affects where crypto code and pentest tools may be shipped or hosted. *[Compliance, Threat Modeling and AI Security]*

Exported component — Android activity, service, receiver or provider callable by any other app on the device. *[OWASP Mobile - Top 10 2024, MASVS v2.1, MASTG]*

Exposure factor — Share of the asset lost if the flaw is exploited (0-100 %), same term as in quantitative risk; drives SLE and therefore priority. *[Vulnerability Management and Monitoring]*

Exposure minimisation — publish only through a DMZ, close unused services, no admin interface on the Internet *[ANSSI Secure Architecture: sensitive and RD systems]*

Expunge — Delete data so it cannot be recovered, including backups and replicas, with evidence of deletion. *[Cloud Outsourcing and Virtualization Lifecycle]*

Extensions and extras — R14-R23: extensions to always use / to assess / never to use, randomness, no compression, ticket lifetime, secure renegotiation, no 0-RTT *[ANSSI TLS and IPsec Guides: Full R Index]*

Extent — One contiguous run of blocks described as (logical start, physical start, length); ext4, XFS, NTFS (runs) and APFS use extents instead of per-block pointers. *[Storage and Filesystems for Defenders]*

External: assessment — Gap analysis by a consultant or customer against a framework; advisory, no certificate. *[Compliance, Audits and Security Awareness]*

External audit — Audit by an outside firm engaged by the organisation, usually for regulators or shareholders. *[CISSP Domain 6: Security Assessment and Testing]*

External: examinations — Deep inspection of one area by a regulator or licensing body, often on-site after an incident or complaint. *[Compliance, Audits and Security Awareness]*

External: independent third-party audit — Accredited firm gives an objective opinion for customers and regulators: SOC 2 report, ISO 27001 certification audit, PCI ROC. *[Compliance, Audits and Security Awareness]*

External: regulatory — Mandatory reviews by the regulator with legal consequences (banking supervisors, health authorities). *[Compliance, Audits and Security Awareness]*

External Secrets Operator — Kubernetes operator that creates Secrets from an external manager (AWS Secrets Manager, Vault) based on committed ExternalSecret references. *[Kubernetes Security; GitOps and Continuous Delivery Security]*

Extraterritorial law — Legislation that compels a provider to hand over client data held anywhere in the world, without informing the client or allowing appeal. **US CLOUD Act** (2018) and **FISA 702** are the reference cases; SecNumCloud 3.2 §19.6 was written to make qualified providers immune. *[Cloud Hosting for Sensitive Systems]*

Extreme but plausible scenarios — Objective 1.2 impact analysis - model tail events (ransomware on all sites, cloud region loss, key supplier bankrupt) with business owners, not average incidents. *[Governance and Risk Management]*

Eyes on runtime and audit — Falco/Tetragon, audit policy, alert on exec and RBAC writes *[Kubernetes Security]*

F

Fail-closed — When the control fails, everything is blocked; security is preserved, availability is lost. Also called fail-secure (for doors: stays locked). *[Securing Enterprise Infrastructure]*

Fail-open — When the control fails, traffic or people are allowed through; availability and safety are preserved, security is lost until repair. *[Securing Enterprise Infrastructure]*

Fail-open vs fail-closed — Inline IPS hardware bypass on failure (availability) vs block all (security). 800-94: decide per segment. *[NIST Network Security Guides]*

Fail-safe — SP 800-123 principle: on failure, the server denies access rather than opening up. *[Security Operations: Logs, Malware, Servers, Media; OWASP Developer Guide v4.2 - Chapter by Chapter]*

Fail secure — When a control errors or its configuration is missing, access is denied rather than granted. *[OWASP Secure Coding Practices and Developer Guide]*

FAIR / ALE — Factor Analysis of Information Risk (quantitative risk model) / annualized loss expectancy = single loss x yearly rate. *[SecurityX Practice Scenarios]*

Fake CAPTCHA / ClickFix — web page tells the victim to press Win+R and paste a command 'to verify you are human'; the clipboard holds a PowerShell or mshta download cradle. Detect: `explorer.exe` spawning `powershell/mshta` with URLs, new values under `HKCU\...\Explorer\RunMRU`; mitigate: block Win+R for standard users where feasible... *[Social Engineering and Deepfakes]*

False negative — Attack missed: the dangerous one; measured by red-team and Atomic tests. *[NIST Network Security Guides]*

False positive — finding reported for a flaw that is not present (patched by a backport, wrong product guess); a false negative is a real flaw the scanner missed. *[Vulnerability and Configuration Scanners for Your Own Estate]*

FAR — False acceptance rate of a biometric: impostors accepted (type II error); most critical for security. *[CISA Domain 5: Protection of Information Assets]*

Fast-forward — a merge where the branch pointer simply slides forward because there were no divergent commits; no merge commit is created. *[Essential Git Commands: a Working Reference]*

FAST (Kerberos armoring) — Protects Kerberos pre-authentication inside an encrypted tunnel built from the ma-

chine's ticket. *[ANSSI Active Directory Recommendation Catalogue; Active Directory Tiering and Kerberos in Depth]*

FAT / SAT — Factory Acceptance Test at the integrator's site / Site Acceptance Test after installation; the right moments to test security settings. *[ANSSI ICS Detailed Measures v2 (1/2): organisation and accounts]*

Fault / blackout — Momentary / prolonged loss of power. *[CISSP Domain 3: Security Architecture and Engineering]*

FCEB — Federal Civilian Executive Branch: the US civilian agencies bound by OMB memos and CISA binding operational directives (BODs). *[CISA Zero Trust Maturity Model v2.0]*

FCoE / iSCSI — Storage over Ethernet (layer 2) / SCSI over IP; isolate storage VLANs and use CHAP or IPsec for iSCSI. *[CISSP Domain 4: Communication and Network Security]*

FDE (full-disk encryption) — Encryption of an entire disk or partition, decrypted on the fly after pre-boot authentication. *[ANSSI Encryption Tools: Zed! and Cryhod (2/2, Cryhod)]*

Feared event (evenement redoute, ER) — breach of a business value's security need (availability, integrity, confidentiality, traceability) with its impacts, rated in severity *[EBIOS Risk Manager]*

Feasibility condition — A neighbour is a loop-free backup only if **RD** < **FD** of the current successor. *[Routing II: EIGRP, BGP at the Enterprise Edge, Redistribution]*

Feasibility study — Assessment of technical, economic, operational and legal viability before committing. *[CISA Domain 3: IS Acquisition, Development and Implementation]*

Feasible distance (FD) — Best total metric from this router to the destination, via the successor. *[Routing II: EIGRP, BGP at the Enterprise Edge, Redistribution]*

Feasible successor — Backup satisfying the condition, kept in the topology table; takes over instantly without queries. *[Routing II: EIGRP, BGP at the Enterprise Edge, Redistribution]*

Federal Contract Information (FCI) — Information not intended for public release, provided by or generated for the government under contract (FAR 52.204-21, Federal Acquisition Regulation clause). Protected by 15 basic safeguarding requirements = CMMC Level 1 (Cybersecurity Maturity Model Certification). *[SP 800-171 Rev. 3, CUI and CMMC 2.0]*

Federation — Trust between an identity provider and service providers across organizational boundaries: authenticate once at home, access partner or SaaS resources without a second cre-

dential. Built on SAML or OIDC plus a metadata/certificate exchange. *[Identity and Access Management]*

Federation (FAL) — assertion strength IdP -> RP, 63C *[Digital Identity Guidelines SP 800-63-4]*

FedRAMP — Federal Risk and Authorization Management Program: US government authorisation of cloud services, built on 800-53 baselines with pre-set ODPs. *[NIST SP 800-53r5 Controls in Practice]*

Fetch Metadata — Sec-Fetch-Site, Sec-Fetch-Mode, Sec-Fetch-Dest and Sec-Fetch-User request headers that tell the server where a request comes from, so it can refuse cross-site requests to sensitive endpoints. *[HTTP Security Headers and Browser Policies]*

FIB — Forwarding Information Base: the kernel's lookup structure built from the routing tables; ip route get queries it exactly as a packet would. *[Linux Networking Toolbox]*

FIDO2 SSH key (-sk) — Key type (ed25519-sk, ecdsa-sk) whose private key stays on a hardware token; the file on disk is only a handle, useless without the token and a physical touch. *[SSH in Depth]*

FIDO2 / WebAuthn — standard for public-key login bound to the website's origin, so a fake site cannot replay it (security keys, passkeys). *[Authentication, MFA and Passwords; CISA Zero Trust Maturity Model v2.0]*

FIDO2 / WebAuthn / passkey — FIDO Alliance standard = W3C WebAuthn (browser API) + CTAP (authenticator protocol); a passkey is a FIDO2 credential, device-bound or synced across a user's devices. *[Identity Protocols: OAuth, OIDC, SAML, FIDO2]*

Field and delimiter — a line split into columns; the delimiter is the character between fields (space, tab, comma). cut -d,, awk -F, and sort -t, all set it. *[Text-Processing and Data Toolkit Reference]*

File systems (Core 2 1.8) — NTFS (permissions, EFS, journaling, 256 TB), FAT32 (4 GB file limit, cross-platform), ex-FAT (flash, large files), ext4/XFS (Linux), APFS (macOS). *[CompTIA A+ Core 1 - Hardware and Troubleshooting]*

FILETIME — Windows timestamp format: 100-nanosecond intervals since 1601-01-01 UTC; artefacts are stored in UTC, displays convert to local time. *[DFIR Artifacts and Tools]*

filetype: / ext: — Find indexed documents and data files (pdf, sql, log, env, bak) that leak internal information or credentials. *[Reconnaissance and OSINT]*

FileVault — full-volume encryption of the data volume (XTS-AES-128 with a 256-bit key); on Apple silicon and T2 Macs storage is always hardware-encrypted and FileVault binds the key to the user password via the Secure Enclave. *[macOS Security for Defenders]*

Filtering policy — Ordered list of rules (source, destination, service, action, log) that a firewall evaluates top-down, first match wins. *[Firewall Policy: Design, Cleanup, Exposed Zone]*

FIN — Finish: this side has no more data to send (half-close) *[TCP and UDP Deep Dive]*

Final — Approved publication; the previous revision is usually withdrawn on the same day or after a transition period. *[NIST Cyber Publications 2024-2026 Roundup]*

Final explicit deny — Last firewall rule that denies and logs everything not allowed above it, making the implicit deny visible. *[VPN, Firewall Policy, Models, QoS: Self-Assessment]*

Financial gain — Ransom, fraud, BEC wire transfers, crypto-jacking (secretly mining cryptocurrency on victims' machines), card theft. *[Threat Actors and Threat Vectors]*

Finding — Documented gap from an audit, assessment or test, rated and assigned to an owner with a remediation date. *[CRISC Domain 3: Risk Response and Reporting; Risk Management Framework (RMF)]*

FIPS — Federal Information Processing Standard: mandatory for US federal systems (cryptographic algorithms, module validation), unlike SP (Special Publication) guidance. *[NIST Cyber Publications 2024-2026 Roundup]*

FIPS 140-3 — Module validation under the Cryptographic Module Validation Program (CMVP): Level 1 software, Level 2 tamper evidence + role auth, Level 3 tamper resistance + identity auth + key zeroization, Level 4 environmental failure protection. FIPS 140-2 certificates moved to the historical list in Sept 2026. *[NIST Cryptography, TLS and PKI]*

First-seen analysis — flag an entity (binary, domain, logon pair) the first time it appears against a learned baseline window. *[Threat Hunting Playbooks]*

FISMA — Federal Information Security Modernization Act: US law requiring agencies to assess and report security; SP 800-115 supports it. *[PTES Phase Tasks, SP 800-115, Kill Chain Analysis]*

Flash loan — uncollateralised loan borrowed and repaid in one transaction; gives any attacker huge temporary capital *[Blockchain and Smart-Contract Security]*

Floating static route — Backup static route given an administrative distance higher than the primary route source, so it is installed only when the primary disappears. **[Switching, Routing, Wireless, Fabrics: Self-Assessment]**

Flow control vs congestion control — Flow control stops the sender overrunning the receiver (rwnd); congestion control stops senders overrunning the network (cwnd). **[TCP and UDP Deep Dive]**

Flow record — Summary of one conversation (addresses, ports, protocol, bytes, packets, start and end times) exported by a router or switch; no payload. **[Network Operations: Documentation, Monitoring, Resilience]**

FMECA (AMDEC) — Failure Modes, Effects and Criticality Analysis: the safety study that splits a plant into functions; PA-084 reuses its split for detection perimeters. **[OT Detection Doctrine, Integrators and Training]**

Focus areas (objective 1.4) — Configurations and misconfigurations (exposed services, default creds), isolated networks (OT segments, jump hosts), business-critical assets and processes (crown jewels, payment flow). **[Threat Intelligence, Hunting and SOC Efficiency]**

Fogg Behaviour Model (B = MAP) — a Behaviour happens when Motivation, Ability and a Prompt meet at the same moment; the cheapest lever is usually ability (make the secure action easy), not motivation **[Security Awareness and Culture Programme]**

Follow-the-sun — Rotation where teams in several time zones hand over at the end of their day, so nobody works nights. **[Working Life in Security]**

Foothold — Any access the attacker keeps (account, backdoor, scheduled task); eradication fails if one is missed. **[SANS Incident Handler Checklists and Enterprise IR]**

Foreign key (FK) — Column that holds the primary key of a row in another table, linking them (`logins.host_id` → `hosts.id`). **[SQL Basics for Security]**

Forensic account — Isolated cloud account/subscription/project where evidence is copied, encrypted with a dedicated key and analysed. **[Cloud Incident Response and Forensics]**

Forensic image — Bit-for-bit copy verified by hash; analysis runs on the copy, never the original. **[Digital Evidence and Chain of Custody; CISA Domain 5: Protection of Information Assets]**

Forensic readiness (SP 800-86 sec. 2) — Policies, guidelines and procedures written **before** an incident: who may collect what, when to call law enforcement, tool validation, logging

configured so that the data exists (SP 800-92, Guide to Computer Security Log Management), staff trained, legal counsel involved in privacy and monitoring notices. **[Digital Forensics in Incident Response]**

Forest — The top-level container and the true security boundary of Active Directory; it holds one schema and one configuration shared by all its domains. **[On-Prem Active Directory Architecture; Windows Administration and Active Directory Basics]**

Forest boundary — The security limit is the forest, not the domain: eviction objectives are met only when attained in every domain of the compromised forest, at the same time. **[Active Directory Tier 0 Remediation]**

Form 10-K Item 1C — annual SEC disclosure of cyber risk management, strategy and governance: board oversight and management's role and expertise **[Global Security and Privacy Regulations]**

Formal methods — Mathematical proof that a design or code has a property (specification languages such as TLA+, model checking; the seL4 microkernel is formally verified) - used for protocols, crypto libraries, safety-critical firmware; expensive, reserved for the highest assurance components. **[Security Architecture - SDLC, IAM Design, Cloud]**

Format string — user data used as a `printf` format; caught by security warnings such as `-Wformat-security` (R37) and hardened `*_s` variants (R38, R178). **[Secure Coding in C and Rust, CMS and JRE Hardening]**

Forward Secure Sealing — journald feature that seals log files at intervals with keys that evolve forward, so an attacker who gains root later cannot forge earlier entries undetected. **[Observability and Security Telemetry Pipelines]**

Fourth party — your vendor's vendor (hosting, subprocessor, support centre); Nth party for deeper levels **[Third-Party Risk Management (TPRM)]**

Fourth-party risk — Risk from your supplier's own suppliers, invisible without contract clauses and inventories. **[CISM Domain 2: Information Security Risk Management]**

FPE (format-preserving encryption) — encryption whose ciphertext has the same format as the plaintext (16 digits stay 16 digits); NIST SP 800-38G defines FF1 and FF3-1 over AES **[Privacy Engineering and PETs]**

Fragile vs robust; blind vs non-blind — Fragile marks break on any edit (integrity use); robust ones survive edits. Blind detection needs no original, the relevant case for synthetic content. **[GenAI Secure Development and Content Transparency]**

Free space — Unallocated clusters, including space outside any partition, where whole deleted files or volumes may survive. **[Forensics by Data Type]**

Freshness value — Counter or timestamp included in the MAC so a recorded valid frame cannot be replayed later; needs a freshness value manager and resynchronisation after resets. **[Automotive and Embedded Security]**

FRP256v1 — French 256-bit elliptic curve published in the Journal officiel on 16/10/2011, conformant to the guide. **[ANSSI Crypto Rules Catalogue (PG-083 v3.00)]**

FRR — False rejection rate: legitimate users rejected (type I error); affects usability. **[CISA Domain 5: Protection of Information Assets]**

FRU — Field-replaceable unit: a component designed to be swapped on site (battery, SSD, keyboard). **[Laptops, Mobile Devices, Virtualization Hardware]**

FSEvents — The `fsevents` daemon writes gzip-compressed pages to `/.fsevents/` on each volume (internal and external). Each record holds a full path, a 64-bit event id and flags (Created, Removed, Renamed, Modified, InodeMetaMod...). Records carry **no timestamp**: approximate times come from the modification time of each page... **[macOS and iOS Forensics for Defenders]**

FSMO (Flexible Single-Master Operation) — Five special roles that must run on exactly one domain controller each to avoid conflicts (two forest-wide, three domain-wide). **[On-Prem Active Directory Architecture]**

FSMO roles — Five single-master operation roles (schema, domain naming, RID, PDC emulator, infrastructure) held by specific DCs; numbered 0-4 in PowerShell. **[Active Directory Tier 0 Remediation]**

FSMO roles (Flexible Single Master Operations) — Five jobs held by one DC each: Schema and Domain Naming master (per forest), RID, PDC emulator and Infrastructure master (per domain); `netdom query fsmo` lists them. **[Windows Administration and Active Directory Basics]**

FTL — Flash translation layer: SSD firmware mapping logical block addresses to physical NAND pages. **[Storage: Interfaces, SSD Internals, RAID, SMART]**

Full-tunnel VPN — Virtual private network configured so that all traffic of the device goes through the company gateway; the opposite, split tunnelling, lets some traffic go straight to the Internet. **[Business Travel and SME Cybersecurity]**

Function — Highest level of the Core; the six Functions are an organized view of the risk management lifecycle, not a sequence. *[NIST Cybersecurity Framework 2.0]*

Function-level vs object-level authz — Function level = can this role call this endpoint at all; object level (BOLA) = can this user act on this specific record. Test both. *[Web Application Assessment]*

Function point analysis — Sizes software by inputs, outputs, inquiries, files and interfaces; basis for effort estimates. *[CISA Domain 3: IS Acquisition, Development and Implementation]*

Function URL — Built-in HTTPS endpoint of a Lambda; with `AuthType NONE` anyone on the Internet can invoke it. *[Serverless and Runtime Security]*

Functional key — Key pair tied to a function or team (e.g. 'HR mailbox') rather than to a named person. *[ANSSI Encryption Tools: Zed! and Cryhod (1/2, Zed!)]*

Fuser — Heated roller assembly in a laser printer that melts toner into the paper. *[Power, Displays, Peripherals and Printers]*

FUZZ marker — A placeholder (FUZZ in ffuf) in the URL or a header that the tool replaces with each wordlist entry in turn. *[Web and API Testing Toolkit for Your Own Apps]*

G

GAC (gestionnaire d'accès centralisé) — Central access management software and database in the management centre (rights, validity dates, logs). *[Physical Access Control and CCTV (ANSSI PA-72)]*

Gadget chain — Sequence of existing classes whose methods, run during deserialization, end in code execution; no attacker code is needed. *[Secure Code Review by Language]*

GAN (generative adversarial network) — Generator creates samples, discriminator judges real vs fake; both improve by competing. Source of deepfakes and synthetic training data; exam objective 3.2 calls this **adversarial networks**. *[AI Fundamentals for Cybersecurity]*

Gap analysis — Comparison of the **current state** of controls with a **target state** (a framework, a regulation or a desired maturity level), producing the list of missing or weak controls and a prioritised plan to close them. *[Fundamental Security Concepts]*

Gas — fee per computation step; bounds execution and makes loops over unbounded arrays a denial-of-service risk *[Blockchain and Smart-Contract Security]*

Gatekeeper — launch-time check (daemon `syspolicyd`) applied to files carrying the `com.apple.quarantine` extended attribute: verifies the Developer ID signature, the notarization ticket and XProtect signatures before first launch. *[macOS Security for Defenders]*

GB/day — Raw volume ingested per day; the unit of most SIEM licences and of storage sizing. *[SIEM Architecture and Sizing]*

GDAP (Granular Delegated Admin Privileges) — Microsoft partner model giving an MSP time-limited, role-scoped admin rights in a customer tenant instead of global admin. *[Designing a Secure SME Network and Cloud Landing Zone]*

General Security Concepts — 1.0, 12 %: controls, CIA (confidentiality, integrity, availability), AAA (authentication, authorization, accounting), Zero Trust, change management, cryptography *[CompTIA Security+ SY0-701]*

Geo / velocity — alert on impossible-travel and distributed failures *[Network and Authentication Attacks]*

Geographic location — Physical place where a sensor or eUtility operates; may change or be unknown, in which case its data should be treated as suspect. *[Networks of Things SP 800-183]*

Geographical considerations — Latency, data sovereignty (GDPR transfers, sovereign cloud), disaster radius (sites far enough apart not to share a flood, grid or earthquake zone), local regulations, export controls. *[Security Architecture - Resilience, Controls, Zero Trust]*

Get deps clean — `go mod tidy`, `go mod verify` *[Go for Security Tooling and Safe Code]*

Get-out-of-jail letter — Signed authorisation carried during physical or social-engineering tests, naming a client contact who confirms the engagement. *[Pentest Methodologies]*

giaddr — Gateway IP address field of a DHCP message, filled by a relay agent with the address of the interface that received the client's broadcast; the server picks the pool from it. *[Protocol Walk-Throughs at Packet Level]*

GitOps — Operating model where the desired state of a system is kept in git (or an OCI registry) and an in-cluster agent continuously reconciles the live state to it. *[GitOps and Continuous Delivery Security]*

GitOps encryption — **Sealed Secrets** (cluster public key, controller decrypts, cluster-bound) or **SOPS** (age/KMS-encrypted values, decrypted by Flux or Argo CD plugin). Never plain Secrets in git. *[Kubernetes Security]*

Given a scenario — Application objectives (1.2, 1.3, 2.1-2.4, 3.2): expect log excerpts, scan output, and "what should the analyst do NEXT" questions. These are the PBQ sources. *[CompTIA CySA+ CS0-003]*

GKE Workload Identity — Kubernetes SA → IAM binding (`principal://iam.googleapis.com/projects/N/locations/global/workloadIdentityPools/PROJECT.svc.id.goog/subject/ns/NS/sa/KSA`); replaces node SA use and metadata concealment. *[GCP Security Essentials]*

Global Catalog (GC) — A partial, forest-wide index of every object, hosted on chosen DCs, so searches and logons resolve across domains (listens on TCP 3268/3269). *[On-Prem Active Directory Architecture; Windows Administration and Active Directory Basics]*

GMDSS / EPIRB — Global Maritime Distress and Safety System / Emergency Position-Indicating Radio Beacon, the distress chain. *[Cyber Security On Board Ships]*

gMSA — Group Managed Service Account: AD rotates a 240-byte random password automatically. *[Active Directory Security; SecurityX Practice Scenarios +2]*

GNSS — Global navigation satellite systems: GPS, Galileo, GLONASS, BeiDou, the position source for almost every bridge system. *[Cyber Security On Board Ships; Space and Satellite Security]*

GNSS spoofing — Counterfeit satellite signals make the receiver compute a false position. 22 June 2017, Black Sea: about 20 ships reported a position at Gelendzhik airport. Mitigation: multi-constellation and multi-frequency receivers, OS-NMA, radar and visual cross-check, BNWAS alarms. *[Cyber Security On Board Ships]*

go.mod — The module file: module path, Go version, and required dependencies with their versions (semantic versioning). *[Go Programming from Zero (Part 2: concurrency and the standard library)]*

go.sum — Checksums of every dependency version ever used; verified on download against the public checksum database so a swapped module is detected. *[Go Programming from Zero (Part 2: concurrency and the standard library)]*

Goal decides the tactic — Deleting files to hide = Indicator Removal: File Deletion (Defense Evasion); deleting files to hurt = Data Destruction (Impact). *[ATT&CK Design Philosophy, ATT&CK for ICS, CISO View]*

Goal reprioritization — Adjusting objectives mid-test with client approval, e.g. shifting effort to a newly found critical path. [*\[Engagement Management\]*](#)

Golden SAML — Forging SAML assertions with a stolen IdP signing key to log in as anyone at every federated service. [*\[Multi-Cloud Identity Federation\]*](#)

Golden ticket — Forged TGT signed with the krbtgt hash; fix requires rotating krbtgt twice. [*\[Identity and Active Directory Assessment\]*](#)

Good metric (SMART, and 'so what') — Specific, measurable from a system of record (not a survey), actionable by a named owner, relevant to a decision, time-bound with a target. Each board metric must answer **so what**: what decision changes if it is red. Reference: **NIST SP 800-55 Rev. 2** (Vol. 1 measurement programme, Vol. 2 catalogue, 2024) and... [*\[Security Metrics and Board Reporting\]*](#)

Good practice — strongly advised, replaceable by an equivalent rule of the team's own convention (layout, include order). [*\[C and Rust Secure Coding Rule Catalogue\]*](#)

Good supervision data — meaningful (reflects IS activity), relevant (capture point makes sense for a feared event), diverse (pivot on IP + timestamp across sources, needs normalisation), enriched (filtered, GeolP, aggregated). [*\[Security Supervision: ANSSI GP-112 and PG-113\]*](#)

Governance over gadgets — policy, process, metrics beat a single tool [*\[CISM Exam Strategy\]*](#)

govulncheck — Official vulnerability scanner (golang.org/x/vuln); flags known CVEs in dependencies that your call graph actually reaches. [*\[Go Programming from Zero \(Part 2: concurrency and the standard library\)\]*](#)

GPAI model — general-purpose AI model: trained on broad data, competent at many tasks, integrated into downstream systems (foundation model) [*\[Cyber Resilience Act and AI Act; AI Governance Programme\]*](#)

GPO — Group Policy Object: a set of settings linked to a site, domain or OU and applied to every computer or user below it. [*\[Windows and Active Directory for Defenders\]*](#)

GPO (Group Policy Object) — A set of settings linked to a site, domain or OU that configures users and computers (security baselines, drive maps, restrictions). [*\[On-Prem Active Directory Architecture\]*](#)

GPO / WEF — Group Policy Object (central Windows configuration pushed from AD) / Windows Event Forwarding (built-in

agentless push of chosen events to a collector server). [*\[Windows Endpoint Telemetry and Sysmon\]*](#)

GPP — Group Policy Preferences: GPO extension that sets arbitrary registry values, services or files, used where no administrative template exists. [*\[Windows Privacy GPOs and VBS Deployment\]*](#)

GPP cpassword — Passwords stored in old Group Policy Preferences XML in SYSVOL, encrypted with a key Microsoft published (fixed by MS14-025). [*\[Identity and Active Directory Assessment\]*](#)

Grab and leak — data theft 32% top impact [*\[IBM Breach Cost and X-Force Index 2024\]*](#)

Graham-Denning — Eight protection rules for securely creating, deleting and transferring subjects, objects and rights. [*\[CISSP Domain 3: Security Architecture and Engineering\]*](#)

GRC (Governance, Risk and Compliance) — functions that set security policy, assess and track risk, and demonstrate conformity with laws and standards [*\[Career Map of Cyber Security Roles\]*](#)

GRC tools — Governance, risk and compliance platforms. Objective 1.1 sub-bullets: mapping (one control satisfies many frameworks), automation (evidence collected by API), compliance tracking, documentation, continuous monitoring (SP 800-53 CA-7: ongoing control assessment instead of a yearly snapshot). Examples: ServiceNow IRM,... [*\[Governance and Risk Management\]*](#)

Greedy / lazy quantifier — Greedy (*, +) consumes as much text as possible then gives back; lazy (*?, +?) consumes as little as possible. [*\[Defender Scripting Toolkit\]*](#)

GREEN — the community [*\[IR Exercises and Threat Information Sharing\]*](#)

Grey-box test — Tester gets partial knowledge: accounts per role, API docs, architecture diagram. [*\[OWASP Web Security Testing Guide v4.2\]*](#)

Grey hat — Acts without permission but claims good intent; still illegal. [*\[CEH v13: Exam Blueprint and Module Map\]*](#)

Groundedness — Degree to which an answer is supported by the retrieved sources; low groundedness signals hallucination. [*\[AI Monitoring, Attacks and Compensating Controls\]*](#)

Grounding — Forcing answers to rest on supplied evidence (logs, docs) and to cite it, so a human can check each claim. [*\[AI Assistants for Defenders\]*](#)

GTFOBins — public catalogue of Unix binaries that can be abused to escape restrictions or spawn a root shell when allowed by sudo or SUID. [*\[Linux Security Command Line\]*](#)

GTK — Group Temporal Key: key for broadcast and multicast frames, chosen by the AP and delivered encrypted in message 3 of the 4-way handshake. [*\[Wi-Fi Security Internals\]*](#)

GTSM (RFC 5082) — Generalised TTL security: directly connected eBGP peers send TTL 255 and accept only 254+, so spoofed packets from afar cannot reach the session. [*\[BGP, 802.1X & VPN\]*](#)

Guard rails — Automated preventive limits that stop unsafe actions before they happen (deny public buckets, block untagged resources). [*\[Incident Response, Forensics, Automation\]*](#)

Guardrail — Rule or classifier around a model that blocks disallowed inputs or outputs (topics, PII, code execution). [*\[Cloud Reference Architectures; CompTIA SecAI+ CY0-001 +1\]*](#)

Guest OS isolation (§3.1) — Hypervisor partitions CPU, memory, storage, network; risks are side channels (cache timing), covert channels and escape bugs in device emulation (VENOM CVE-2015-3456 floppy controller). [*\[Container and Virtualization Security\]*](#)

Guest physical address (GPA) — Address the guest believes is physical RAM; the hypervisor maps it to a host physical address (HPA). [*\[Virtualization Internals and VM Isolation\]*](#)

H

Hack value — How worthwhile or interesting a target is to an attacker. [*\[CEH v13: Core Concepts, Phases and Legal Framework\]*](#)

Hacktivist — Attacks to promote a political or social cause. [*\[CEH v13: Exam Blueprint and Module Map\]*](#)

HAE-NCF — Hybrid Application Environment - Network Configuration Function: the guide's numbered recommendations (HAE-NCF-1 to 5), each stated in full below. [*\[Secure Enterprise Network Landscape SP 800-215\]*](#)

Hallucination — Fluent output not supported by the input or by reality: an invented event ID, KQL table, CVE (Common Vulnerabilities and Exposures) number or library function. [*\[AI Assistants for Defenders\]*](#)

HAMR / helium — Heat-assisted recording (Seagate 30 TB+ class drives, 2024-2025) and helium-filled enclosures push HDD capacity; HDD cost per TB still beats SSD for bulk data. [*\[Storage: Interfaces, SSD Internals, RAID, SMART\]*](#)

Handle — reference a process holds to a kernel object (file, registry key, mutex, process); a locked file is a file someone holds a handle to. *[Windows Internals for Defenders; Sysinternals Suite for Windows Administrators]*

Handover — Structured transfer of open work, context and risks from one shift or person to the next. *[Working Life in Security]*

Hardening level letters — M minimal, I intermediate, E enhanced, H high; the guide prints the letters of every level that includes the rule, so M I E means the rule starts at enhanced. *[ANSSI GNU/Linux Hardening Deep Dive (BP-028 R1-R49)]*

Hardware assurance — Certification and validation: FIPS 140-3 (US/Canada validation of cryptographic modules, security levels 1-4, level 3+ adds tamper response), Common Criteria (ISO/IEC 15408) EAL1-7 evaluation assurance levels against Protection Profiles, trusted foundry for chips, tamper-evident supply chain. *[Security Architecture - SDLC, IAM Design, Cloud]*

Hardware Security Module (HSM) — Tamper-resistant device that generates and stores private keys and signs inside itself, so the key never appears in software. CA keys target FIPS 140-2/140-3 Level 3. *[PKI and Certificate Architecture]*

Hardware TTPs (3.4) — Firmware tampering (UEFI implants like LoJax, 2018; BlackLotus bootkit bypassing Secure Boot, revoked by 2023 dbx updates), shimming (thin skimmer between card and reader; also Windows application shims abused for persistence), USB attacks (BadUSB firmware, keystroke-injection devices, malicious cables) - counter... *[Security Engineering - IAM, Endpoints, Network, Hardware, OT, Automation]*

Harmful bias and homogenization — amplified societal biases and performance gaps between groups; homogenization = outputs that become uniform, reducing diversity of content and decisions. *[AI Risk Management Program Design]*

Harms (§1.1) — to people (civil rights, safety, discrimination), to organisations (operations, reputation, legal), to ecosystems (supply chains, global financial system, natural resources). *[AI Risk Management Framework]*

Harness — Small function that feeds fuzzer-generated bytes into the code under test (for libFuzzer: LLVMFuzzerTestOneInput). *[Memory Safety and Fuzzing]*

Harrison-Ruzzo-Ullman (HRU) — Extends Graham-Denning; shows that deciding whether a right can leak is undecidable in general. *[CISSP Domain 3: Security Architecture and Engineering]*

Hash condition — SHA-256 of the file: strongest, but every update needs a new rule. *[Windows Application Control and Endpoint Monitoring]*

Hash / PRF — SHA-256, SHA-384 *[NIST Cryptography, TLS and PKI]*

Hash total — Sum of a non-financial field (e.g. account numbers) used only to detect lost or altered records in a batch. *[CISA Domain 3: IS Acquisition, Development and Implementation]*

Hash value (message digest) — Fixed-length fingerprint computed from all the bytes of an item. **SHA-256** (256 bits, 64 hex characters) is today's reference. MD5 and SHA-1 have practical collision attacks, which matter less for proving that *your* copy is unchanged, but opposing experts will raise them: record SHA-256, keep MD5 or SHA-1 only as... *[Digital Evidence and Chain of Custody]*

Hashing — One-way fixed-length digest (SHA-256). Integrity checks and password storage (salted, bcrypt/Argon2id). Cannot be reversed: it is not encryption. *[Cryptography; Data Protection and Resilience]*

Hashing vs MAC vs signature — Hash = integrity only (SHA-256); HMAC = integrity + authenticity with shared key (no non-repudiation); signature = integrity + authenticity + non-repudiation with private key. *[Cryptography Engineering and PQC]*

HCI (Hyperconverged Infrastructure) — A cluster of standard servers where software pools their local disks into shared storage and runs the VMs, removing the dedicated SAN. *[Data-Centre Architecture]*

HDO — healthcare delivery organisation: hospital, clinic or lab that operates medical devices *[IoT and Medical Device Security]*

HDS — Hebergeur de données de santé: mandatory French certification for hosting personal health data. *[Start-ups, Municipalities, Teleassistance, Open Source]*

HEAD — The current position: usually `ref: refs/heads/main` (a symbolic ref); a raw hash means detached HEAD. *[Git Internals and Repository Security; Essential Git Commands: a Working Reference]*

Head-of-line blocking — One lost TCP segment holds back every later byte of the stream until it is retransmitted; QUIC avoids it per stream. *[TCP and UDP Deep Dive]*

Header From (RFC5322.From) — What the user sees; DMARC aligns SPF and DKIM results to it. *[Phishing Analysis and Email Header Forensics; Email Security: SPF, DKIM, DMARC]*

Health Data Access Body (HDAB) — National EHDS authority that assesses applications and issues data permits for secondary use of health data. *[Data Act, Data Governance Act and EHDS]*

Hearsay — Second-hand evidence; business records made in the normal course of business are an accepted exception. *[CISSP Domain 7: Security Operations]*

Helm chart — A versioned, parameterised package of Kubernetes manifests installed, upgraded and rolled back as one release. *[Helm, operators and the CRD ecosystem (with security)]*

Help-desk impersonation — caller poses as an employee to reset password and MFA, often with personal data from breaches and a spoofed number. Mitigate: identity proofing that the attacker cannot research (video with ID, manager callback, verified push to the existing device). *[Social Engineering and Deepfakes]*

Helper / kfunc — Kernel functions a program may call (`bpf_map_lookup_elem`, `bpf_get_current_pid_tgid`); the allowed set depends on the program type. *[eBPF in Depth]*

Hextet — One of the 8 groups of 16 bits (4 hex digits) that make up an IPv6 address, separated by colons. *[IPv6 in Depth: Addressing, NDP, SLAAC, Security]*

HFDS / FSSI — Haut fonctionnaire de défense et de sécurité (senior defence official of a ministry) / his information systems security official (fonctionnaire de sécurité des SI). *[PPST Research Protection and Buying Qualified Security]*

Hibernation — Saving RAM to disk and stopping the machine: halts the malware while keeping memory contents (keys, processes) for analysis, unlike a power cut. *[Ransomware: Respond and Recover]*

HID — Human Interface Device (keyboard, mouse). A trapped USB stick presenting itself as a keyboard (BadUSB) bypasses file scanning: the profile forbids mounting anything but 'MassStorage'. *[Removable Media Airlock and White Station]*

Hidden primary — Authoritative server holding the master copy of a zone, not listed in NS records, reachable only by its secondaries. *[DNS, Wi-Fi & DDoS Architectures; ICMP, Path MTU, DHCP and DNS Operations +1]*

Hidden SSID — AP stops including the name in beacons; clients then probe for it by name everywhere, which leaks it. Not a security control. *[Wireless, Data-Center Fabrics and Cloud Networking]*

HIDPS (host-based IDPS) agents (7.1.3-7.1.4) — Critical and public servers first; they see decrypted traffic. Criteria: cost, OS support, host importance, bandwidth. Prevention via shims (interception code) on network, file, system-call and registry paths. *[Firewall Policy and IDPS Deployment]*

HIDS — Host Intrusion Detection System; file sealing (integrity checking) is one of its functions (AIDE, Tripwire, Samhain, Wazuh). *[GNU/Linux BP-028: Kernel Build, Files and Services]*

High-risk AI system — AI in Annex I products (medical devices, machinery, toys...) or Annex III areas (biometrics, critical infrastructure, education, employment, essential services, law enforcement, migration, justice); must meet Arts. 9-15. *[AI Compliance Frameworks]*

High-water mark — Rule that a system is classified at the level of the most sensitive data it holds. *[CISSP Domain 2: Asset Security]*

Hijack by more-specific — An attacker announcing a longer prefix than your summary wins every router's longest-match decision. Announce /24s for critical space and publish ROAs (Route Origin Authorizations, signed in the RPKI, Resource Public Key Infrastructure) with a maxLength so routers doing ROV (Route Origin Validation, RFC 6811) reject... *[IPv4 Addressing, Subnetting, VLSM and NAT]*

Hiring manager — the person you would report to, who decides on the hire and defines what the role really needs *[CV, Portfolio and Job Interviews in Security]*

Historian — Time-series database of process values, often replicated to IT for reporting. *[Industrial (OT/ICS) Architecture; NIST OT and IoT Security]*

HKDF — HMAC-based Key Derivation Function (RFC 5869): extract-then-expand, turns one strong secret into several independent keys labelled by an info string. *[Cryptography in Code]*

HKLM — HKEY_LOCAL_MACHINE registry hive - machine-wide settings; persistence keys HKLM\...\Run, services under HKLM\SYSTEM\CurrentControlSet\Services (Sysmon 12/13 registry events). *[CompTIA SecurityX CAS-005 - Exam Overview]*

HMAC — Hash-based message authentication code: keyed hash with a shared secret, giving integrity + authentication but no non-repudiation. Used in TOTP codes, API request signing, TLS record protection. *[Cryptography]*

HMAC-based protocol (Fig. 8-36) — Both nonces plus both identities go into one HMAC keyed with K_AB, so a reflected value never matches. Today: HMAC-SHA-256 (RFC 2104) in TLS, IPsec, JWT HS256. *[Network Security II - Authentication, Email, Web]*

HMI / EWS / MES — Human-machine interface (operator screen) / engineering workstation (programs PLCs) / manufacturing execution system (production scheduling at Level 3). *[OT Architecture and the SP 800-82r3 OT Overlay]*

HMI (human-machine interface) — Operator screen that displays process values and sends commands. *[Industrial (OT/ICS) Architecture; NIST OT and IoT Security]*

Hold-down timer — After a route goes down, ignore worse news about it for a while (180 s in RIP) so a stale path is not reinstalled. *[Routing I: Routing Table, Static Routes, OSPF]*

Holder-of-key assertion — Assertion references a key the subscriber proves possession of at the RP (mutual TLS, or DPoP-style proof-of-possession tokens); a stolen copy is useless. *[Digital Identity Guidelines SP 800-63-4]*

Holding statement — Short, pre-approved public message issued before full facts are known, to show control without speculating. *[Reporting and Communication; Crisis Communication and Tabletop Exercises]*

Homologation — Security accreditation: an authority formally accepts the residual risks of an IS before it runs. *[Protecting Essential IS - PA-085 R1 to R62; ANSSI Encryption Tools: Zed! and Cryhod (1/2, Zed!) +2]*

Homologation de securite — Formal decision by which a **business authority** (autorite d'homologation, AH) acknowledges the risks of using an information system and **accepts them**, authorising its use in production. Mandatory under the regimes listed below (RGS, PSSIE, IGI 1300, II 901, LPM, NIS rule 3); expected by NIS2 supervisors. The... *[Security Accreditation (Homologation)]*

Honeynet — Network of decoy systems used to observe attacker behaviour. *[Deception: Honeypots, Honeytokens, Canaries; CISSP Domain 7: Security Operations]*

Honeypot — A decoy system that has no production use, so any interaction is suspicious. *[Deception: Honeypots, Honey-

tokens, Canaries; CEH v13: Countermeasures by Module Family]*

Honeytoken — decoy data rather than a system: fake credential, database row, API key, document, DNS name; alerts when used. *[Deception: Honeypots, Honeytokens, Canaries]*

Hook (attach point) — Place in the kernel where a program runs: tracepoint, kprobe, fentry, uprobe, XDP, tc, cgroup, LSM hook, socket. *[eBPF in Depth]*

Hop limit 255 — Valid NDP packets are sent with hop limit 255 and receivers check it: every router decrements it, so an off-link attacker cannot inject NDP through a router (same idea as GTSM, the Generalized TTL Security Mechanism of RFC 5082 for BGP). *[IPv6 in Depth: Addressing, NDP, SLAAC, Security]*

Host-based vs network firewall — Windows Defender Firewall, nftables/firewalld protect the host from its own segment (lateral movement); network firewalls enforce zone policy. 800-41r1: use both. *[NIST Network Security Guides]*

Host key — Long-term server key pair (/etc/ssh/ssh_host_*_key) whose signature proves the client talks to the expected server and not to a man in the middle. *[SSH in Depth]*

Host OS — minimal, patched kernel *[NIST Cloud, Virtualization, and Container Security]*

Hot-swappable — SATA, SAS, USB, U.2 and Thunderbolt drives can be swapped powered on if the controller supports it; NVMe M.2 usually cannot. *[CompTIA A+ Core 1 - Hardware and Troubleshooting]*

Hot wash — immediate debrief at the end of an exercise, capturing participants' impressions before they fade *[Crisis Communication and Tabletop Exercises]*

Hot wash / RETEX — Immediate (hot) and delayed (cold) feedback collection after the exercise; the French term is retour d'experience. *[Organising a Cyber Crisis Management Exercise]*

HPACK / QPACK — Header compression schemes of HTTP/2 (RFC 7541) and HTTP/3 (RFC 9204): static and dynamic tables replace repeated header names and values by small indexes. *[Protocol Walk-Throughs at Packet Level]*

HPP — HTTP Parameter Pollution: sending the same parameter twice so front end and back end read different values. *[OWASP Web Security Testing Guide v4.2]*

HR and logistics — One person dedicated to monitoring hours and turnover, one to logistics: catering, accommodation, trans-

port, childcare, 24/7 badges, rooms, adapted digital tools. *[Cyber Crisis Management & Communication]*

HSI — Host Security ID: fwupd score from 0 to 4 summarising which firmware protections a Linux host has. *[OpenSSH Hardening and Hardware Security; Platform Firmware, BMC, DMA and USB Attacks]*

HSM — Tamper-resistant device that generates, stores and uses keys; FIPS 140-3 validated. *[PKI and ACME Certificate Automation; HTTPS Flow Inspection: Proxy and Reverse Proxy +2]*

HSM (hardware security module, automotive) — Secure core inside the ECU microcontroller (EVITA full / medium / light classes, or the smaller SHE, Secure Hardware Extension) that stores keys and runs AES, ECC and secure boot checks. *[Automotive and Embedded Security]*

HSM / KMS / TPM — Hardware Security Module (tamper-resistant key store and crypto engine) / cloud Key Management Service / Trusted Platform Module (chip in each PC holding keys and boot measurements). *[Cryptography Primer]*

HSM vs KMS vs TPM — HSM: dedicated tamper-responsive module, high throughput, quorum control. Cloud KMS (key management service): multi-tenant service usually backed by HSMs, API-driven. TPM: one per platform, few keys, slow, binds keys to that device. *[HSMs, Supply Chain, Physical Security, Decommissioning]*

HSTS — HTTP Strict Transport Security: header telling the browser to use only HTTPS for the domain. *[Browser-Side Web Security Standards; Web Server and TLS Configuration]*

HSTS preload list — List compiled into Chrome, Firefox, Safari and Edge of domains that are HTTPS-only before the first visit. *[Web Server and TLS Configuration]*

HSTS / QUIC — HTTP Strict Transport Security (header forcing browsers to use HTTPS) / UDP-based transport under HTTP/3 with TLS 1.3 built in. *[Networking Ports and Protocols]*

HTML scraping — Parse page source, comments and JS for emails, internal hostnames, versions and hidden endpoints. Passive when done on already-served content. *[Reconnaissance and OSINT]*

Hub-and-spoke — Topology where shared services and connectivity live in a central hub network that every workload (spoke) network attaches to, instead of meshing spokes together. *[Cloud Reference Architectures]*

Human-AI configuration — risks from how people and AI interact: automation bias, over-reliance, emotional attachment, anthropomorphising the system. *[AI Risk Management Program Design]*

Human and cultural factors — behaviour influences every stage *[CRISC Domain 1: Governance]*

Human element — breaches involving a non-malicious person: error, falling for social engineering, or use of stolen credentials. *[Breach and Threat Landscape 2024]*

Human risk management (HRM) — evolution of awareness that scores individual and team risk from real signals (phishing, DLP, identity events) and targets interventions accordingly *[Security Awareness and Culture Programme]*

Hunt — the same artifact collected on every client matching a label or OS, including clients that come online later, until the hunt expires. *[osquery and Velociraptor for Fleet Visibility]*

Hunt log — record per hunt: hypothesis, ATT&CK IDs, data sources, queries, findings, outcome (rule, ticket, gap, negative). The organisation's memory. *[Threat Hunting Playbooks]*

HVCI — Hypervisor-protected Code Integrity (Memory integrity): the hypervisor checks every kernel code page and forbids memory that is both writable and executable. *[Windows Privacy GPOs and VBS Deployment]*

Hybrid Azure AD join — A device joined to both on-prem AD and Entra ID, so it obeys GPO and, in the cloud, Conditional Access and Intune policy. *[On-Prem Active Directory Architecture]*

Hybrid (big.LITTLE) — **P-cores** (performance) + **E-cores** (efficiency) since Intel 12th gen (2021, Thread Director) and all ARM SoCs. Intel Core Ultra 200S (Arrow Lake, 2024) dropped Hyper-Threading on P-cores. *[CPUs, Memory, Motherboards and Buses]*

Hybrid cloud — On-premises data centre(s) connected to one cloud so workloads and data span both as one logical network. *[Hybrid, Multi-Cloud and Connectivity Architecture]*

Hybrid control — Control partly inherited and partly implemented by the system, such as an incident response policy (common) with system-specific procedures. *[Risk Management Framework (RMF)]*

Hybrid key exchange — Combining a classical ECDH secret with a post-quantum ML-KEM secret so the session stays safe if either one is broken. *[TLS, IPsec and SSH Hardening; Post-Quantum Migration Playbook +1]*

Hybrid signature — A classical and a post-quantum signature over the same data, accepted only if both verify. *[ANSSI PQC Transition: Positions and Protocols]*

Hybrid transport — CTAP 2.2 cross-device flow: a phone signs in on a nearby computer after scanning a QR code, with Bluetooth proving proximity (formerly caBLE, cloud-assisted BLE). *[Passkeys and Passwordless Authentication]*

Hypercall — Deliberate call from guest to hypervisor (VMCALL on Intel, VMCALL on AMD), the VM equivalent of a system call. *[Virtualization Internals and VM Isolation]*

Hyperjacking — A rogue hypervisor under the legitimate one, invisible to every guest. Countered by Secure Boot, TPM measured boot and remote attestation. *[ToIP and Virtualization Security]*

Hypervisor — Software (also VMM, virtual machine monitor) that creates VMs and multiplexes CPU, memory and devices between them. *[Data-Centre Architecture; Virtualization Internals and VM Isolation]*

Hypervisor cluster — A group of hosts pooled for HA and live migration (vMotion): a VM restarts elsewhere if a host dies, and moves without downtime for maintenance. *[Data-Centre Architecture]*

I

I/G bit — Least significant bit of the first octet: 0 = individual (unicast), 1 = group. 01:00:5e:xx = IPv4 multicast (low 23 bits of the group), 33:33:xx = IPv6 multicast. *[Ethernet, MAC Tables and ARP]*

IaaS / PaaS / SaaS — Infrastructure as a Service (you rent VMs, storage, networks) / Platform as a Service (you deploy code on a managed runtime) / Software as a Service (you use a finished application such as Microsoft 365). *[Security Architecture Models]*

IaaS-specific concerns (\$7.5) — legacy vulnerabilities in consumer-run OS, VM sprawl, verifying provider web site authenticity, robustness of VM isolation, dynamic network configuration for isolation, data erase practices. *[Cloud Computing Security]*

IAB — Initial Access Broker: sells footholds (VPN credentials, web shells, RDP) to ransomware affiliates. *[Threat Actor Profiles]*

IACS — International Association of Classification Societies: the class societies (DNV, Bureau Veritas, Lloyd's Register...)

whose Unified Requirements (UR) bind newbuilds. *[Cyber Security On Board Ships]*

IAL / AAL / FAL — Identity, authentication and federation assurance levels, each 1 (basic) to 3 (very high), chosen separately from an impact assessment. *[Digital Identity Guidelines SP 800-63-4]*

IAM / MFA / SSO — Identity and Access Management; Multifactor Authentication; Single Sign-On (one login, many applications). *[CompTIA CySA+ CS0-003]*

iam:PassRole — Permission to hand a role to a service (EC2, Lambda); on * it lets a low-privilege user launch compute running as an admin role. *[AWS Security Essentials]*

ICAM — Identity, Credential and Access Management: DoD's name for the full identity lifecycle, from vetting a person to revoking their access. *[DoD Zero Trust and NSA Hardening Guidance]*

ICAM (Identity, Credential and Access Management) — The processes and systems that create identities, issue credentials (passwords, certificates, keys) and grant access. *[Zero Trust Architecture SP 800-207]*

ICAP — Internet Content Adaptation Protocol: lets a proxy hand content to an antivirus or DLP (data loss prevention) engine. *[HTTPS Flow Inspection: Proxy and Reverse Proxy]*

ICMP — Internet Control Message Protocol (IP protocol 1): error and diagnostic messages (unreachable, TTL exceeded, echo) identified by a type and a code. *[IP Addressing, ICMP, DHCP and Network Triage]*

ICMP (Internet Control Message Protocol) — IP protocol 1 (ICMPv6: next header 58) that carries error reports and diagnostics; every message has a type (category) and a code (detail). *[ICMP, Path MTU, DHCP and DNS Operations]*

ID.RA-P2 bias — Data analytic inputs and outputs evaluated for bias: the hook for AI and automated decision systems, later expanded in the NIST AI RMF (MAP, MEASURE). *[NIST Privacy Framework 1.0]*

ID Token — JSON Web Token (JWT) signed as a JWS, carrying who logged in (sub, iss), for whom (aud), when (iat, exp, auth_time) and how (acr, amr). *[ANSSI Identity: MFA, AD Tiering, OpenID Connect]*

IDEAL model — Software process improvement cycle: Initiating, Diagnosing, Establishing, Acting, Learning. *[CISSP Domain 8: Software Development Security]*

Idempotent — Running the same automation twice gives the same end state and changes nothing the second time; the prop-

erty that makes re-runs and drift repair safe. *[Network Automation and Observability]*

Idempotent method — Sending the request once or ten times leaves the server in the same state (PUT, DELETE and all safe methods); clients may retry it after a network error. *[How the Web Works for Security People]*

Identification — Claiming an identity (user ID); authentication proves it, authorisation grants rights, accountability logs use. *[CISA Domain 5: Protection of Information Assets; Fundamental Security Concepts]*

Identify the problem — question user, recent changes, back up first *[Hardware: Self-Assessment]*

Identity concealment — 5G SA with SUCI enabled, null scheme disabled *[Telecom and 5G Security]*

Identity (IAL) — who you are: proofing strength, 63A *[Digital Identity Guidelines SP 800-63-4]*

Identity proofing — Verifying that a claimed identity belongs to the real person before issuing credentials (NIST IAL). *[CISSP Domain 5: Identity and Access Management; Security Engineering - IAM, Endpoints, Network, Hardware, OT, Automation]*

IDMZ — industrial demilitarised zone between IT and OT (level 3.5): no flow crosses it directly, every exchange is relayed. *[ANSSI ICS/SCADA Security]*

IDOR — Insecure Direct Object Reference: changing an id in a request returns another user's record. *[Host and Web Application Attacks; Web Application Assessment +1]*

IDP — Identity Provider: the service that authenticates users and issues tokens (Microsoft Entra ID, Okta); its sign-in logs are a key detection source. *[SIEM and Detection Engineering]*

IDP / OP — Identity provider (SAML) / OpenID provider: authenticates the user, issues assertions or tokens. *[Identity Protocols: OAuth, OIDC, SAML, FIDO2]*

IDP / RP — Identity provider: authenticates the subscriber and issues assertions. Relying party: the service that consumes the assertion or the authentication result. *[Digital Identity Guidelines SP 800-63-4]*

IDPS (intrusion detection and prevention system) — Sensors or agents that detect attacks (IDS) and optionally block them inline (IPS). *[Firewall Policy and IDPS Deployment]*

IDS / IPS — Intrusion Detection System (watches a copy of traffic and alerts) / Intrusion Prevention System (sits inline and can drop packets). *[Network Traffic Analysis: Zeek and Suricata]*

IDS / IPS / IDPS — An intrusion detection system monitors events and alerts on possible incidents; an intrusion prevention system can also try to stop them. SP 800-94 calls both IDPS. *[Firewall Policy Management and IDS/IPS]*

IDS vs IPS — An Intrusion Detection System watches a copy of traffic and alerts; an Intrusion Prevention System sits inline and can drop. IDS never delays traffic; IPS can, and a false positive there blocks users. *[Classic Enterprise Network Architecture]*

IGC / PKI — Infrastructure de gestion de clés: public key infrastructure issuing machine and user certificates. *[Remote Work (Digital Nomadism)*]

IGI 1300 — General interministerial instruction 1300 on the protection of national defence classified information. *[Start-ups, Municipalities, Teleassistance, Open Source; Security Accreditation (Homologation) +1]*

IGMP (Internet Group Management Protocol) — Hosts tell their local router which groups they want: v2 joins any source (*,G) and has leave messages; v3 (RFC 3376) adds source filtering for SSM. IPv6 equivalent: MLDv1/v2. *[QoS, Multicast and WAN Services]*

IGMP snooping — The switch listens to IGMP joins and forwards group traffic only to ports that asked, instead of flooding it like broadcast to the whole VLAN. *[QoS, Multicast and WAN Services]*

IGTK — Integrity Group Temporal Key: protects broadcast management frames (deauthentication, disassociation) under PMF with the BIP integrity algorithm. *[Wi-Fi Security Internals]*

II 901 — Interministerial instruction no. 901 on the protection of sensitive and DR information systems. *[PPST Research Protection and Buying Qualified Security; Multi-Environment Workstation and Refurbishing +2]*

II 901 / DR — Interministerial instruction 901 protecting Diffusion Restreinte (restricted, non-classified sensitive) information systems. *[Start-ups, Municipalities, Teleassistance, Open Source]*

IID (Interface Identifier) — The low 64 bits of a unicast address, identifying the interface inside its /64 subnet. *[IPv6 in Depth: Addressing, NDP, SLAAC, Security]*

IIoT chain — collection (IIoT sensor, radio link such as Zigbee or LoRaWAN, local concentration point), transport (networks, intermediate concentrators), central storage and processing (data lake, AI analytics, visualisation). *[ANSSI IoT and IIoT Recommendations]*

IIoT (ISO 24591-1:2024, 3.1.7) — industrial infrastructure of interconnected entities, people, systems and information sources with services that process and react to physical and virtual world data. *[ANSSI IoT and IIoT Recommendations]*

IKE — Internet Key Exchange (UDP 500, NAT-T 4500): negotiates SAs; IKEv2 is current. *[CISSP Domain 4: Communication and Network Security]*

IKE (Internet Key Exchange) — Protocol that authenticates the peers and negotiates SAs; IKEv2 (RFC 7296) is the recommended version. *[VPN and Firewall Security]*

IKEv2 — Internet Key Exchange v2, the IPsec handshake that authenticates peers and negotiates SAs (UDP 500/4500). *[TLS, IPsec and SSH Hardening]*

Illicit consent grant — Phishing that tricks a user into consenting to a malicious OAuth app, which then reads mail or files with a refresh token and no password. *[Azure and Entra ID Security Essentials]*

Image — the executable or DLL file a process or module was loaded from; 'image path' = where it lives on disk. *[Docker and Containers Hands-On; Container and Virtualization Security +1]*

Image and snapshot management (§3.3) — Images and snapshots contain credentials and memory; store encrypted, control access, patch dormant images before use, record provenance. *[Container and Virtualization Security]*

IMDS — Instance Metadata Service at 169.254.169.254: gives a VM its temporary role credentials; v2 requires a session token. *[AWS Security Essentials; Cloud Configuration Review +1]*

IMDSv2 — AWS Instance Metadata Service v2: requires a session token from a PUT request, which blocks most SSRF credential theft. *[OWASP API Security Top 10 - 2023]*

Immutable backup — A recovery point that cannot be modified or deleted before its retention date, even by an administrator of the backup system. *[Backup and Recovery Engineering; Ransomware Defense End to End]*

Immutable backups — offline copy with separate credentials beats replication for ransomware *[Business Continuity and ISO 22301]*

immutable or offline — one copy an attacker with admin rights cannot delete *[Emerging Topics: Self-Assessment]*

IMO — International Maritime Organization: UN agency setting ship safety rules; its Maritime Safety Committee (MSC) adopted the cyber resolution. *[Cyber Security On Board Ships]*

Impersonation patterns — Display-name spoofing (name right, address wrong), lookalike domain (acme-pay.co vs .com), Reply-To to a free mailbox, compromised real account (all checks pass - look at content and history). *[Security Tools and Techniques]*

imphash — MD5 of the ordered, lower-cased `dll.function` import list (Mandiant, 2014): rebuilt samples of one family share it although file hashes differ; used to cluster malware in Virus-Total and EDR (Endpoint Detection and Response). Linux analogue: **telfhash**. Useless on packed files (every UPX stub looks alike). *[Windows Endpoint Telemetry and Sysmon; Executable Formats: ELF and PE]*

Implementation Example — New in 2.0: concise, action-oriented illustrations of how a Subcategory can be achieved. Not exhaustive, not a checklist. *[NIST Cybersecurity Framework 2.0; CSF 2.0 Core: the 106 Outcomes Explained]*

Implementation (the how) — The concrete measures chosen to reach the barrier's objective. *[Defence in Depth & Secure Internet Gateway]*

Implicit rejection — ML-KEM decapsulation of an invalid ciphertext returns a pseudo-random secret instead of an error, avoiding chosen-ciphertext oracles *[Quantum-Safe Network Protocols: Status]*

Implicit rule — Flow allowed by a vendor default that does not appear in the rule list (management access, DNS or VPN helper rules); ANSSI asks to disable them. *[Firewall Policy Management and IDS/IPS]*

Implicit rules — Hidden, pre-enabled filter rules (e.g. admin access from internal interfaces, outbound flows of the appliance's own services) applied before the visible policy. *[Stormshield SNS 3.7.17 Hardening by Chapter]*

Implicit TLS — TLS before any protocol byte, dedicated port (465, 990, 993, 995, 636). *[Networking Ports and Protocols]*

Implicit trust zone — The (small) area behind a PEP where traffic is trusted after the decision; zero trust shrinks it toward a single session to one resource. *[Zero-Trust Architecture]*

Important entity (IE) — Any other in-scope NIS2 entity; same measures and reporting, reactive (ex post) supervision and EUR 7 M / 1.4 % fines. *[NIS2 Directive: EU-wide Obligations]*

Improve with data — telemetry feeds policy *[Zero Trust Architecture SP 800-207]*

Imputability — Ability to attribute every privileged action to one named person (BP-028 R33): named admin accounts, root dis-

abled, sudo and auditd logs. *[ANSSI GNU/Linux Hardening Deep Dive (BP-028 R1-R49)]*

Imputation vs attribution — Imputation is the technical link of an attack to a known *modus operandi* or group; attribution is the political decision, taken at the highest State level, to name the responsible actor. *[Incident Qualification & Remediation Decision Keys]*

IMSI catcher — Fake base station that lures phones, often forcing 2G without mutual authentication, to track or intercept them. *[Mobile Device Security and MDM; Telecom and 5G Security]*

IMSI / SUPI — International Mobile Subscriber Identity, the permanent SIM identity (country code + network code + subscriber number); called SUPI (Subscription Permanent Identifier) in 5G. *[Telecom and 5G Security]*

in-toto — CNCF framework and format for attestations: a Statement names subjects by digest and carries a typed predicate. *[Software Supply Chain Security]*

Inbox rules — delete or move rules hiding replies *[Microsoft 365 Hardening]*

Incidence rate — Share of tested applications that had at least one CWE of the category (not the number of findings). *[OWASP Top 10 - Web (2021 and 2025)]*

Incident — Unplanned interruption or quality reduction of an IT service; incident management restores service as fast as possible. *[SOC Operations and SOAR; CRISC Domain 4: Information Technology and Security]*

Incident response — 20 % - frameworks, detection, containment, preparation, post-incident *[CompTIA CySA+ CS0-003]*

Incident vs breach — incident = any security event compromising confidentiality, integrity or availability; breach = incident with confirmed disclosure of data to an unauthorised party. *[Breach and Threat Landscape 2024]*

IND-CCA / EUF-CMA — Standard security goals: ciphertexts reveal nothing even to an attacker with a decryption oracle; signatures cannot be forged even after seeing chosen-message signatures. *[ANSSI Cryptographic Mechanisms and PQC]*

Independent expert — Expert required by the CNIL deliberation who audits the voting solution before the poll. *[Internet Voting for Non-Political Elections]*

Indicator of compromise (IoC) — Observable evidence that an attack happened or is under way: a file hash, a malicious IP address or domain, a registry key, an unusual log event or be-

haviour. Objective 2.4 asks you to read such indicators in a scenario and name the attack. *[Malware, Attacks and Indicators]*

Indicators of compromise — Precursor = sign an incident may occur (scan, new exploit published); indicator = sign it has occurred or is occurring (alert, hash, C2 beacon). Correlate across the SIEM (central log platform), EDR (endpoint agent) and threat intelligence (TI). *[Incident Response and Management]*

Indirect PPE (I-PPE) — The pipeline file is protected, but it calls files the attacker can change: Makefile, test scripts, package.json scripts, linters' config. *[CI/CD Pipeline Security]*

Indirect prompt injection — Instructions hidden in content the model reads (web page, file, email) hijack it on behalf of a third party. *[OWASP LLM Top 10 v1.1 (2023) and the 2025 Shift]*

Individual contributor (IC) track — career path where seniority grows through technical depth and scope (senior, staff, principal) without managing people *[Career Map of Cyber Security Roles]*

Industry / organizational impact — Regulated sector, safety impact, contractual SLAs, reputational exposure: the same CVE ranks differently in a hospital and a blog. *[Vulnerability Management and Monitoring]*

Industry-specific compliance — Objective 1.3 names health-care (HIPAA), financial (PCI DSS, SOX, GLBA = US Gramm-Leach-Bliley Act for customer financial data, DORA), government (FedRAMP, FISMA = US federal agency security law, CMMC = Cybersecurity Maturity Model Certification for defense contractors), utilities (NERC CIP = North American bulk. . .) *[Compliance, Threat Modeling and AI Security]*

Inference — deducing an attribute of a person with significant probability from other values; third test *[CISSP Domain 8: Software Development Security; Privacy Engineering and PETs]*

Info disclosure — confidentiality *[CompTIA PenTest+ PT0-003]*

info (Texinfo) — GNU's hyperlinked manual format, organised as a tree of nodes with menus; many GNU tools put their short reference in `man` and their full manual in `info`. *[Read the Manual: man, help, tldr and info]*

Infogérance — IT outsourcing: a provider runs all or part of the IS under a multi-year contract with defined service levels

(AFNOR Z 67-801-1). *[IT Usage Charter and Outsourcing Security]*

Information assurance (IA) — Assurance that information and systems keep integrity, availability, confidentiality and authenticity, through policy, controls and training. *[CEH v13: Core Concepts, Phases and Legal Framework]*

Information disclosure — Any leak that helps an attacker: verbose errors, stack traces, server headers, comments, metadata (EXIF in images, author names in documents). *[DevSecOps and Supply-Chain Security; CISSP Domain 1: Security and Risk Management +6]*

Information disclosure → confidentiality — encryption, secrets vault, segmentation, tokenisation *[Secure Architecture Patterns]*

Information integrity — cheap generation of content that blurs fact and fiction: deepfakes, mis- and disinformation at scale. *[AI Risk Management Program Design]*

Information security — lowers the bar for attackers (vulnerability discovery, malicious code) and widens the attack surface of AI systems (prompt injection, data poisoning). *[AI Risk Management Program Design]*

Information security governance — The board and executive system that sets direction, accountability and oversight so security supports business objectives and risk stays within appetite. *[CISM Domain 1: Information Security Governance]*

Information security program — The set of projects, activities, resources and controls that executes the security strategy over time. *[CISM Domain 3: Information Security Program]*

Information security steering committee — Cross-functional senior group that prioritizes security initiatives, resolves conflicts and secures buy-in. *[CISM Domain 1: Information Security Governance]*

Informatique de l'ombre / Shadow IT — IS built and run inside an organisation without approval of the IT department (DSI). *[ANSSI CyberDico FR/EN Glossary]*

Informative Reference — Mapping from a Subcategory to a clause of another standard (SP 800-53r5 control, ISO/IEC 27001 Annex A control, CIS Control), published in the CPRT (Cybersecurity and Privacy Reference Tool). *[NIST Cybersecurity Framework 2.0; CSF 2.0 Core: the 106 Outcomes Explained]*

Informer — Client-side cache fed by one LIST then a WATCH stream; controllers read the cache, not etcd, to keep API load low. *[Kubernetes Architecture in Depth]*

Infostealer — malware that harvests saved passwords, cookies and tokens from a browser and sends them to criminals who resell them. *[Data Protection: Classification, Leaks, GDPR; Browser and Extension Security]*

Infostealers +266% — feed the credential market *[IBM Breach Cost and X-Force Index 2024]*

Infrared (PIR) — passive infrared: body heat and motion; indoor, misses objects at room temperature *[Fundamental Security Concepts]*

Ingress — HTTP(S) routing rules (host/path -> Service); needs an Ingress controller (e.g. ingress-nginx) actually installed to do anything. *[Kubernetes hands-on: learn it in your own lab]*

Inherent risk — Risk level before any control is considered. *[CISA Domain 1: Information System Auditing Process; CISM Domain 2: Information Security Risk Management +3]*

Inherent vs residual risk — Risk before any control vs risk left after controls. Residual risk is what the owner accepts, transfers or treats further; it must sit within appetite. *[Governance, Risk and Third-Party Management]*

Inheritable / ambient sets — What survives `execve`: inheritable only with matching file caps, ambient even for plain binaries. *[Linux Isolation Primitives and Sandboxes]*

Initial access broker — criminal who sells footholds (stolen VPN credentials, web shells) to ransomware affiliates. *[CISA #StopRansomware Guide]*

Initial access broker (IAB) — Criminal who breaks in or buys credentials and sells the foothold to ransomware affiliates. *[Ransomware Defense End to End]*

initramfs (initial RAM filesystem) — Compressed `cpio` archive the kernel unpacks into memory at boot; holds drivers, LUKS and LVM tools to reach the real root. Not signed in a classic GRUB setup. *[Linux Boot, Processes and System Calls]*

Inject — Piece of scenario sent by the moderating unit to the players (email, call, SMS, fake article) to steer their actions. *[Organising a Cyber Crisis Management Exercise; Crisis Communication and Tabletop Exercises]*

Injected RST — A TCP reset forged by a middlebox; its IP TTL or ID differs from the real peer's packets. *[Operations, Security, Troubleshooting: Self-Assessment]*

Inline vs passive — Inline sensors sit in the traffic path and can block (IPS); passive sensors receive a copy from a SPAN port or TAP and can only alert or send resets. *[Firewall Policy Management and IDS/IPS]*

Inno (innocuity check) — anti-malware scan of transferred data, ideally with the same policies and supervision as the OT side. **[ANSSI ICS Detailed Measures v2 (2/2): technical measures]**

Innocuity control — Check that incoming data is harmless: antiviruses, format and structure validation, active content removal. **[Multilevel Interconnections & Trusted Core]**

Inode — Unix filesystem record holding a file's metadata (type, permissions, owner, size, timestamps, block pointers or extents) but not its name; names live in directory entries. **[Storage and Filesystems for Defenders]**

Inside local / inside global — Cisco NAT names for an internal host's real private address and the public address (and port) it is translated to. **[Cisco IOS Configuration Lab]**

Insider risk management — the broader, less accusatory framing (used by Microsoft Purview and CERT): manage risky behaviour before it becomes an incident. **[Insider Threat Program]**

Insider threat — The risk that a person with authorised access (employee, contractor, partner, former staff whose access was not removed) uses that access or inside knowledge, intentionally or not, to harm the organisation's people, data, systems or reputation. **[Insider Threat Program; Threat Actors and Threat Vectors]**

Instant recovery — Running a VM directly from the backup file mounted as a datastore, then migrating it to production storage while users work. **[Backup and Recovery Engineering]**

Insurance — Activated by the strategic unit on pre-established criteria; expertise obtainable through the policy identified; summary of events formalised for the insurer. **[Cyber Crisis Management & Communication]**

Integer overflow / wrap — arithmetic exceeding the type's range: remove every possible signed overflow (R105), detect unsigned wraps (R106), remove division by zero (R107); sizes computed before malloc are the classic victim. **[Secure Coding in C and Rust, CMS and JRE Hardening]**

Integration test — Tests interfaces and data passed between modules. **[CISA Domain 3: IS Acquisition, Development and Implementation]**

Integrity — Data and systems are changed only in authorized ways; countered by alteration. **[CISSP Domain 1: Security and Risk Management]**

Integrity and confidentiality — Art. 5(1)(f): appropriate security, the security team's principle **[GDPR for Security Teams]**

Integrity level — Windows trust label on a process token (Low, Medium, High = elevated admin, System); shown in Process Explorer's Security tab. **[Sysinternals Suite for Windows Administrators]**

Integrity of the monitor — tasks cannot modify it or its policies; it runs at a higher privilege (R20.2, R21) **[System Partitioning: ANSSI PG-040]**

Intel CSME / AMT — Management Engine: separate processor in the chipset running its own OS below ring 0. **AMT** (Active Management Technology, part of vPro) adds remote KVM (keyboard-video-mouse), power control and disk redirection over ports 16992-16995. INTEL-SA-00075 (CVE-2017-5689, May 2017) let an empty digest authenticate to... **[Platform Firmware, BMC, DMA and USB Attacks]**

Intel SGX (Software Guard Extensions) — since 2015; enclave pages live in the EPC (Enclave Page Cache); removed from client CPUs from 11th/12th gen Core, kept on Xeon; scalable SGX (Ice Lake Xeon, 2021) raised EPC to hundreds of GB but dropped the integrity tree (replay protection) **[Confidential Computing and Remote Attestation]**

Intel sharing consumers — Incident response (scope, attribution), vulnerability management (what is exploited), risk management (actor likelihood), security engineering (controls), detection and monitoring (rules). **[Threat Intelligence, Hunting and SOC Efficiency]**

Intel TDX (Trust Domain Extensions) — VM TEE on 4th gen Xeon (Sapphire Rapids, limited) and 5th gen (Emerald Rapids, 2023, general); a signed TDX module running in SEAM (Secure Arbitration Mode) mediates between the VMM and trust domains **[Confidential Computing and Remote Attestation]**

Intellectual property — reproduction of copyrighted, trademarked or licensed content without authorisation; exposure of trade secrets. **[AI Risk Management Program Design]**

Intelligence-driven defense — Detection in any phase lets analysts infer earlier phases; one mitigation anywhere breaks the chain. **[Pentest Methodologies]**

Intelligence gap — An EOI no current source can answer; drives new collection or partnerships. **[Cyber Threat Intelligence Lifecycle]**

Intent-based networking — Operators state business goals ("guests never reach finance"); the system translates, deploys and continuously checks that the network still satisfies them (RFC 9315, 2022). **[Network Automation and Observability]**

Interactive intrusion — hands-on-keyboard activity by a human operator rather than automated malware. **[Vendor Threat Reports: Identity, Endpoint, IR]**

Intercepting proxy — Tool between browser and server (Burp Suite, ZAP) that records and lets the tester replay or modify requests. **[Web Application Assessment; Web and API Testing Toolkit for Your Own Apps]**

Intercommunalite — Public body grouping several communes (communaute de communes, d'agglomeration, urbaine, metropole) to run shared services. **[Start-ups, Municipalities, Teleassistance, Open Source]**

Interface — A set of method signatures; satisfied implicitly by any type implementing them. io.Reader (one method Read) and error (one method Error) are the classics. **[Go Programming from Zero (Part 1: language basics)]**

Interface resets / flapping — Keepalive failures, bad optic, autonegotiation fights; check %LINK-3-UPDOWN frequency in syslog. **[Network Troubleshooting: Method, Layers, Tools, Symptoms]**

Intermittent encryption — Only parts of each file are encrypted (LockBit, BlackCat): faster, harder to detect by I/O volume; recovery still impossible without the key. **[Ransomware: Anatomy, Detection, Prevention]**

Internal and external monitoring — Internal: control self-assessments, compliance team spot checks, continuous control monitoring. External: regulator examinations, auditor testing, customer audits. **[Compliance, Audits and Security Awareness]**

Internal audit — Audit by the organisation's own audit function, reporting to the board or audit committee to stay independent of IT. **[CISSP Domain 6: Security Assessment and Testing]**

Internal: audit committee — Board sub-committee that keeps internal audit independent, approves the audit plan and receives results. **[Compliance, Audits and Security Awareness]**

Internal: compliance — Second-line team checks that policies and regulations are followed; findings tracked to closure. **[Compliance, Audits and Security Awareness]**

Internal interface — Interface flagged as protected (shield icon): anti-spoofing only accepts sources from its own or routed subnets. **[Stormshield SNS 3.7.17 Hardening by Chapter]**

Internal: self-assessments — Control owners answer questionnaires and gather evidence before the real audit (PCI SAQ, CIS Controls self-scoring against the Center for Internet Security list). **[Compliance, Audits and Security Awareness]**

Interoperability — Choose standard protocols (SAML, OIDC, SCIM, LDAP) so directories, IdPs and apps from different vendors work together; avoid proprietary connectors that block migration. *[Identity and Access Management; Security Architecture - Resilience, Controls, Zero Trust]*

INTERPOL African Cyberthreat Assessment 2024 — 3rd edition, April 2024, by INTERPOL's African Joint Operation against Cybercrime (AFJOC). Top threats reported by African member countries in 2023: **ransomware**, **BEC**, **online scams**; ransomware hit critical infrastructure in nearly half of surveyed countries (African Union attacked by BlackCat in 2023). *[Edge, Readiness and Awareness Reports]*

Interpreter — The `python3` program that reads your source code and executes it line by line; no separate compile step. *[Python for Security from Zero]*

Interrupt — A hardware signal (timer tick, key press, packet arrival) that makes the CPU pause the current work and run kernel code. *[Operating System Concepts for Beginners]*

Interruption window — Time the organisation can wait from failure to restoring critical services before losses become unacceptable. *[CISA Domain 4: IS Operations and Business Resilience]*

Interview — Talk to the people who run the control to confirm they know and apply it. *[SP 800-53r5 Key Controls Explained]*

Intimidation / urgency — deadline, penalty, account closed *[Social Engineering and Phishing Simulation]*

IntServ / RSVP — Per-flow reservation signalled end to end with RSVP (Resource Reservation Protocol); precise but does not scale to the Internet core; survives in MPLS traffic engineering. *[QoS, Multicast and WAN Services]*

Investigation — Acquisition of technical knowledge on an incident to understand its impacts, identify the compromised perimeter and make the right choices, notably for remediation. *[Incident Qualification & Remediation Decision Keys]*

Involve owners — the business owns risk and data; senior management approves *[CISM Exam Strategy]*

IoC — Indicator of compromise: an artifact (hash, IP, domain) showing an intrusion. *[Threat Hunting Playbooks; Cyber Threat Intelligence Lifecycle +1]*

IoC / IoA — Indicator of Compromise (evidence left after the fact) / Indicator of Attack (behaviour observed while the attack runs). *[CySA+ Practice Scenarios]*

IOC vs TTP — an IOC is an observable (hash, IP, domain, mutex); a TTP is the behaviour behind it. Share both, act on TTPs. *[Malware Triage and Analysis]*

IOMMU — Input-output memory management unit (Intel VT-d, AMD-Vi): translates and restricts device DMA addresses per domain, so a passed-through device reaches only its VM's memory. *[ANSSI GNU/Linux Hardening Deep Dive (BP-028 R1-R49); Virtualization Internals and VM Isolation +1]*

IOMMU group — Smallest set of devices the IOMMU can isolate from each other; all devices of a group must be passed to the same VM. *[Virtualization Internals and VM Isolation]*

IP config — `ipconfig /all`: valid IP, mask, gateway, no 169.254 *[CompTIA A+ Core 1 - Networking, SOHO, Network Troubleshooting]*

IP Source Guard (IPSG) — Drops IP packets whose source address is not the one bound to that port. *[Network Equipment Hardening]*

IPAM — IP address management: single source of truth for prefixes and leases; often bundled as **DDI** (DNS + DHCP + IPAM). Open source: NetBox, phpIPAM; commercial: Infoblox, BlueCat, EfficientIP. *[Network Operations: Documentation, Monitoring, Resilience]*

IPBX / call server — IP private branch exchange: the company switch that registers phones, routes calls and hosts voicemail. *[ToIP and Virtualization Security]*

IPC — Inter-process communication: intents, content providers, URL schemes and app links through which apps talk to each other. *[OWASP Mobile - Top 10 2024, MASVS v2.1, MASTG]*

IPComp — IP payload compression applied before encryption (encrypted data no longer compresses). *[VPN Planning, Design and Operations]*

IPD / 2PD / FPD — Initial, second and final public draft: open for comments, not to be cited as a requirement; content can still change. *[NIST Cyber Publications 2024-2026 Roundup]*

IPMI — Intelligent Platform Management Interface: legacy BMC protocol on UDP 623, weak by design (RAKP hash leak). *[Platform Firmware, BMC, DMA and USB Attacks]*

IPsec — IETF suite that authenticates and encrypts IP packets at layer 3; every protocol above IP (TCP, UDP, ICMP) is protected transparently. *[VPN and Firewall Security]*

IPsec (IP Security) — IETF suite protecting IP packets at layer 3 (RFC 4301 architecture): ESP for confidentiality and integrity, AH for integrity only, IKE to authenticate peers and

negotiate keys. *[VPNs in Depth: IPsec/IKEv2, TLS VPN, WireGuard]*

IPT (integrated product team) — Cross-functional team (dev, ops, security, business) that owns a product through its lifecycle. *[CISSP Domain 8: Software Development Security]*

IPv6 — 128-bit addresses, IPsec support built into the design, no broadcast, NDP replaces ARP; watch tunnels (6to4, Teredo) bypassing IPv4 controls. *[CISSP Domain 4: Communication and Network Security]*

IPv6 takeover (mitm6) — Rogue DHCPv6/DNS server answers Windows hosts that prefer IPv6 on an IPv4 network; fix: RA Guard and DHCPv6 Guard on switches, disable unused IPv6. *[Network and Infrastructure Assessment]*

IPX — IP Packet eXchange: private inter-operator network carrying roaming signalling and traffic; trust between thousands of parties is its weakness. *[Telecom and 5G Security]*

IR retainer — Pre-signed contract with an incident response firm guaranteeing hours and response time, so no procurement delay during a crisis. *[IR Teams, Playbooks and Lessons Learned]*

IRR (information a regime restrictif) — Information whose disclosure would significantly impact the risks that justified the ZRR. Always sensitive, so under **II 901**, and marked per the local sensitivity scale (red frames on paper, file or folder name, label on a USB key). *[PPST Research Protection and Buying Qualified Security]*

IRSA — IAM Roles for Service Accounts: EKS pods get their own AWS role via an OIDC-signed service-account token instead of the node role. *[Cloud and DevSecOps: Self-Assessment]*

IS (SI) — Information system (système d'information): the set of networks, hosts and applications being protected. *[Firewall Policy: Design, Cleanup, Exposed Zone]*

ISAC — Information Sharing and Analysis Center: sector body (finance, health, energy) where members exchange threat information. *[CompTIA CySA+ CS0-003; Incident Handling and Response]*

ISAC / CISA — Information Sharing and Analysis Center (sector intel-sharing body) / US Cybersecurity and Infrastructure Security Agency, which publishes joint advisories with TTPs. *[Threat Hunting Playbooks]*

ISACA — Professional association for audit, governance and risk; issues CISA, CISM, CRISC, CGEIT and CDPSE. *[Security Certification Landscape]*

ISC2 — Non-profit that issues CISSP, CCSP, SSCP, CC and the CISSP concentrations (ISSAP, ISSEP, ISSMP). *[Security Certification Landscape]*

ISCM — Information security continuous monitoring (NIST SP 800-137): ongoing awareness of vulnerabilities and threats. *[CISSP Domain 6: Security Assessment and Testing]*

ISM / SMS — International Safety Management Code, which requires each company to run a Safety Management System (SMS) of written procedures. *[Cyber Security On Board Ships]*

ISMS — Information security management system: the policies, processes, roles and records an organisation uses to manage information risk (ISO 27001 clauses 4-10). *[ISO/IEC 27001:2022 and 27002:2022]*

ISO/IEC 17024 — Standard for bodies that certify persons; CISSP, CISM, CISA, CRISC, CEH and the CompTIA security exams are accredited under it (check each issuer). *[Security Certification Landscape]*

ISO/IEC 27001:2022 — International standard for an ISMS (information security management system), certifiable by an accredited auditor; its Annex A lists 93 controls. *[CompTIA Security+ SY0-701]*

ISO/IEC 27037 processes — International guideline for identification, collection, acquisition and preservation of digital evidence; the four processes a first responder follows. *[Digital Forensics in Incident Response]*

ISSP (PSSI) — information systems security policy (politique de securite des systemes d'information): the top-level document of rules and responsibilities. *[Digital Risk Governance - ANSSI-AMRAE 15 Steps]*

Issue — Realised problem or control failure that needs action now, tracked to closure (unlike a risk, it has already occurred). *[CRISC Domain 3: Risk Response and Reporting]*

IT general controls (ITGC) — Controls over the IT environment that support every application: access, change, development and operations. If ITGCs fail, the auditor cannot rely on automated application controls and must expand substantive testing. SOC 2 common criteria test the same ground: CC6 logical and physical access, CC7 system operations... *[CISA Domain 4: IS Operations and Business Resilience]*

IT risk — Business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise (ISACA Risk IT definition). *[CRISC Domain 1: Governance]*

ITDR — Identity Threat Detection and Response: detections and playbooks on identity-provider, directory and SaaS sign-in logs. *[Security Outlook 2026]*

ITDR (Identity Threat Detection and Response) — Detection of attacks on identity systems: token replay, MFA fatigue, impossible travel, privilege escalation in the IdP. *[SaaS Security and Google Workspace]*

ITGC — IT general controls: controls over access, change management, operations and development that apply to all applications and support application controls. *[CISA Domain 1: Information System Auditing Process]*

ITSEF — Information Technology Security Evaluation Facility: lab licensed by ANSSI to evaluate products for a CC or CSPN certificate. *[ANSSI PQC Transition: Positions and Protocols]*

IXP — Internet exchange point: shared switching fabric where many operators peer. *[BGP, 802.1X & VPN]*

J

JA3 / JA4 — fingerprints of how a TLS client builds its ClientHello (version, ciphers, extensions); JA3 = MD5 of those fields, JA4 = readable, sorted successor (FoxIO, 2023). *[Network Traffic Analysis: Zeek and Suricata]*

Jailbreak — Exploit chain that disables code-signature enforcement and sandbox checks on a device, letting unsigned code and hooking frameworks run. As with Android rooting, the app cannot prevent it; only server-side attestation (App Attest) reduces trust in such a device. *[AI Monitoring, Attacks and Compensating Controls; LLM Application Security Testing +1]*

JEDEC — Standards body that defines DRAM generations, speeds and module formats. *[CPUs, Memory, Motherboards and Buses]*

Job — a pipeline started from an interactive shell, numbered %1, %2, which can be stopped, resumed in the background or brought to the foreground. *[Shell and Terminal Productivity on Every OS]*

Job boards — Job ads name the exact products a company runs (firewall brand, EDR, cloud, ERP version) and the teams it is hiring for - a free technology inventory. *[Reconnaissance and OSINT]*

Job practice — ISACA's name for the exam outline: domains, weights and task statements derived from a survey of practitioners. *[Security Certification Landscape]*

job_workflow_ref — Claim naming the reusable workflow file and ref that runs the job; pin it to force deployments through a central workflow. *[CI/CD Pipeline Security]*

Journal — Write-ahead log of pending filesystem changes so a crash can be replayed to a consistent state; also a forensic record of recent activity. *[Storage and Filesystems for Defenders]*

journald / rsyslog — systemd's binary log store (read with journalctl) / the classic syslog daemon that writes text files and forwards logs over the network (TCP 6514 with TLS). *[Linux and Cloud Logging]*

jq — Command-line JSON processor: a **filter** reads JSON values and emits JSON values, and filters chain with | exactly like a shell pipeline, but on structured objects instead of lines. `.Records[]` iterates an array, `select(cond)` keeps matching objects, `-r` prints raw strings, `-c` one compact object per line... *[Defender Scripting Toolkit]*

Just culture — environment where honest errors are reported without blame, while reckless or malicious acts remain accountable *[Security Awareness and Culture Programme; Working Life in Security]*

Just-in-time access (JIT) — Privilege granted on request for a limited time, with justification and often approval, then removed automatically. *[Cloud Entitlement Management and Least Privilege]*

Just-in-time (JIT) access — Privilege granted only for the time a task needs, then removed automatically. *[CISSP Domain 5: Identity and Access Management]*

Just-in-time permissions — No standing admin rights. Elevation requested with justification, approved, granted for a window (1-8 h), then removed automatically: Microsoft Entra PIM (Privileged Identity Management), AWS IAM Identity Center permission sets, CyberArk, BeyondTrust. *[Identity and Access Management]*

JWT — JSON Web Token: signed (JWS) set of claims such as sub, exp, aud, iss, sent as a bearer token. *[OWASP API Security Top 10 - 2023]*

JWT (JSON Web Token) — RFC 7519: `base64url(header).base64url(claims).signature`. The header names the algorithm (alg) and key (kid); claims include iss issuer, sub subject, aud audience, exp expiry, nbf not before, jti token id. Signed (JWS) tokens are readable by anyone: never put secrets in claims. *[Authentication and Session Design]*

JWT / RCE — JSON Web Token is a signed claims token (alg=none must be rejected); Remote Code Execution is attacker code running on the server - the highest-impact web outcome. *[Host and Web Application Attacks]*

K

KCC / ISTG — The Knowledge Consistency Checker builds the replication connections automatically; the Inter-Site Topology Generator picks the bridgehead DCs between sites. *[On-Prem Active Directory Architecture]*

KCI — Key control indicator: shows whether a control operates as designed and covers its scope. *[CRISC Domain 3: Risk Response and Reporting; Security Metrics and Board Reporting +1]*

KCI (Key Control Indicator) — measures whether a specific control works (share of backups restored successfully in tests) *[Building a Security Program]*

KDC — Kerberos Key Distribution Center (on every domain controller): answers AS-REQ (login, returns a TGT, ticket-granting ticket) and TGS-REQ (service ticket requests). *[Networking Ports and Protocols]*

KDC (Key Distribution Center) — Kerberos service on each domain controller, made of the Authentication Service (issues TGTs) and the Ticket-Granting Service (issues service tickets). *[Active Directory Tiering and Kerberos in Depth]*

KDF — Key derivation function: slow, salted hash (argon2id, scrypt, bcrypt, PBKDF2) used to store passwords. *[Crypto Mechanisms, Key Policy and AES Internals; ASVS 5.0 - Chapter Highlights and 4.0.3 Delta]*

KDF / HKDF — Key Derivation Function: turns a secret (password or shared key) into one or more keys; HKDF = HMAC-based KDF (RFC 5869) used in TLS 1.3. *[Cryptography Primer]*

KDF (key derivation function) — Function that turns one or more secrets into uniform keys (HKDF); used to combine hybrid secrets. *[ANSSI Cryptographic Mechanisms and PQC]*

KDS root key / gMSA — Key Distribution Service root key from which the passwords of group Managed Service Accounts (automatically rotated service accounts) are derived; stolen key = all gMSA passwords. *[Active Directory Tier 0 Remediation]*

KEM — Key encapsulation mechanism: public-key scheme that produces a random shared secret and its ciphertext (encapsu-

late), recovered with the private key (decapsulate). *[Post-Quantum Migration Playbook; Cryptography Primer]*

KEM combiner — the key derivation (KDF) step that mixes both shared secrets (in TLS: concatenation of ML-KEM and ECDH secrets fed into the key schedule) *[Quantum-Safe Network Protocols: Status]*

KEM (key encapsulation mechanism) — Public-key primitive that produces a fresh shared secret and a ciphertext only the private-key holder can open (ML-KEM, ECIES-KEM). *[ANSSI Cryptographic Mechanisms and PQC]*

KEM = ML-KEM (FIPS 203) — key encapsulation - replaces ECDH *[Cryptography Engineering and PQC]*

Kerberoasting — Any domain user can request a service ticket (TGS) for an account that has a Service Principal Name (SPN). The ticket is encrypted with the service account's password hash, so a weak service-account password can be recovered offline. Evidence: Event ID 4769 requests, especially many at once or using legacy RC4. ... *[ANSSI Active Directory Recommendation Catalogue; Network and Authentication Attacks]*

Kerberos TGT / service ticket — a Ticket-Granting Ticket proves who you are to the KDC (on the DC); a service ticket (ST) proves it to one service. Both are encrypted with account keys derived from passwords. *[Windows and Active Directory for Defenders]*

Kerckhoffs' principle (1883) — All algorithms must be public; only the keys are secret. Hiding the algorithm is **security by obscurity**; the book's key-size rule of thumb: 64 bits for your kid brother, 128 commercial, 256 against governments. *[Network Security I - Crypto, PKI, IPsec, Firewalls, Wi-Fi]*

Kerckhoffs's principle — Security rests on the key, never on the secrecy of the algorithm. *[CISSP Domain 3: Security Architecture and Engineering; Cryptography Primer]*

Kernel — The core of the OS that runs in the CPU's privileged mode and owns the hardware, memory and the list of processes. *[Operating System Concepts for Beginners]*

Kernel callback — Function a driver registers so that Windows calls it on an event (process start, image load, handle open); the EDR's primary, tamper-resistant view. *[EDR Telemetry, Tamper and Evasion Detection]*

Kernel DMA Protection — Windows feature using the IOMMU to block external PCIe devices until the user logs in and drivers opt in. *[Platform Firmware, BMC, DMA and USB Attacks]*

Kernel lockdown — Linux Security Module (mainline since kernel 5.4, 2019) that stops root, not just normal users, from

modifying or reading the running kernel, closing the gap between a verified boot (Secure Boot) and a root compromise. *[Linux Hardening in Practice]*

Kernel taint — Bitmask in /proc/sys/kernel/tainted recording events such as loading an out-of-tree (4096) or unsigned (8192) module; 0 means untainted. *[Linux DFIR and Live Response]*

KEV — CISA Known Exploited Vulnerabilities catalogue: CVEs with confirmed exploitation, to patch first. *[Famous Vulnerabilities Explained; CISSP Domain 6: Security Assessment and Testing +6]*

KEX — SSH key exchange algorithm that derives the session keys (curve25519, hybrid post-quantum ML-KEM or sntrup761 variants). *[OpenSSH Hardening and Hardware Security]*

Key — Secret value that parameterises the cipher; security rests on the key, not on hiding the algorithm (Kerckhoffs's principle). *[Cryptography]*

Key agreement vs key transport — Agreement: both parties contribute to the key (Diffie-Hellman). Transport: one party generates the key and sends it encrypted to the other (RSA). *[Crypto Mechanisms, Key Policy and AES Internals]*

Key attestation — Certificate chain proving a key lives in secure hardware and reporting the device boot state. *[Laptops, Mobile Devices, Virtualization Hardware]*

Key attributes that matter — CKA_SENSITIVE=true (never revealed in clear), CKA_EXTRACTABLE=false (cannot be wrapped out), CKA_TOKEN=true (persistent), CKA_WRAP_WITH_TRUSTED (export only under a trusted key). Audit these: a sensitive but extractable key can be wrapped under an attacker-chosen key. *[HSMs, Supply Chain, Physical Security, Decommissioning]*

Key ceremony — A scripted, witnessed, video-recorded procedure to generate or use the root key inside the HSM. Control is split M-of-N (several custodians each hold a share; a quorum is needed to act), performed air-gapped and fully audited. Detailed in 'PKI Operations and Key Management'. *[PKI and Certificate Architecture; PKI Operations and Key Management]*

Key confirmation — Extra step proving to each party that the other derived the same key, e.g. by exchanging a MAC computed with it. *[Crypto Mechanisms, Key Policy and AES Internals]*

Key escrow — Copy of a key held by a trusted third party for recovery; recovery agents may also reconstruct keys (M of N control). *[CISSP Domain 3: Security Architecture and Engineering]*

Key escrow and recovery agent — Copies of encryption private keys held for recovery (EFS, S/MIME); never escrow signing keys (non-repudiation). *[NIST Cryptography, TLS and PKI]*

Key escrow (sequestre) — Controlled copy of keys kept by a trusted party so data can be recovered legally. *[ANSSI Crypto Rules Catalogue (PG-083 v3.00); ANSSI Encryption Tools: Zed! and Cryhod (1/2, Zed!)]*

Key exchange — ECDHE, DHE, (RSA transport: removed) *[ANSSI TLS and IPsec Guides: Full R Index; NIST Cryptography, TLS and PKI]*

Key hunt — Investigation after a complaint that seeks the attackers' decryption keys on seized servers; can lead to free decryption for victims. *[Ransomware: Respond and Recover]*

Key inventory (9.2.1) — All long-term keys SHALL be inventoried: owner, type, algorithm, length, application, expiry; a reference to the key, never the secret or private key itself (unless the inventory is also the backup). *[Crypto Mechanisms, Key Policy and AES Internals]*

Key length — Size of the key in bits; each extra bit doubles a brute-force search. Compare within the same algorithm family only (AES-128 is far stronger than RSA-1024). *[Cryptography]*

Key point / parameter — aspects of the IS measured for an objective; e.g. objective 'all servers highly available in 3 years': key points = years elapsed and number of servers, parameter = HA state of each server *[SSI Maturity and Security Dashboards]*

Key rotation and storage (3.6) — Rotation process defined by the trust agreement over an authenticated protected channel (e.g. JWKS, JSON Web Key Set URL). Non-exportable keys live in a secure element, trusted execution environment (TEE) or TPM chip separate from the host CPU. *[Proofing Evidence and FAL Requirements]*

Key separation — One key, one purpose: never sign with an encryption key. Data-encryption key (DEK) protected by a key-encryption key (KEK, wrapping) protected by a master key in an HSM. *[NIST Cryptographic Standards]*

Key signs headers — From, Date, Subject and body hash *[Security Engineering - IAM, Endpoints, Network, Hardware, OT, Automation]*

Key stretching — Deliberately slow hashing that makes every guess expensive: PBKDF2 (Password-Based Key Derivation Function 2, many iterations), bcrypt (cost factor), scrypt

and Argon2id (memory-hard). Used for password storage and password-derived keys. *[Cryptography]*

Key wear vs crypto-period — Wear is a mathematical limit on data per key; the crypto-period is an organisational maximum use time. R13 sets both a time and a volume limit. *[ANSSI TLS and IPsec Guides: Full R Index]*

Keyless signing — Sigstore signing where a short-lived certificate is issued to the CI's OIDC identity, so no long-lived signing key exists. *[Container Image and Registry Security; Software Supply Chain Security]*

Keylogger — Hardware or software capture of keystrokes for credential theft; indicator: unknown USB dongle between keyboard and PC, software hooks on keyboard input. *[Malware, Attacks and Indicators]*

Keystore / Keychain — OS-protected key and secret storage (Android Keystore, iOS Keychain, backed by TEE or Secure Enclave hardware). *[OWASP Mobile - Top 10 2024, MASVS v2.1, MASTG]*

KGI — Key goal indicator: lagging measure of whether an objective was achieved. *[CISA Domain 2: Governance and Management of IT; CISM Domain 1: Information Security Governance]*

Kibana KQL — Kibana Query Language: a simple filter syntax (`process.name : "cmd.exe"`) in the Kibana search bar; no pipes, no aggregation. Unrelated to Kusto KQL. *[Query Languages: KQL, SPL, EQL, ES|QL, osquery]*

Kill ring — readline's clipboard: text cut with Ctrl+K, Ctrl+U or Ctrl+W is pushed on it and pasted with Ctrl+Y (Alt+Y cycles older kills). *[Shell and Terminal Productivity on Every OS]*

Kill switch — Condition that makes malware stop; WannaCry halted when a hard-coded unregistered domain started to resolve. *[Landmark Incidents and Lessons]*

kind (Kubernetes IN Docker) — A tool that runs a full Kubernetes cluster inside Docker containers, one container per node; ideal for CI and throwaway labs. *[Kubernetes hands-on: learn it in your own lab]*

Kiosk-based IAL3 (4.3.8) — Formerly supervised remote identity proofing (SRIP): high-resolution video of the whole session, live remote agent for collection, validation and verification, integrated tamper-protected scanners. *[Proofing Evidence and FAL Requirements]*

KISS — Keep It Short and Simple: small, simple components are easier to review, test and prove. *[System Partitioning: ANSSI PG-040]*

KMCI / UMCI — Kernel-mode and user-mode code integrity: WDAC checks drivers and applications against the policy before they load. *[Windows Application Control and Endpoint Monitoring]*

KMI (IGC) — Key management infrastructure: a PKI plus registration, devices and revocation processes. *[ANSSI Crypto Rules Catalogue (PG-083 v3.00)]*

Knowledge (K) — A retrievable set of concepts in memory: "Knowledge of network protocols". Statement starts with **Knowledge of**. *[NICE Workforce Framework for Cybersecurity]*

KnowledgeC / Biome — Pattern-of-life stores: KnowledgeC.db (SQLite) records app focus, device lock and backlight periods; from macOS 13 / iOS 16 many streams moved to Biome (SEGB protobuf files). *[macOS and iOS Forensics for Defenders]*

Known error — Problem with a documented root cause and workaround, awaiting a permanent fix. *[CISA Domain 4: IS Operations and Business Resilience]*

known_hosts — Client file mapping host names to trusted host keys; a changed key triggers the REMOTE HOST IDENTIFICATION HAS CHANGED warning. *[SSH in Depth]*

KPI — Key performance indicator: shows how well a process performs toward a goal. *[CISA Domain 2: Governance and Management of IT; CISM Domain 1: Information Security Governance +2]*

KPI (Key Performance Indicator) — Backward-looking measure of how well a process performs, e.g. mean time to patch. *[CISSP Domain 6: Security Assessment and Testing; Building a Security Program]*

KPTI — Kernel page-table isolation: user mode runs without kernel mappings; costs a TLB (translation lookaside buffer, the address-translation cache) switch per syscall. Not needed on CPUs reporting Meltdown 'Not affected'. *[CPU Side Channels and Memory Attacks]*

KQL (Kusto Query Language) — Microsoft's read-only pipe-based query language for Sentinel, Defender XDR and Azure Data Explorer; each `|` passes rows to the next operator. *[Query Languages: KQL, SPL, EQL, ES|QL, osquery; SQL Basics for Security]*

krbtgt — Built-in account whose key signs every TGT in the domain. *[ANSSI Active Directory Recommendation Catalogue; Active Directory Security +1]*

KRI — Key risk indicator: metric that signals rising exposure before a loss. *[CISA Domain 2: Governance and Management of IT; CISM Domain 1: Information Security Governance +1]*

KRI (Key Risk Indicator) — Metric that signals a rising risk level early enough to act, compared with a threshold. *[CISM Domain 2: Information Security Risk Management; CISSP Domain 6: Security Assessment and Testing +2]*

KRI selection criteria — Impact (linked to a significant risk), effort (cheap to collect), reliability (accurate, predictive), sensitivity (moves when risk changes). *[CRISC Exam Strategy]*

KRITIS — German critical infrastructure: BSI-KritisV sets thresholds (e.g. 500,000 people served); s. 8a BSIG requires proof of state-of-the-art security every 2 years. *[NCSC, BSI and Allied Cyber Authorities]*

KRL — Key Revocation List: compact OpenSSH file of revoked keys and certificates read through RevokedKeys. *[OpenSSH Hardening and Hardware Security]*

KSK / ZSK — DNSSEC key-signing key (signs the zone's key set, referenced by the parent's DS) / zone-signing key (signs every record set). *[DNS Security in Practice]*

KSPP — Kernel Self Protection Project: upstream effort whose recommended kernel settings BP-028 R15-R27 largely follow. *[ANSSI GNU/Linux Hardening Deep Dive (BP-028 R1-R49)]*

Kubebuilder — Scaffolds Go controllers on controller-runtime; the mainstream way to build a custom operator. *[Helm, operators and the CRD ecosystem (with security)]*

kubeconfig — The ~/.kube/config file holding cluster addresses, CAs and credentials as named contexts that kubectl switches between. *[Kubernetes hands-on: learn it in your own lab]*

L

Landing zone — Pre-built multi-account cloud environment with identity, network, logging and guardrails in place before any workload arrives. *[Cloud Reference Architectures; Designing a Secure SME Network and Cloud Landing Zone]*

Landing zone hub — The central network account/VPC that owns the hybrid links, transit, DNS and egress inspection; spokes and on-prem attach to it. *[Hybrid, Multi-Cloud and Connectivity Architecture]*

LAPS — Local Administrator Password Solution: unique, rotated local admin password per machine, stored in AD. *[ANSSI Endpoint Security: Overview and Windows; Active Directory Security +3]*

Large community — BGP tag of three 32-bit numbers (ASN: function:parameter, RFC 8092), usable by networks with 32-bit ASNs. *[BGP and Internet Routing in Practice]*

Late collisions — Collision after the first 64 bytes: the half-duplex side of a **duplex mismatch**, or a cable beyond spec. *[Network Troubleshooting: Method, Layers, Tools, Symptoms]*

Latency / jitter — Latency = one-way or round-trip delay; jitter = variation of that delay between packets, what hurts voice and video. *[Network Models, Performance and the Physical Layer]*

Lateral movement — Using obtained credentials or access to reach other hosts in the same network or domain. *[OSCP / OSCP+: Readiness and Self-Assessment]*

Layer — tar archive of filesystem changes, content-addressed by its sha256 digest; deleting a file in a later layer does **not** remove it from the earlier one (secrets stay recoverable). *[Container Image and Registry Security]*

LC_ALL=C — forces the C locale: byte-order sorting and much faster sort/grep on ASCII logs. Prefix a command with it (LC_ALL=C sort big.log) when Unicode collation is not needed. *[Text-Processing and Data Toolkit Reference]*

LDAP / Global Catalog — Lightweight Directory Access Protocol (queries Active Directory) / partial replica of every domain in the AD forest, queried on 3268/3269. *[Networking Ports and Protocols]*

ldflags — Linker flags: -s -w strip the symbol table and DWARF debug info (smaller binary); -X pkg.var=value stamps a string variable, e.g. a version, at build time. *[Go for Security Tooling and Safe Code]*

Leading zeros — 53A writes CM-02, AC-17(01); SP 800-53r5 writes CM-2, AC-17(1). NIST states future 800-53 revisions will adopt the leading zero (footnote 25). *[SP 800-53A and 800-53B in Practice]*

Leaf switch — Where servers and storage connect (the ToR). Every leaf links to every spine and never to another leaf. *[Data-Centre Architecture]*

Leak site — Extortion group's website (often on Tor) listing victims and publishing stolen data of those who do not pay. *[Ransomware Defense End to End]*

Least common mechanism — Minimise mechanisms shared between users *[Security Operations: Logs, Malware, Servers, Media; OWASP Developer Guide v4.2 - Chapter by Chapter]*

Least functionality — (control CM-7) Only required ports, protocols, services, functions; allow/deny lists for software. *[Patch, Configuration and Continuous Monitoring]*

Least privilege — minimum rights, JIT admin, ACLs *[Mitigation Techniques]*

Least privilege / separation of duties — Minimum rights for the task; no single person controls a whole critical process *[OWASP Developer Guide v4.2 - Chapter by Chapter]*

Leg-up — Access or information deliberately handed to the red team by the control team (a user account, a foothold) to skip a stage that would take too long or is out of scope. *[Red Team Programme and Rules of Engagement]*

Legacy application in a VM — Run an unsupported legacy OS in a guest; add authentication, auditing and monitoring at the host or hypervisor level as compensating controls. *[Cloud Outsourcing and Virtualization Lifecycle]*

Legacy authentication — Protocols sending a username and password on each request (basic auth over IMAP, POP3, SMTP AUTH, old EWS clients) that cannot enforce MFA. *[Microsoft 365 Hardening]*

Legacy use — Only to process already-protected data (decrypt, verify). *[NIST Cryptographic Standards]*

Legal hold — instruction to suspend deletion of data relevant to a reasonably anticipated dispute or investigation (also litigation hold) *[Digital Evidence and Chain of Custody; Incident Response, Forensics, Automation]*

Legal hold and e-discovery — Litigation hold suspends normal retention deletion; e-discovery produces ESI (electronically stored information) under rules such as US FRCP (Federal Rules of Civil Procedure) 26 and 34 - design log retention and DLP so holds can be applied per custodian (person whose data is held). *[Compliance, Threat Modeling and AI Security]*

Lessons learned — NIST: post-incident activity *[DFIR Artifacts and Tools; Incident Response and Management +3]*

Lethal trifecta — Agent that has private data access, reads untrusted content and can communicate externally: exfiltration is then one injected instruction away. *[Emerging Topics: Self-Assessment]*

Levee de doute — 'Clearing the doubt': checking a vague or weak signal to confirm or rule out a real compromise. *[Incident Qualification & Remediation Decision Keys]*

Level of assurance (LoA) — Degree of confidence in a claimed identity (low, substantial, high) based on proofing, authenticator strength and issuance controls. *[eIDAS 2 and the EU Digital Identity Wallet]*

Lex specialis — A specific law that takes precedence over a general one on the same subject: for banks and insurers, DORA's ICT rules replace NIS2's security and reporting duties. *[NIS2 Directive: EU-wide Obligations; ENISA, NIS2 and the EU Threat Landscape]*

LFI / RFI / RCE — Local File Inclusion; Remote File Inclusion; Remote Code Execution. *[CompTIA CySA+ CS0-003]*

libinjection — Tokenizing library that recognizes SQL injection and XSS syntax; used by CRS rules 942100 and 941100. *[WAF and API Gateway Configuration]*

Lifecycle position — identify, assess, respond, monitor: the best answer is usually the next step, not a later one *[CRISC Practice Scenarios]*

Likelihood vs probability — Likelihood is the qualitative chance of a risk event (rare, possible, likely: a heat-map axis). Probability is its quantitative expression (0-1 or a percentage; per year it becomes the ARO). The exam uses likelihood in qualitative analysis and probability/ARO in quantitative. *[Governance, Risk and Third-Party Management]*

Liking / social proof — everyone else did it, friendly tone *[Social Engineering and Phishing Simulation]*

Limited risk (transparency) — Art. 50: tell users they are talking to an AI, label deepfakes and AI-generated text on matters of public interest, disclose emotion recognition. *[AI Compliance Frameworks]*

Line-oriented — these tools process text one line (record) at a time; a line is text ending in a newline. This is why they scale to huge logs: they never load the whole file. *[Text-Processing and Data Toolkit Reference]*

Linkability — ability to connect two records about the same person, within or across datasets; second test *[Privacy Engineering and PETs]*

Linux capabilities — About 41 slices of root power (CAP_NET_RAW, CAP_SYS_ADMIN...) grantable to a binary or process; the guide warns at least 19 give trivial full root. *[GNU/Linux BP-028: Kernel Build, Files and Services]*

Live boot — Running the OS from a USB/ISO without installing, useful for forensics on a suspect machine you are authorised to examine. *[Kali Linux and Security Distros: Orientation for Learners]*

Live migration — Moving a running VM to another host by copying its RAM and device state while it runs, then pausing it briefly for the final copy. *[Virtualization Internals and VM Isolation]*

Live response — Collection of volatile and targeted evidence from a running system with minimal, documented changes to it. *[Linux DFIR and Live Response]*

Living Off Trusted Sites (LOTS) — command-and-control (C2) and exfiltration disguised as ordinary traffic to Slack, Telegram, cloud storage; extends living off the land (LOTL: abusing built-in admin tools) into the cloud. *[Breach and Threat Landscape 2024]*

LLM — Large language model: neural network trained on text that predicts the next token; follows instructions found anywhere in its context. *[OWASP Top 10 for LLM Applications 2025]*

LLMNR / NBT-NS poisoning — Broadcast name resolution answered by an attacker to capture NTLM hashes; fix: disable both, enable SMB signing. *[Network and Infrastructure Assessment]*

LMS / XMSS — Stateful hash-based signature schemes (SP 800-208) for firmware signing; reusing a one-time key breaks them. *[Emerging Topics: Self-Assessment]*

Load balancing — Layer 4 (TCP/UDP, fast, blind to content) vs layer 7 (HTTP, routes on URL/headers, can host a WAF); health checks remove failed nodes; session persistence (sticky sessions) via cookie or source IP; global server load balancing (GSLB) uses DNS for multi-region. *[Security Architecture - Resilience, Controls, Zero Trust]*

Local policy — applied first, weakest *[Windows and Active Directory for Defenders]*

Local preference — highest, default 100, shared inside the AS: outbound choice *[Routing II: EIGRP, BGP at the Enterprise Edge, Redistribution]*

local.txt — Flag file proving low-privilege access on an exam machine. *[OSCP / OSCP+: Exam Format and Rules]*

Locally originated — network, aggregate or redistribute on this router *[Routing II: EIGRP, BGP at the Enterprise Edge, Redistribution]*

Locard's exchange principle — Every contact leaves a trace: the attacker takes something and leaves something behind. *[CISSP Domain 7: Security Operations]*

Locate the layer — silicon, firmware, boot chain, OS, peripheral, BMC, supply chain *[Hardware Security: Self-Assessment]*

Location (6.4.2) — Internal tests onsite, via encrypted VPN or a dedicated link from a test lab; one named admin account per assessor, disabled afterwards. External tests from an independent connection or a rented, rebuilt server; firewalls and intrusion prevention systems (IPS) in the path can hide findings. *[Security Testing and Assessment in Depth]*

Location (the where) — Component the barrier applies to: user, premises, identity, network, equipment, application, data. *[Defence in Depth & Secure Internet Gateway]*

Lock picking — Mechanical bypass; include only if explicitly in scope. *[Vulnerability Discovery and Analysis]*

Lockdown mode — ESXi setting that refuses direct host logins so all management goes through vCenter (normal) or nowhere (strict). *[VMware vSphere and ESXi Security; macOS Security for Defenders]*

Log (main courante) — Opened at activation; traces actions, decisions, costs (for insurer and courts). One log per unit, consolidated by information management. *[Cyber Crisis Management & Communication]*

Log management — SP 800-92: generating, transmitting, storing, analysing and disposing of log data, the whole lifecycle, not just collection. *[Security Operations: Logs, Malware, Servers, Media]*

Log normalization — Converting each field to one representation (e.g. all dates to UTC ISO 8601, IPs in one format) so sources can be compared. *[Log Management and ISCM in Depth]*

Log parsing — Extracting fields (date, source IP, user) from a log entry so they can feed other functions. *[Log Management and ISCM in Depth]*

Log reduction — Removing unneeded entries to create a new, smaller log file. *[Log Management and ISCM in Depth]*

Log reduction / normalization — Reduction removes unneeded entries; normalization converts every field to a common representation (timestamps to UTC, IPs, usernames) so correlation works across sources. *[NIST SP 800-92 Log Management]*

Log retention vs preservation — Retention = routine archival on a schedule. **Preservation** = keeping logs that would normally be discarded because they hold evidence (legal hold, incident). Keep originals plus centralized copies for evidentiary fidelity. *[NIST SP 800-92 Log Management]*

logarchive — Portable bundle made by log collect (or found inside a sysdiagnose) holding tracev3, uidtext and timesync

data so another Mac can run `log show --archive` on it. [*\[macOS and iOS Forensics for Defenders\]*](#)

Logging and auditing design — Log every authentication outcome, privilege change and policy decision with correlation IDs; forward IdP sign-in logs, Active Directory events 4624/4625 (logon success/failure), 4768/4769 (Kerberos TGT/service ticket requested), 4776 (NTLM credential validation) and cloud IAM audit logs to the SIEM. [*\[Security Architecture - SDLC, IAM Design, Cloud\]*](#)

Logic bomb — Dormant code that fires on a condition (a date, a user removed from payroll); insider favourite. Indicator: scheduled task or script with a time or event trigger. [*\[Malware, Attacks and Indicators\]*](#)

Logical image — Copy of files and folders only (e.g. KAPE targets, VHDX from live host). Faster, loses deleted data. [*\[Digital Forensics in Incident Response\]*](#)

Logical isolation — Copy still online but in a separate trust domain: other account or tenant, other identity provider, no shared credentials, write-once API. [*\[Backup and Recovery Engineering\]*](#)

Logical partitioning — VLANs, VRFs, firewalls, host rules on shared hardware; the degraded options of PG-075 (R5- single sensitive IS with logically separated data, R50- IPsec-protected logical network) and PA-108 (R106- logical partitioning at compute, network and storage level); acceptable only when physical is impossible. [*\[Segmentation and IS Mapping\]*](#)

LOLBin — Living-off-the-land binary: a legitimate, signed tool shipped with the operating system (PowerShell, certutil, wmic) that an attacker abuses so no malware file ever touches disk. [*\[Windows Application Control and Endpoint Monitoring; Windows Endpoint Telemetry and Sysmon +2\]*](#)

LOLBins — certutil, mshta, rundll32, bitsadmin - trusted binaries evading allowlisting. [*\[Windows and AD Logging: ANSSI PB-090; Host and Web Application Attacks\]*](#)

Longest prefix match — The forwarding rule: the most specific route wins (Fig. 5-52). Basis of BGP hijacks: announce a /24 inside a victim's /23 and traffic follows you (YouTube/Pakistan Telecom 2008). [*\[Networking Fundamentals II - Routing, L2, IPv6, Wi-Fi, Tools; IPv4 Addressing, Subnetting, VLSM and NAT\]*](#)

Look at risk — assess before you act or buy [*\[CISM Exam Strategy\]*](#)

Lookalike domain — Domain registered to resemble a trusted one (typo, swapped characters, extra word, other TLD, Uni-

code homoglyph) so that a glance at the sender or link looks right. [*\[Phishing Analysis and E-mail Header Forensics\]*](#)

LoRA adapter — Low-Rank Adaptation: small add-on weight file that fine-tunes a base model; can carry a backdoor. [*\[OWASP Top 10 for LLM Applications 2025\]*](#)

Loss exceedance curve — probability that annual loss exceeds X; compare with appetite lines; output of a Monte Carlo run [*\[Risk Quantification and Cyber Insurance\]*](#)

LOTL — Living off the land: using built-in admin tools (PowerShell, WMI, ntdsutil, netsh) so no malware file exists to detect. [*\[Threat Actor Profiles\]*](#)

Low profile — Investigate without alerting the attacker: no ping-ing their IPs, no mass password resets before scoping. [*\[SANS Incident Handler Checklists and Enterprise IR\]*](#)

LPM — Loi de programmation militaire: the military planning law that imposes security rules on operators of vital importance (OIV). [*\[Start-ups, Municipalities, Teleassistance, Open Source\]*](#)

LPM / SIIV — military programming law (2013) obliging vital operators (OIV) to accredit their vital information systems (SIIV). [*\[Security Accreditation \(Homologation\)\]*](#)

LSA / LSASS — Local Security Authority (lsass.exe process): validates logons and caches credential material; RunAsPPL and Credential Guard protect it. [*\[Windows and Active Directory for Defenders\]*](#)

LSA protection (PPL) — Runs LSASS, the process holding logon secrets, as a Protected Process Light so unsigned code cannot read its memory. [*\[ANSSI Endpoint Security: Overview and Windows\]*](#)

LSA protection (RunAsPPL) — Runs lsass.exe as a Protected Process Light: only Microsoft-signed code may open it or load into it, which stops Mimikatz-style memory reading by administrators. [*\[Windows Internals for Defenders; Windows Hardening Baseline\]*](#)

LSAiso — Isolated LSA trustlet running in VTL1 that keeps NTLM hashes and Kerberos keys for Credential Guard. [*\[Windows Privacy GPOs and VBS Deployment\]*](#)

LSASS — Local Security Authority Subsystem Service, the Windows process holding logon secrets in memory (hashes, tickets), target of credential dumping. [*\[Active Directory Security; Windows Endpoint Telemetry and Sysmon\]*](#)

LSASS (Local Security Authority Subsystem Service) — lsass.exe, started by wininit.exe: authenticates logons, creates tokens, enforces local security policy and holds credential ma-

terial for single sign-on in memory. [*\[Windows Internals for Defenders\]*](#)

LSM (Linux Security Module) — Kernel hook framework for mandatory access control: SELinux (labels) or AppArmor (path profiles). [*\[ANSSI GNU/Linux Hardening Deep Dive \(BP-028 R1-R49\); Linux Isolation Primitives and Sandboxes\]*](#)

Lumens — Total light output of a projector (ANSI lumens), not comparable with nits. [*\[Power, Displays, Peripherals and Printers\]*](#)

LVFS — Linux Vendor Firmware Service: repository of signed vendor firmware installed by fwupdmg. [*\[OpenSSH Hardening and Hardware Security\]*](#)

M

M-21-31 EL0-EL3 — OMB logging memo: event logging tiers from EL0 (not effective) to EL3 (advanced), with log retention of 12 months active plus 18 months cold storage. [*\[CISA Zero Trust Maturity Model v2.0\]*](#)

(M)LWE / (M)SIS — (Module) Learning With Errors / Short Integer Solution: lattice problems believed hard for quantum computers, basis of ML-KEM and ML-DSA. [*\[ANSSI Cryptographic Mechanisms and PQC\]*](#)

M2M API — Machine-to-machine API: called by other services, no browser and no human session. [*\[OWASP ASVS 5.0 - Application Security Verification Standard\]*](#)

MAB — MAC authentication bypass: the switch submits the device's MAC address as identity when it has no supplicant. [*\[Segmentation and IS Mapping; BGP, 802.1X & VPN\]*](#)

MAB (MAC Authentication Bypass) — Fallback where the switch sends the device's MAC address to RADIUS as its identity; weak, reserved for devices without a supplicant. [*\[Network Equipment Hardening; First-Hop Security and Gateway Redundancy\]*](#)

MAC — Message authentication code: keyed checksum proving integrity and origin to someone holding the same key. [*\[ANSSI Cryptographic Mechanisms and PQC\]*](#)

MAC / HMAC / CMAC — Message Authentication Code: keyed checksum proving integrity and origin; HMAC is built on a hash, CMAC on a block cipher (AES). [*\[Cryptography Primer\]*](#)

MAC (Mandatory Access Control) — Access rules set by a central policy that the file owner cannot change, unlike Unix DAC (Discretionary Access Control) permissions. [*\[ANSSI GNU/Linux Hardening Deep Dive \(BP-028 R1-R49\)\]*](#)

MAC (SELinux / AppArmor) — Mandatory Access Control: a kernel policy that confines processes even when they run as root, unlike discretionary Unix permissions. *[Linux Security Command Line]*

MACB — the four file timestamps: Modified (content), Accessed, Changed (metadata / MFT record changed), Born (created); the basic columns of any file-system timeline. *[DFIR Artifacts and Tools]*

MACB timestamps — Modified, Accessed, Changed (metadata), Born (created). NTFS \$STANDARD_INFORMATION is easy to timestamp; compare with \$FILE_NAME attribute. *[NIST IR, Forensics, and Exercises; Digital Forensics in Incident Response]*

Mach-O — Executable format of Apple platforms: header, load commands (libraries, segments, code signature, encryption info), then segments. *[iOS Application Internals and Security]*

Macro vs micro segmentation — macro = large zones (enclaves, VLANs); micro = per-workload or per-application rules enforced by software. *[DoD Zero Trust and NSA Hardening Guidance]*

MACsec — IEEE 802.1AE link-layer encryption between device and switch, keyed by MKA (MACsec Key Agreement) after 802.1X: every frame is authenticated, not only the port opening. *[Wi-Fi and 802.1X: Full Recommendation Sets]*

MACsec (IEEE 802.1AE) — Hop-by-hop L2 encryption (AES-GCM-128/256) with keys negotiated by MKA (802.1X-2010). Use on uplinks and inter-building fibre where physical security is not guaranteed; macsec network-link + mka policy on IOS-XE. It protects the wire, not the switch: management hardening above still applies. *[Network Equipment Hardening; Automotive and Embedded Security]*

Mailbox permissions — FullAccess, SendAs, folder delegation *[Microsoft 365 Hardening]*

Main courante (log) — Time-stamped crisis log of every fact, decision, action and cost; evidence for the insurer, the courts and the RETEX. *[Cyber Crisis Management & Communication]*

Maintenance group — SP 800-40r4: set of assets with similar maintenance needs (e.g. laptops, OT, containers) that share one patching plan per scenario. *[Patch, Configuration and Continuous Monitoring]*

Major ICT-related incident (DORA) — Incident with high adverse impact on the network and information systems support-

ing critical or important functions of a financial entity, classified with the criteria of Delegated Reg. 2024/1772. *[Cyber Incident Reporting Obligations]*

Major incident — **Major incident** (OMB M-20-04) - an incident likely to cause demonstrable harm to US national security, foreign relations, economy, public confidence, civil liberties or public health and safety, or a breach of PII with the same potential. Major incident determination is required for breaches involving the PII of... *[CISA Playbooks, KEV and Mobile Guidance]*

Major nonconformity — absence or total breakdown of a requirement, or a set of minors showing systemic failure; raises significant doubt on the ISMS; corrective action plan and verification before certification *[ISO/IEC 27001:2022 and 27002:2022]*

Major security incident — Sequence of technical events severely impacting, or threatening, business lines essential to the organisation; **impact, not nature, sets severity**; it can degenerate into a crisis. *[Managing Cyber Remediation]*

Malicious insider — acts on purpose: theft of intellectual property, fraud, sabotage, espionage, leaking. *[Insider Threat Program]*

Malware-free attack — intrusion using valid credentials and built-in tools only, so no malicious file is detected. *[Vendor Threat Reports: Identity, Endpoint, IR]*

Man page — the reference manual page of a Unix command, file format or function, read with `man`, split into numbered sections (1 = user commands, 5 = file formats, 8 = admin commands). *[Master Any Command-Line Program Fast, on Every OS; Read the Manual: man, help, tldr and info]*

Managed identity — Service principal whose credentials Azure creates and rotates automatically for a resource; no secret to leak. *[Azure and Entra ID Security Essentials]*

Management domain / workload domain — VMware Cloud Foundation terms for the administration cluster and the production clusters (R7). *[VMware vSphere and ESXi Security]*

Management plane compromise — vCenter or Proxmox access gives snapshot, console, clone and network control over every VM; ransomware crews now encrypt at the hypervisor level. *[ToIP and Virtualization Security]*

Management rules / detection rules — who answers out of hours, escalation criteria, reminders / technical translation of the strategy, signature or behavioural, generic or sensor-specific, exchanged as Sigma, YARA, MISP JSON or pseudo-

code, with exemption lists. *[Security Supervision: ANSSI GP-112 and PG-113]*

Managing security risk — governance, risk, assets, supply chain *[NCSC, BSI and Allied Cyber Authorities]*

Mandatory access (accès obligatoire) — An access automatically added to every encrypted partition of the fleet; its holder can decrypt them all. *[ANSSI Encryption Tools: Zed! and Cryhod (2/2, Cryhod)]*

Mandatory reporting requirement — An obligation to report certain discoveries immediately regardless of the test (illegal content such as child abuse material, active compromise, safety hazards, legal or regulatory duties). *[Engagement Management]*

Manifest / index — JSON listing config and layers (manifest) or one manifest per platform (image index, multi-arch); its digest is the image identity: `repo@sha256:...` *[Container Image and Registry Security]*

Manifest V3 — Chrome extension platform version: service worker background, declarativeNetRequest instead of blocking webRequest, no remotely hosted code *[Browser and Extension Security]*

MANRS — Mutually Agreed Norms for Routing Security: operator programme of four actions (filtering, anti-spoofing, coordination, global validation). *[BGP, 802.1X & VPN]*

Mantrap — Two interlocked doors allowing one authenticated person through at a time; prevents tailgating. *[CISA Domain 5: Protection of Information Assets]*

Mantrap (access control vestibule) — Two interlocked doors that hold one person at a time to stop tailgating. *[CISSP Domain 3: Security Architecture and Engineering]*

Manufacturer TCB vs User-provided TCB — CPU, memory controller, encryption engine and their firmware (vendor) vs the code running inside the enclave (user - but in practice also CSP-injected VM firmware and virtual TPM, hence *ISV TCB*, independent software vendor). *[Confidential Computing]*

Map — Kernel key/value store shared by eBPF programs and user space (hash, array, ring buffer, LPM trie...). *[eBPF in Depth; Go Programming from Zero (Part 1: language basics)]*

Map scan — Discover what exists (hosts, MACs, OUIs) to build the inventory; shadow IT and rogue devices show up here before any CVE does. *[Vulnerability Scanning Methods]*

MAPS — Microsoft Active Protection Service (SpyNet): Defender cloud protection that sends file metadata and samples for verdicts. *[Windows Privacy GPOs and VBS Deployment]*

MAS Testing Profiles — Since the 2023 MASVS refactoring the verification levels L1, L2 and R left the standard and became MAS Testing Profiles in the MASTG, aligned with NIST OSCAL (Open Security Controls Assessment Language); the MAS Checklist assigns each test to profiles L1, L2, R (and P for privacy). The standard itself only states... *[\[OWASP Mobile - Top 10 2024, MASVS v2.1, MASTG\]](#)*

Masking — Display only part of a value (**** **** **** 4242). The original stays intact in the store; the mask is irreversible on screen. *[\[Data Protection and Resilience\]](#)*

Mass assignment — Client sets fields the server should own (role=admin) because the binder trusts input. *[\[Web Application Assessment; OWASP API Security Top 10 - 2023 +1\]](#)*

matchConstraints — The resource rules (group/resource/verbs) a VAP applies to; further narrowed with `matchConditions` (CEL guards) to skip requests cheaply. *[\[Kubernetes Admission Control and Policy as Code\]](#)*

Materiality — Significance for investors or the business; triggers disclosure duties such as the US SEC Form 8-K Item 1.05. *[\[CISA Domain 1: Information System Auditing Process; Communicating Risk to Executives and Boards\]](#)*

MBCO (Minimum Business Continuity Objective) — minimum service level acceptable during the disruption (e.g. 60 % of orders, priority customers only) *[\[Business Continuity and ISO 22301\]](#)*

MBR vs GPT — MBR: 4 primary partitions, 2 TB limit, boot code in sector 0. GPT: 128 partitions, 9.4 ZB, protective MBR, needs UEFI to boot. `diskpart > convert gpt, mbr2gpt /convert`. *[\[CompTIA A+ Core 1 - Hardware and Troubleshooting\]](#)*

MCO / MCS — *Maintien en condition operationnelle / de securite*: keeping systems running / keeping them patched and securely configured. *[\[Remote Work \(Digital Nomadism\); Start-ups, Municipalities, Teleassistance, Open Source +5\]](#)*

MCP — Model Context Protocol: standard for connecting AI assistants to tool and data servers. *[\[SecAI+ Discriminators and Practice Scenarios; Emerging Topics: Self-Assessment +1\]](#)*

MCP client — One connection per server inside the host; forwards tool calls and results. *[\[AI-Assisted Security\]](#)*

MCP host — The application embedding the model (IDE, chat client, agent runtime) that decides which servers to connect and mediates user consent. *[\[AI-Assisted Security\]](#)*

MCP (Model Context Protocol) — Open protocol connecting AI hosts to servers that expose tools, resources and prompts over JSON-RPC. *[\[Agentic AI and MCP Security\]](#)*

MCP server — Exposes **tools** (callable actions), **resources** (readable data) and **prompts** (templates) over stdio or streamable HTTP. Tool descriptions are read by the model, so they are an injection surface. *[\[AI-Assisted Security\]](#)*

MCS (*maintien en conditions de securite*) — security maintenance: watching for vulnerabilities and applying fixes so the system keeps its security level over time. *[\[Protecting Essential IS - PA-085 R1 to R62\]](#)*

MDA (Mail Delivery Agent) — Component that stores accepted mail in the recipient's mailbox (Dovecot LDA/LMTP, Exchange mailbox store), then read by IMAP or POP. *[\[Email Infrastructure Operations\]](#)*

MDLC — Model development life cycle: business case, data collection and preparation, development, evaluation, deployment, validation, monitoring, feedback. *[\[SecAI+ Discriminators and Practice Scenarios\]](#)*

MDM — Mobile Device Management: central console pushing security profiles, apps and compliance rules to enrolled phones (NT-010 R1). *[\[Remote Work \(Digital Nomadism\); Mobile Device Security and MDM\]](#)*

MDM (Mobile Device Management) — server (Jamf Pro, Intune, Kandji, Mosyle, ...) that pushes configuration profiles and commands through the Apple Push Notification service (APNs). *[\[macOS Security for Defenders\]](#)*

MDPH / CCAS — Departmental house for disabled people / municipal social action centre: typical holders of health and social data. *[\[Local Authorities: the Regulatory Security Framework\]](#)*

MDR (Managed Detection and Response) — Outsourced 24/7 service that monitors your security telemetry, investigates alerts and takes agreed containment actions. *[\[Designing a Secure SME Network and Cloud Landing Zone\]](#)*

MDS2 — Manufacturer Disclosure Statement for Medical Device Security: standard questionnaire on a device's security features *[\[IoT and Medical Device Security\]](#)*

MEAE — *Ministere de l'Europe et des Affaires etrangeres* (foreign ministry), co-author of the travel passport; publishes country advice (*Conseils aux voyageurs*). *[\[Business Travel and SME Cybersecurity\]](#)*

Measure (*mesure*) — Basic organisational, technical or operational unit whose function contributes to a barrier's objective. *[\[Defence in Depth & Secure Internet Gateway\]](#)*

Measured boot — Each boot stage hashes the next into PCRs before running it, creating evidence for later checks. *[\[Remote Work \(Digital Nomadism\); ANSSI GNU/Linux Hardening Deep Dive \(BP-028 R1-R49\) +1\]](#)*

Measured service — metering per resource type; usage monitored, controlled and reported to both parties *[\[Cloud Computing Security\]](#)*

Measurement — cryptographic hash (usually SHA-384) of code and configuration loaded into the TEE, computed by the hardware at launch or extended at runtime *[\[Confidential Computing and Remote Attestation; CIS Controls v8.1: All 153 Safeguards\]](#)*

MED — Multi-Exit Discriminator, lowest wins; a neighbour AS's hint about which of its links to use; compared only between paths from the same neighbour AS by default *[\[Routing II: EIGRP, BGP at the Enterprise Edge, Redistribution\]](#)*

media or platforms — different failure domains: disk + object storage, disk + tape, two cloud providers *[\[Backup and Recovery Engineering\]](#)*

Mega breach — breach of more than 1 million records; excluded from IBM's average and analysed separately. *[\[IBM Breach Cost and X-Force Index 2024\]](#)*

Memory ballooning — Guest driver that allocates and hands pages back to the host on request, letting the host overcommit RAM. *[\[Virtualization Internals and VM Isolation\]](#)*

Memory-hard function — Password hash (Argon2, scrypt) that needs large RAM per guess, making GPU/ASIC cracking costly. *[\[Authentication, MFA and Passwords\]](#)*

Memory image — File holding a copy of physical RAM (raw `.raw/.mem`, crash dump `.dmp`, VMware `.vmem` + `.vmss`, Hyper-V `.bin` + `.vsv`, LiME `.lime`). *[\[Memory Forensics with Volatility 3\]](#)*

Memory smear — Inconsistency in an image because RAM kept changing during the minutes of acquisition; broken lists and half-written structures are normal, not proof of a rootkit. *[\[Memory Forensics with Volatility 3\]](#)*

Message-bound signature — A signature is valid for one message only, whatever the key. *[\[ANSSI Crypto Rules Catalogue \(PG-083 v3.00\)\]](#)*

Message bus — Queue or event stream (e.g. RabbitMQ, Kafka) that decouples producers from consumers so a slow or down

consumer does not block the producer. *[Web Application and Microservices Architecture]*

Meta key — the modifier readline calls M- (Alt on PC keyboards, Option on a Mac once enabled, or Esc pressed then released before the next key). *[Shell and Terminal Productivity on Every OS]*

Metastructure — CSA term for the management plane (consoles, APIs, identities that configure the cloud); its compromise gives control of everything below it. *[CCSP and CCSK: Cloud Security Certifications]*

Metrics (3.2.1) — Derived from objectives; examples: vulnerabilities found and fixed, unauthorized access attempts, baseline compliance, contingency test dates, training currency. Metrics from **unassessed controls** are like an uncalibrated scale. *[Log Management and ISCM in Depth]*

MEV (maximal extractable value) — profit from ordering, inserting or censoring transactions in a block (front-running, sandwich attacks) *[Blockchain and Smart-Contract Security]*

MFA fatigue — Flooding a user with push prompts until one is approved by mistake. *[Authentication, MFA and Passwords]*

MFA (multi-factor authentication) — Proof of identity with two or more factor types: something you know, have or are. *[Zero Trust Architecture SP 800-207]*

MFA without SMS — FIDO2 / passkeys; SIM-swap check on risky flows *[Telecom and 5G Security]*

MFP — Multifunction printer (print, scan, copy, fax) with its own OS, disk and network services. *[Power, Displays, Peripherals and Printers]*

MFT — Master File Table: NTFS metadata file with one 1,024-byte record per file or directory, holding its attributes and timestamps. *[Storage and Filesystems for Defenders]*

MIB / OID — The MIB (Management Information Base) is the tree of values a device exposes; each value has an OID (object identifier) such as 1.3.6.1.2.1.1.3.0 = sysUpTime. *[Network Operations: Documentation, Monitoring, Resilience]*

Micro-segmentation — Filtering between small groups of workloads, tied to identity or tags rather than IP ranges. *[ANSSI Zero Trust Model; Classic Enterprise Network Architecture +1]*

Microcode — CPU-internal firmware patch loaded at boot by UEFI or the OS; the main delivery path for side-channel fixes. *[CPU Side Channels and Memory Attacks]*

Middlebox ossification — Network devices that break when protocols change shape, such as a ClientHello larger than one packet. *[Quantum-Safe Network Protocols: Status]*

Mimikatz — LSASS dump, pass-the-hash, golden/silver ticket, DCSync. *[Host and Web Application Attacks]*

Minifilter altitude — Number that places a file-system filter driver in the stack; Microsoft assigns ranges (anti-virus filters sit around 320000-329999) and a filter sees I/O before those below it. *[EDR Telemetry, Tamper and Evasion Detection]*

Minimal defaults — deny by default, few configuration knobs (R22, R23) *[System Partitioning: ANSSI PG-040]*

Minimal risk — Spam filters, AI in video games and similar uses: no new obligations, voluntary codes of conduct. *[AI Compliance Frameworks]*

Minimising the impact of incidents — response and recovery, lessons learned *[NCSC, BSI and Allied Cyber Authorities]*

Minimum viable company (MVC) — smallest set of business services, people, identity, network and data the organisation needs to operate at MBCO; restored first, rehearsed in advance *[Business Continuity and ISO 22301]*

Minor nonconformity — single lapse that does not affect the capability of the ISMS; corrective action plan accepted, verified at next audit *[ISO/IEC 27001:2022 and 27002:2022]*

Mirai — 2016 botnet that enslaved hundreds of thousands of cameras and routers through default Telnet passwords and ran record DDoS attacks. *[IoT/IloT Security and OT Detection]*

Mishandling of Exceptional Conditions — A10:2025. Errors, unexpected states and failed checks that leave the application insecure: fail-open logic (a failed authorization call treated as allowed), swallowed exceptions, missing timeouts, stack traces shown to users. Root-cause category, like Insecure Design. *[OWASP Top 10 - Web (2021 and 2025)]*

MISP attribute — One typed value (ip-dst, domain, sha256, url) with a category and a to_ids flag: only to_ids=true values are exported to detection tools. *[Cyber Threat Intelligence Lifecycle]*

MISP event — Container for one incident, campaign or report: attributes, objects, tags, analyst notes and a distribution level. *[Cyber Threat Intelligence Lifecycle]*

MISP galaxy — Knowledge-base clusters attached to events: threat actors, malware families, ATT&CK techniques, sectors. *[Cyber Threat Intelligence Lifecycle]*

MISP / OpenCTI — open-source threat intelligence platforms that store, correlate and share indicators and reports. *[Malware Triage and Analysis]*

Mitigation — control that removes or reduces a threat; recorded as a security requirement with a test. *[Threat Modeling Methods]*

Mitigation and recovery functions (6.4) — Response plan establishment, ad hoc measures and containment, system restoration, support to other security entities. *[SOC 2 Trust Services Criteria, COBIT 2019, CSIRT Services]*

MITRE ATT&CK — Public knowledge base of adversary tactics (the why) and techniques (the how) observed in real intrusions, used to map detections. *[CEH v13: Exam Blueprint and Module Map; CompTIA PenTest+ PT0-003]*

ML-BOM (LLM03) — Machine Learning Bill of Materials: attestations of datasets and models, now part of CycloneDX. The 2025 text calls it an AI BOM. *[OWASP LLM Top 10 v1.1 (2023) and the 2025 Shift]*

MLAG / vPC — Multi-chassis Link Aggregation (Cisco vPC): two switches appear as one to a server so both uplinks are active and either switch can fail. *[Data-Centre Architecture]*

MOAS — Multiple Origin AS: the same prefix announced with different origin ASNs at the same time; a classic hijack signal (sometimes legitimate anycast). *[BGP and Internet Routing in Practice]*

MODDIR — Moderating director: heads the moderating unit, checks each moderator plays their role and that players understand the information received. *[Organising a Cyber Crisis Management Exercise]*

Mode opératoire d'attaque (MOA) / TTPs — The attacker's signature: how a group targets and attacks its victims. *[ANSSI CyberDico FR/EN Glossary]*

Model access — who may query, fine-tune, export or delete which model version *[Securing AI Systems]*

Model extraction — Rebuilding a functional copy of a model by querying it at scale and training on its answers (model theft). *[AI Monitoring, Attacks and Compensating Controls]*

Model skewing — Gradual shift of a model's decisions caused by attacker-controlled feedback data fed into retraining. *[AI Monitoring, Attacks and Compensating Controls]*

Model theft — Copying proprietary weights (leak, insider) or cloning behaviour by querying the API and training a copy. *[OWASP LLM Top 10 v1.1 (2023) and the 2025 Shift]*

Moderating unit — Moderators simulating everyone outside the exercise (technical teams, press, authorities, customers, attacker) who interact with the players. *[Organising a Cyber Crisis Management Exercise]*

Modular — Detachable cables: never mix cables between PSU brands, pinouts differ at the PSU end. *[Power, Displays, Peripherals and Printers]*

Module — A .py file whose functions you reuse with `import`; a package is a folder of modules, installed with `pip` from PyPI (the Python Package Index). *[Python for Security from Zero]*

Monetary unit sampling — Each currency unit has an equal chance, so high-value items are favoured. *[CISA Domain 1: Information System Auditing Process]*

Monitor mode — Wi-Fi adapter mode that captures all 802.11 frames on a channel, including management frames, without associating. *[Packet Analysis in Practice and the N10-009 Exam Map]*

Monitor posture — no asset is inherently trusted *[Zero Trust Architecture SP 800-207]*

Monitoring — Continuous telemetry from systems, applications and infrastructure: logs to SIEM, EDR agent, FIM on config files, performance baselines, uptime probes. Alert on deviation from the baseline, not just on signatures. *[Security Operations - Baselines, Wireless, Mobile, Assets]*

Monitoring OT without touching it — OT devices are fragile, so monitoring is passive: mirror traffic (SPAN port) or a network TAP into an OT-aware Intrusion Detection System (e.g. Dragos, Clarity, Nozomi) that speaks industrial protocols and builds an asset inventory. It learns the normal baseline and alerts on a new device, an unexpected command, or a... *[Industrial (OT/ICS) Architecture]*

MORlock / HSTI / WSMT — Secure Memory Overwrite Request lock (RAM wiped on reboot), Hardware Security Testability Interface (firmware self-report), Windows SMM Security Mitigations Table (protects System Management Mode). *[Windows Privacy GPOs and VBS Deployment]*

Mosca's inequality — Act now if data shelf life X plus migration time Y exceeds the years Z until a quantum computer can break today's public-key crypto. *[Emerging Topics: Self-Assessment]*

MOU / SLA — Memorandum of Understanding (non-binding agreement); Service Level Agreement (contractual target, e.g. 99.9 % uptime). *[CompTIA CySA+ CS0-003]*

Mozilla intermediate profile — Recommended general-purpose TLS configuration: TLS 1.2 and 1.3, ECDHE key exchange, AEAD ciphers only. *[Web Server and TLS Configuration]*

MPLS — Label switching between layers 2 and 3; provides traffic separation, not encryption. *[CISSP Domain 4: Communication and Network Security]*

MPLS (Multiprotocol Label Switching) — Carrier-managed private WAN circuits that link branches to a central data center. *[Secure Enterprise Network Landscape SP 800-215]*

MRP — Media Redundancy Protocol (IEC 62439-2): industrial ring protocol recovering from a link cut in tens of milliseconds. *[OT Switch and Firewall Hardening: Hirschmann, SCALANCE]*

MS-RPC / SMB — Microsoft Remote Procedure Call (endpoint mapper 135 then dynamic ports) / Server Message Block (file shares, named pipes, remote admin on 445). *[Networking Ports and Protocols]*

MSA — Master service agreement. Overarching terms, liability, insurance. *[Engagement Management; Engagement Methodology and Reporting]*

MSA (Mail Submission Agent) — Server that accepts mail from authenticated users on port 587 (STARTTLS) or 465 (implicit TLS) and hands it to the MTA. *[Email Infrastructure Operations]*

MSA (Master Service Agreement) — Umbrella contract between client and testing firm: liability, payment terms, confidentiality; reused across jobs. *[Penetration Methodologies]*

MSEL (Master Scenario Events List) — the timetable of all injects with sender, recipient, expected action and the objective each one tests *[Crisis Communication and Tabletop Exercises]*

MSRT — Malicious Software Removal Tool, monthly Microsoft cleaner that reports infections unless `DontReportInfectionInformation=1`. *[Windows Privacy GPOs and VBS Deployment]*

MSS clamping — A router rewrites the Maximum Segment Size in TCP SYNs so both ends send segments that fit a tunnel, without needing ICMP. *[ICMP, Path MTU, DHCP and DNS Operations]*

MSSP — Managed security service provider: runs monitoring or security operations for customers under contract. *[CISM Domain 3: Information Security Program; IR Teams, Playbooks and Lessons Learned]*

MSSP / MDR — Managed Security Service Provider (outsourced monitoring, often alert forwarding) / Managed Detection and Response (outsourced detection plus hands-on investigation and containment). *[SOC Operations and SOAR]*

MSTG-ARCH — The v1 architecture group was dropped; only ARCH-9 (enforced updates) survives, as **CODE-2**. *[MASVS v2.1 Controls and Their MASTG v1.7 Tests]*

MSTG-STORAGE-7 / -9 — Sensitive data in the UI and in auto-generated screenshots: v1 storage items that became **PLATFORM-3** (UI) in v2. *[MASVS v2.1 Controls and Their MASTG v1.7 Tests]*

MT/s — Mega-transfers per second: DDR data rate, twice the real clock in MHz. *[CPUs, Memory, Motherboards and Buses]*

MTA — Mail Transfer Agent (Postfix, Exim, sendmail) delivering system mail such as cron output. *[GNU/Linux BP-028: Kernel Build, Files and Services]*

MTA (Mail Transfer Agent) — Server that relays mail between domains over SMTP port 25, choosing the destination from MX records (Postfix, Exim, Exchange, EOP). *[Email Infrastructure Operations]*

MTA / MSA — Mail Transfer Agent (server relaying mail to other servers, port 25) / Mail Submission Agent (accepts mail from authenticated users, port 587 or 465). *[Networking Ports and Protocols]*

MTA-STS / TLS-RPT — SMTP MTA Strict Transport Security (RFC 8461): policy forcing TLS between mail servers / SMTP TLS Reporting (RFC 8460): daily reports of TLS failures. *[Email Security: SPF, DKIM, DMARC]*

MTBF — Mean time between failures; higher means more reliable. *[IT Usage Charter and Outsourcing Security; CISA Domain 4: IS Operations and Business Resilience]*

MTD — Maximum tolerable downtime (MTO, maximum tolerable outage): point beyond which the business suffers unacceptable harm; RTO must be below it. *[CISA Domain 4: IS Operations and Business Resilience]*

MTD (Maximum Tolerable Downtime) — Longest outage the business survives; RTO plus verification time (WRT, work recovery time) must stay below it. *[CISM Domain 4: Incident Management; Backup and Recovery Engineering +1]*

MTD (MTPD, MAO) — Maximum tolerable downtime before the business suffers irrecoverable harm. *[CISSP Domain 1: Security and Risk Management]*

MTE — Memory Tagging Extension (ARMv8.5): hardware tags that catch use-after-free and overflow bugs, used by Android Advanced Protection. *[Mobile Device Security and MDM]*

mTLS — mutual TLS: both ends present certificates; a service mesh issues short-lived workload certificates and rotates them automatically. *[IoT/IIoT Security and OT Detection; Kubernetes and Container Networking Explained]*

MTPD (Maximum Tolerable Period of Disruption) — time after which the impact of not resuming an activity becomes unacceptable; also called MTD or MAO (maximum acceptable outage) *[Business Continuity and ISO 22301]*

MTTD — Mean Time To Detect: average delay between the start of malicious activity and its detection. *[Communicating Risk to Executives and Boards]*

MTTD / MTTR — Mean (or median) time to detect a compromise, and to respond or remediate after detection. *[CompTIA CySA+ CS0-003; Security Metrics and Board Reporting]*

MTTI / MTTC — mean time to identify / to contain a breach, in days (IBM); their sum is the breach lifecycle. *[Breach and Threat Landscape 2024]*

MTTR — Mean time to repair or restore; lower means faster recovery. *[CISA Domain 4: IS Operations and Business Resilience; Communicating Risk to Executives and Boards]*

MTU (Maximum Transmission Unit) — Largest IP packet a link carries without fragmentation: 1 500 bytes on Ethernet. The path MTU is the smallest MTU along the path. *[ICMP, Path MTU, DHCP and DNS Operations]*

MUA (Mail User Agent) — The mail client (Outlook, Thunderbird, a phone app, a web client) that composes and reads messages. *[Email Infrastructure Operations]*

Multi-cloud — Workloads deliberately spread across two or more cloud providers, each reachable and governed consistently. *[Hybrid, Multi-Cloud and Connectivity Architecture]*

Multi-tenancy — Several customers (tenants) share the same physical hosts and software, separated only logically. *[ENISA Cloud Computing Risk Register (2009); Cloud Computing Security]*

Multi-tenancy authorization — centralized (provider keeps one authorization DB for all tenants), decentralized (tenant runs its own), hybrid; choose per tenant attributes/roles and hierarchy relationships. *[Cloud Reference Architecture and Access Control]*

Multicast groups — 224.0.0.5 all OSPF routers (DR to others), 224.0.0.6 DR/BDR (DROTHERs to DR). IPv6: ff02::5

and ff02::6. IP protocol 89. *[Routing I: Routing Table, Static Routes, OSPF]*

Multifactor authentication (MFA) — Proof of identity by verifying **several factors of different categories**; missing any factor must fail the authentication. PIN + password is **not** MFA (same category, same threats): the guide calls that *double authentication*. A location factor (IP range, GPS) is immature and easy to bypass: treat with caution.... *[ANSSI Identity: MFA, AD Tiering, OpenID Connect; Authentication, MFA and Passwords]*

Mutating vs validating — Mutating admission may change the object (inject, default); validating admission may only accept or reject. Mutation always runs first. *[Kubernetes Admission Control and Policy as Code]*

Mutualisation — sharing of physical storage or servers between clients - the property that separates public/community commercial offers from dedicated ones. *[Cloud Hosting for Sensitive Systems]*

MVC rehearsed — know and test the minimum viable company before the crisis *[Business Continuity and ISO 22301]*

MVP — minimum viable product: the smallest version that yields validated learning with the least effort; GP-112 builds supervision from one. *[Security Supervision: ANSSI GP-112 and PG-113]*

MVT — Mobile Verification Toolkit: Amnesty International Security Lab's open-source tool (2021) that checks iOS backups and filesystem dumps against spyware indicators. *[macOS and iOS Forensics for Defenders]*

MX record — DNS record naming the servers that receive mail for a domain, with a priority (lower = preferred). *[Email Security: SPF, DKIM, DMARC]*

N

N+1 vs 2N — N+1 provides one spare unit beyond need (power/cooling); 2N fully duplicates everything. 2N costs more but survives a whole side failing. *[Data-Centre Architecture]*

NAC / DLP — Network access control (device admitted to the network after checks); data loss prevention (blocks sensitive data leaving). *[ANSSI Zero Trust Model]*

NAC (Network Access Control) — Admission control that authenticates a device/user (802.1X) before granting a VLAN, quarantine or deny. *[Classic Enterprise Network Architecture; Security Architecture - Resilience, Controls, Zero Trust]*

NACL — Network access control list: stateless allow/deny rules on a cloud subnet, used to restrict who reaches an AI endpoint. *[SecAI+ Discriminators and Practice Scenarios]*

Nagle + delayed ACK — Nagle holds small writes until the previous one is acked; the peer delays ACKs (40 ms Linux minimum, up to 200 ms Windows). Together: 40-200 ms stalls in chatty protocols. Fix with TCP_NODELAY. *[TCP and UDP Deep Dive]*

Name constraints — Extension of a CA certificate limiting the names it may certify (permitted/excluded DNS suffixes, IP ranges), so a stolen issuing CA cannot mint certificates for google.com. *[PKI Operations and Key Management]*

Named group (TLS) — Identifier of a key-exchange algorithm negotiated in the TLS 1.3 key_share extension, such as X25519MLKEM768 (0x11EC). *[Quantum-Safe Network Protocols: Status]*

Namespace — A named scope that groups and isolates objects (dev/prod), and the boundary for quotas and most RBAC rules. *[Docker Container Security; Linux Isolation Primitives and Sandboxes +1]*

NAT — Router rewrites private source addresses to its one public address; incoming traffic needs forwarding rules. *[CompTIA A+ Core 1 - Networking, SOHO, Network Troubleshooting]*

NAT / PAT — Network Address Translation rewrites IP addresses at a boundary; Port Address Translation (NAT overload) also rewrites ports so many private hosts share one public address. *[NIST Network Security Guides; IPv4 Addressing, Subnetting, VLSM and NAT]*

NAT / PAT (RFC 3022) — Many private hosts share one public IP via source-port rewriting; breaks end-to-end model, hides hosts but is not a security control. *[Networking Fundamentals I - Models, IP, TCP, Ports]*

NAT-T (NAT traversal) — ESP wrapped in UDP 4500 so NAT and PAT devices can track it; keepalives every 20 s hold the NAT mapping. *[VPNs in Depth: IPsec/IKEv2, TLS VPN, WireGuard; VPN and Firewall Security]*

Native VLAN — The VLAN whose frames cross an 802.1Q trunk untagged; both ends must agree on it. *[Network Equipment Hardening; Access Switch Audit Grid: DAT-NT-025 R1-R71 +2]*

NBA (network behavior analysis) sensors (6.1.3) — Mostly passive; inline models sit between the perimeter firewall and the border router to absorb floods. *[Firewall Policy and IDPS Deployment]*

NDA — Non-disclosure agreement - protects findings and client data; often mutual. *[Engagement Management; Engagement Methodology and Reporting]*

NDA (Non-Disclosure Agreement) — Binds the tester to keep client data and findings confidential. *[Pentest Methodologies]*

NDP (Neighbor Discovery Protocol) — Five ICMPv6 messages (types 133-137) that replace ARP, router discovery and ICMP redirects (RFC 4861). *[IPv6 in Depth: Addressing, NDP, SLAAC, Security]*

Nearly 4 days — access to ransomware deployment *[IBM Breach Cost and X-Force Index 2024]*

Negligent insider — no intent to harm: mis-sent email, public cloud share, ignored policy; the most frequent category. *[Insider Threat Program]*

Neighbour type — eBGP over iBGP, then lowest IGP metric to next hop *[Routing II: EIGRP, BGP at the Enterprise Edge, Redistribution]*

Nested virtualization — Running a hypervisor inside a VM; the real hypervisor (L0) emulates VT-x or AMD-V for the guest hypervisor (L1). *[Virtualization Internals and VM Isolation]*

NetBIOS / NBT-NS / LLMNR — legacy Windows naming (NetBIOS Name Service) and Link-Local Multicast Name Resolution: fallbacks that any host can answer, so an attacker (Responder tool) impersonates the target and captures hashes. *[Networking Ports and Protocols]*

NetFlow / IPFIX — Per-connection summaries exported by routers/firewalls. High fan-out (one src to many dst/ports) is the flow signature of scanning. *[Network Scanning and Enumeration Reference (Authorized Labs)*]

Network / API access — private endpoints, VPC (virtual private cloud), NACL (network ACL), WAF, mTLS (mutual TLS), egress allowlists *[Securing AI Systems]*

Network namespace — Isolated copy of the network stack (interfaces, routes, rules, nftables, sockets); the basis of containers and of lab topologies on one host. *[Linux Networking Toolbox]*

Network sniffing — Passive capture on a shared segment. Obj 2.1 flags IoT/OT protocols (Modbus, DNP3) that are plaintext by design - creds and register values ride in clear. *[Reconnaissance and OSINT]*

NetworkPolicy default deny — per namespace, egress too, block 169.254.169.254 *[Kubernetes Security]*

Never exposed — hypervisor management never on production or Internet *[VMware vSphere and ESXi Security]*

Never go rogue — follow the plan, escalate, document; no lone heroics *[CISM Exam Strategy]*

NFS / SAN — Network File System (TCP/UDP 2049; restrict exports, root_squash, NFSv4 with Kerberos) and storage area network (zoning, LUN masking, encryption at rest). *[CompTIA SecurityX CAS-005 - Exam Overview]*

NGFW (next-generation firewall) — Firewall that filters by application and user identity, not only port, and can inspect TLS and run IPS signatures. *[Security Architecture - Resilience, Controls, Zero Trust]*

NHI — Non-human identity: service account, API key or pipeline credential used by software rather than a person. *[Start-ups, Municipalities, Teleassistance, Open Source]*

NICE Framework — US Workforce Framework for Cybersecurity (NIST SP 800-181 Rev. 1, 2020) organising work roles as sets of task, knowledge and skill statements; role catalogue updated regularly by NIST *[Career Map of Cyber Security Roles]*

NIDPS (network-based IDPS) placement (4.2.2) — Management network or VLAN for sensor traffic; inline where prevention is wanted, passive at network divisions and key segments such as the DMZ. *[Firewall Policy and IDPS Deployment]*

NIS rule 3 — rule 3 of the French NIS decree (arrete 14/09/2018): operators of essential services accredit each essential IS. *[Security Accreditation (Homologation)*]

NIS2 — EU Directive 2022/2555 on network and information security: risk measures and 24 h / 72 h incident reporting for essential and important entities. *[Business Travel and SME Cybersecurity; ENISA ETL 2024, DoD Zero Trust, ATT&CK for ICS]*

NIS2 EE / EI — Entites essentielles / entites importantes: the two NIS2 categories, with different supervision and fines. *[Start-ups, Municipalities, Teleassistance, Open Source]*

NIS2UmsuCG — German NIS2 transposition act (adopted Nov 2025) extending BSI supervision to roughly 30,000 entities. *[NCSC, BSI and Allied Cyber Authorities]*

NIST AI 600-1 (July 2024) — The Generative AI Profile of the AI RMF: twelve risks unique to or amplified by GenAI and about 200 suggested actions, each tagged with an RMF sub-category id such as GV-1.1-001 or MS-2.7-001. Use it as the checklist behind objective 4.2. *[AI Governance and Risk]*

NIST CSF 2.0 — US National Institute of Standards and Technology Cybersecurity Framework (Feb 2024): six functions

Govern, Identify, Protect, Detect, Respond, Recover. *[CompTIA Security+ SY0-701]*

NIST SP 800-207 — Special Publication 'Zero Trust Architecture' (2020): policy engine, administrator and enforcement point (objective 1.2). *[CompTIA Security+ SY0-701]*

NIST SP 800-61r3 — 'Incident Response Recommendations and Considerations for Cybersecurity Risk Management' (April 2025), maps IR onto CSF 2.0; revision 2 gave the classic four-phase IR lifecycle. *[CompTIA Security+ SY0-701]*

Nits — Candela per square metre: screen brightness; ~250-350 office, 1000+ for HDR. *[Power, Displays, Peripherals and Printers]*

NLA — Network Level Authentication: RDP users authenticate before a desktop session is created. *[Start-ups, Municipalities, Teleassistance, Open Source; Networking Ports and Protocols +1]*

NLP (natural language processing) — Understanding and generating language: tokenisation, embeddings, classification, translation, summarisation. LLMs and SLMs are its generative branch. *[AI Fundamentals for Cybersecurity]*

NLRI — Network Layer Reachability Information: the list of prefixes an UPDATE message announces with the attached path attributes. *[BGP and Internet Routing in Practice]*

no_new_privs — Flag (NoNewPrivs: 1): execve never grants privilege (setuid and file caps ignored); set by allowPrivilegeEscalation: false. *[Linux Isolation Primitives and Sandboxes]*

No security guarantee — Nothing is 100% secure; the goal is to make attacks too costly for their reward *[OWASP Developer Guide v4.2 - Chapter by Chapter]*

NodePort — A Service type that opens the same high port (30000-32767) on every node so an app is reachable without a cloud load-balancer. *[Kubernetes hands-on: learn it in your own lab]*

Noisy neighbour — One VM starves CPU, memory or I/O of co-located VMs; a denial of service in practice (risk 2). Reservations and limits. *[ToIP and Virtualization Security]*

Nomenclature — CVSS-B = base only; CVSS-BT adds Threat; CVSS-BTE adds Environmental. State which you used. *[Report Templates and Severity Rating]*

Non-public CA — CA trusted only inside the IS; the only kind allowed to sign the forged certificates a proxy shows its clients (R4). *[HTTPS Flow Inspection: Proxy and Reverse Proxy]*

Non-repudiation — Ability to prove to a third party who signed; only asymmetric signatures support it, because only the signer holds the private key. *[Crypto Mechanisms, Key Policy and AES Internals]*

Non-resignability — A third party cannot re-sign an unknown message from its signature; the DRKey key-establishment protocol was vulnerable without it. *[ANSSI Crypto Rules Catalogue (PG-083 v3.00)]*

Nonce — Number used once: per-message input (96 bits for AES-GCM) that must never repeat under the same key; it need not be secret and is stored beside the ciphertext. *[Cryptography in Code]*

Nonce (CSP) — Random value (at least 128 bits, base64) generated fresh for every response and placed both in the CSP header and in the nonce attribute of each allowed script tag. *[HTTP Security Headers and Browser Policies]*

Nonce / IV — Public value that must never repeat under the same key (nonce) or be unpredictable (CBC IV). Not secret. *[Cryptography; Cryptography Primer]*

Noninterference (Goguen-Meseguer) — High-level actions must not affect what low-level users observe; addresses covert channels and inference. *[CISSP Domain 3: Security Architecture and Engineering]*

Nonrepudiation — The originator cannot deny an action; needs digital signatures plus identity binding, not symmetric MACs. *[CISSP Domain 1: Security and Risk Management]*

North-south vs east-west — North-south crosses the perimeter (internet edge); east-west is internal lateral traffic. Instrument both: many attacks are only visible east-west. *[Network Traffic Analysis: Zeek and Suricata]*

NoT (Network of Things) — A distributed system of 'things' that sense, compute, communicate and actuate. **IoT** is one kind of NoT whose things are tethered to the Internet; a closed factory LAN of sensors is a NoT that is not IoT. SP 800-183 does not define what a 'thing' is: it defines five building blocks (primitives) whose behavior can... *[Networks of Things SP 800-183]*

Notarization — Apple's automated malware scan of Developer ID software; a passing build gets a ticket, stapled to the app or fetched online. Required for new software since macOS 10.15 Catalina; submitted with `xcrun notarytool`. *[macOS Security for Defenders]*

NPU — Neural processing unit for on-device AI; Microsoft **Copilot+ PC** requires an NPU of 40+ TOPS (tera = 10^{12} oper-

ations per second, the usual NPU speed metric) (Snapdragon X, Core Ultra 200V, Ryzen AI 300). *[CPUs, Memory, Motherboards and Buses]*

NSE — Nmap Scripting Engine: scripts for version detail, vulnerability checks and (intrusive) brute force. *[Network and Infrastructure Assessment]*

NSG (network security group) — stateful 5-tuple rules, priority 100-4096 (lower wins), on subnet and/or NIC (both are evaluated); default rules 65000+ allow VNet and load balancer, deny Internet inbound. Service tags (Storage, AzureCloud, Internet) replace IP lists. *[Azure and Entra ID Security Essentials]*

NSM — Network Security Monitoring: collection, detection and analysis of network data to find intrusions the endpoint missed. *[Network Traffic Analysis: Zeek and Suricata]*

NSRPC — Stormshield's command protocol and CLI (TCP 1300) used by admin tools and scripts; also available as a console inside the web UI. *[Stormshield SNS 3.7.17 Hardening by Chapter]*

NSS — Name Service Switch: glibc layer that resolves users, groups and hosts from files, LDAP or SSSD. *[GNU/Linux BP-028: Kernel Build, Files and Services]*

NSS (Name Service Switch) — `/etc/nsswitch.conf` decides where names come from (files, SSSD, LDAP); `getent passwd alice` shows the answer the system really uses. *[Linux Users, Groups, Permissions and ACLs]*

NSX — micro-segmentation: Manager (rules), Controllers (consistency), ESXi kernel module (per-vNIC firewall), optional Edges (replaceable by physical firewalls). *[VMware vSphere and ESXi Security]*

NTDS.dit — The AD database file on every DC; it contains all password hashes, so a DC's disk or backup is a Tier 0 secret. *[On-Prem Active Directory Architecture]*

NTLM — older challenge-response authentication; the password hash itself is the secret, so a stolen hash can be replayed (pass-the-hash) or relayed. *[Windows and Active Directory for Defenders]*

NTLM relay — Forwarding a victim's NTLM authentication to another server (LDAP, SMB, HTTP) to act as the victim. *[ANSSI Active Directory Recommendation Catalogue; Active Directory Security +1]*

NUD and cache states — INCOMPLETE → REACHABLE → STALE → DELAY → PROBE; STALE entries are reused un-

til traffic triggers a probe. Seen in `ip -6 neigh`. *[IPv6 in Depth: Addressing, NDP, SLAAC, Security]*

NUD state — Neighbour Unreachability Detection state of an ARP / NDP entry: REACHABLE (confirmed recently), STALE (usable, unconfirmed), DELAY, PROBE, FAILED, PERMANENT (static). *[Linux Networking Toolbox]*

Nudge — change in the choice architecture that steers behaviour without forbidding options: secure defaults, report button in the toolbar, banner on external email *[Security Awareness and Culture Programme]*

NULL — The marker for unknown or missing; NULL = NULL is not true, so test it with `IS NULL`. *[SQL Basics for Security]*

Null MX (RFC 7505) — `example.com. MX 0 .` declares that the domain accepts no mail; pair with SPF `-all` and DMARC `p=reject` on parked domains. *[Email Security: SPF, DKIM, DMARC]*

Numbers quoted by INTERPOL — Weekly attacks per organisation in Africa +23% YoY, highest in the world (Check Point); 1 in 15 African organisations saw a weekly ransomware attempt in Q1 2023 vs 1 in 31 globally; 10,490 cybercrime arrests reported by 19 countries; phishing emails the main BEC vector in nearly 80% of countries. *[Edge, Readiness and Awareness Reports]*

NVD — US National Vulnerability Database (NIST): enriches CVEs with CVSS, CWE and CPE product identifiers *[Vulnerability Management Programme]*

NVIDIA confidential computing — H100 (Hopper) first GPU with a CC mode: HBM memory protected, device identity key fused at manufacture, SPDM attestation; driver in the CVM encrypts traffic to the GPU through bounce buffers; Blackwell adds TEE-I/O with inline PCIe IDE and a protected multi-GPU mode *[Confidential Computing and Remote Attestation]*

NVT — Network Vulnerability Test: one Greenbone check script (about 100 000+ in the community feed, estimate), identified by an OID. *[Vulnerability and Configuration Scanners for Your Own Estate]*

O

OAEP / PSS — Optimal Asymmetric Encryption Padding and Probabilistic Signature Scheme: the modern, provably safer paddings for RSA encryption and RSA signatures (PKCS #1 v2). *[Cryptography Primer]*

Obfuscation — Make data hard to read without keyed encryption (minification, steganography, XOR, base64). Not a control on its own. *[Data Protection and Resilience]*

Obfuscation and serialization — Obfuscation hides code/logic (minification, packing) - not security, slows reversing; serialization formats (JSON, Python pickle, Java serialization) must be signed/validated because deserializing untrusted data can give RCE (remote code execution, objective 4.2). *[Cryptography Engineering and PQC]*

Object — Passive entity (file, database, printer) that holds or receives information. *[Firewall Policy: Design, Cleanup, Exposed Zone; CISSP Domain 5: Identity and Access Management +1]*

Object Lock — S3 feature enforcing WORM retention per object version, in governance or compliance mode, plus legal holds. *[Storage and Filesystems for Defenders]*

Objectif vise — why: the couple SR/OV is the unit of workshop 2 *[EBIOS Risk Manager]*

Objective at stake — which business objective or asset the scenario threatens *[CRISC Practice Scenarios]*

Objectivity — Individual auditor's impartial, unbiased attitude; impaired by auditing one's own work or a recent former role. *[CISA Domain 1: Information System Auditing Process]*

Observation / OFI (opportunity for improvement) — opportunity for improvement, not a failure; auditors cannot consult (ISO 19011 independence) *[ISO/IEC 27001:2022 and 27002:2022]*

OCI (Open Container Initiative) — Standards for image format, registry API and runtime so that Docker, Podman, containerd and Kubernetes interoperate. *[Docker and Containers Hands-On]*

OCI runtime — Program (runc, crun, gVisor runsc) that creates the container from an Open Container Initiative bundle. *[Docker Container Security; Linux Isolation Primitives and Sandboxes]*

OCSF — Open Cybersecurity Schema Framework: vendor-neutral event schema organised in categories and classes (class_uid) with numeric activity and status ids. *[Observability and Security Telemetry Pipelines]*

OCSP / CRL — Online Certificate Status Protocol (ask the CA about one certificate) / Certificate Revocation List (download the CA's list of revoked serial numbers). *[TLS and Certificates in Practice]*

OCSP (RFC 6960) — Per-certificate status query; the responder certificate carries id-pkix-ocsp-nocheck; stapling (RFC 6066) lets the server present a fresh signed response. *[PKI and ACME Certificate Automation]*

OCSP stapling — Server attaches a signed, recent OCSP response so clients need not query the CA; CRLs are the older batch list. *[Remote Work (Digital Nomadism); TLS, IPsec and SSH Hardening +3]*

ODP declared as a variable — Each ODP has its own determination statement ("frequency ... is defined"). An undefined ODP makes every dependent statement other than satisfied, as in the CP-03 example of Appendix E. *[SP 800-53A and 800-53B in Practice]*

ODP (organization-defined parameter) — Bracketed value the organisation must fill in, e.g. AC-7 Unsuccessful Logon Attempts: lock after [Assignment: number] invalid attempts in [time period]. Assessors check that every ODP is documented in the SSP and that the system actually enforces that value. Baselines and FedRAMP pre-fill many ODPs (FedRAMP AC-7: ... *[NIST SP 800-53r5 Controls in Practice; SP 800-53 Rev. 5 Security and Privacy Controls]*

Offences at stake — Secrecy of private correspondence (Code pénal art. 226-15), personal-data offences (226-16 to 226-24), private life (226-1 to 226-7). *[HTTPS Flow Inspection: Proxy and Reverse Proxy]*

Offline backup — copy on a medium disconnected from any information system (tape is still the most effective); ransomware cannot reach it. *[IT Backup - ANSSI BP-100 R1-R32]*

offline or immutable — air gap, tape, Object Lock; attacker with domain admin cannot delete *[Backup and Recovery Engineering; Ransomware Defense End to End]*

Offline vs online cracking — Offline = guessing against a stolen hash file with no rate limit (fast, invisible to you). Online = guessing against your live login (slow, rate-limited, logged). *[Password and Hash Auditing for Defenders]*

OffSec — Offensive Security, the company behind the PEN-200 course and the hands-on OSCP exam. *[Security Certification Landscape; Kali Linux and Security Distros: Orientation for Learners]*

OIDC — OpenID Connect: identity layer on top of OAuth 2.0 that returns an ID token describing the logged-in user. *[OWASP ASVS 5.0 - Application Security Verification Standard]*

OIDC attacks — Abuse OAuth2/OpenID Connect: replayed access/refresh tokens, redirect_uri tampering, missing PKCE. Defend with exact redirect match, PKCE, short TTL, nonce/audience checks. *[Network and Authentication Attacks]*

OIDC federation — A CI/CD job exchanges a signed identity token for short-lived cloud credentials, so no stored keys are needed. *[Cloud Configuration Review]*

OIDC federation (CI) — The CI platform issues a signed short-lived identity token per job that the cloud exchanges for temporary credentials, replacing stored keys. *[Infrastructure as Code and Secrets]*

OIV (opérateur d'importance vitale) — operator designated under the LPM (loi de programmation militaire, the 2013 military programming law whose article 22 created cyber duties) in one of the 12 SAIV sectors; list is classified (about 250 operators); must protect its SIIV *[Priority Measures and Essential Systems]*

OIV / OSE — operators of vital importance (French LPM critical operators) / operators of essential services (NIS1); NIS2 now speaks of essential and important entities. *[IoT/IIoT Security and OT Detection]*

OIV / OSE / FSN — Operator of vital importance (French LPM) / operator of essential services (NIS) / digital service provider (NIS). *[Local Authorities: the Regulatory Security Framework]*

OIV / SIIV — operators of vital importance (Defence Code) and their critical IS; cyber obligations since the 2013 military programming law, detailed in sector orders. *[Cloud Hosting for Sensitive Systems; Cyber Incident Reporting Obligations]*

OLA — Internal operational agreement between IT teams that supports an SLA. *[CISA Domain 4: IS Operations and Business Resilience]*

OLM (Operator Lifecycle Manager) — Installs, updates and manages operators and their RBAC from catalogs such as OperatorHub. *[Helm, operators and the CRD ecosystem (with security)]*

On-call — Period when a person must be reachable and able to respond within an agreed time, outside normal hours; in French law 'astreinte'. *[Working Life in Security]*

On-demand self-service — consumer provisions compute/storage without human interaction with the provider *[Cloud Computing Security]*

On-premises vs cloud vs hybrid — Hybrid needs one policy plane and one log plane; inconsistent controls between the two halves are the classic exam gap. *[Security Operations Architecture]**

Ongoing authorization (2.2) — Authorization decisions refreshed by monitoring data instead of fixed re-authorization cycles (traditionally every 3 years); ISCM is the Risk Management Framework (RMF, SP 800-37) Monitor step at scale. *[Log Management and ISCM in Depth]**

OOB authenticator — Out-of-band factor: a code or approval sent over a second channel (SMS, push, phone call). *[ASVS 5.0 - Chapter Highlights and 4.0.3 Delta]**

Open design — Security must not depend on the design being secret *[OWASP Developer Guide v4.2 - Chapter by Chapter]**

Open redirect — A page that forwards the user to any URL given in a parameter, abused to make phishing links look trusted. *[OWASP Top 10 2017 and Risk Rating]**

OpenCRE — Open Common Requirement Enumeration: OWASP site linking equivalent requirements across standards. *[OWASP ASVS 5.0 - Application Security Verification Standard]**

OpenID Connect (OIDC) — Identity layer on OAuth 2.0: the identity provider (IdP) authenticates the user and returns a signed ID Token to the client application (service provider, relying party). *[ANSSI Identity: MFA, AD Tiering, OpenID Connect]**

OpenSCAP / SSG — Open-source SCAP (Security Content Automation Protocol) scanner; the SCAP Security Guide ships XCCDF benchmark profiles, including ANSSI BP-028 ones. *[GNU/Linux BP-028: Kernel Build, Files and Services]**

OpenTelemetry (OTel) — CNCF project (merger of OpenTracing and OpenCensus, 2019) defining vendor-neutral APIs, SDKs, the OTLP protocol, semantic conventions and the Collector for traces, metrics and logs. *[Observability and Security Telemetry Pipelines]**

Operations — **Nervone** (June 2023) arrested key members of OPERA1ER, a French-speaking financial-crime group (up to \$35M stolen across 15 countries); **Jackal** targeted West African groups including Black Axe; **Africa Cyber Surge II**. Legal anchors: Malabo Convention (AU), Budapest Convention. *[Edge, Readiness and Awareness Reports]**

Operator — A controller that watches custom resources and reconciles real cluster objects to encode an application's operational knowledge. *[Helm, operators and the CRD ecosystem (with security)]**

Operator Lifecycle Manager (OLM) — A framework that installs, updates and manages operators and their RBAC from catalogs such as OperatorHub. *[Helm, operators and the CRD ecosystem (with security)]**

Operator SDK — Red Hat toolkit for Go, Ansible or Helm-based operators; packages them as bundles for OLM. *[Helm, operators and the CRD ecosystem (with security)]**

Oracle — service that brings off-chain data (prices, events) on-chain; a trusted input the contract cannot verify *[Blockchain and Smart-Contract Security]**

Orchestration — Several automated tasks across different tools chained into one workflow with decisions (a SOAR playbook). *[Incident Response, Forensics, Automation]**

Orchestrator — Scheduler that places containers on hosts and manages network and secrets (Kubernetes). *[Container and Virtualization Security]**

Order of volatility — the sequence for collecting evidence from most to least perishable (RFC 3227); memory before disk. *[DFIR Artifacts and Tools; CISA Domain 5: Protection of Information Assets]**

Order of volatility (RFC 3227) — Collect in order: CPU registers and cache, RAM, network state and running processes, disk, remote logs, archival media. Image memory before pulling the plug. *[SANS Incident Handling]**

Organisational independence — The audit function reports to a level that lets it act free of interference, normally the audit committee (ITAF 1002). *[CISA Domain 1: Information System Auditing Process]**

Organisational Unit (OU) — A container for users/computers used to link Group Policy and delegate admin rights. Not a security boundary: a domain admin can act in any OU. *[On-Prem Active Directory Architecture]**

Organizational Profile — Description of an organization's current and/or target cybersecurity posture in terms of Core outcomes. **Current Profile** = outcomes being achieved now and how. **Target Profile** = desired outcomes, prioritized from mission, risk appetite, regulations and threat intelligence. *[NIST Cybersecurity Framework 2.0]**

Organizational Unit — closest OU wins; Enforced links and Block Inheritance change the order *[Windows and Active Directory for Defenders]**

Organized crime — money: ransomware, BEC (business email compromise), carding (stolen card fraud) *[Threat Actors and Threat Vectors]**

Origin — The triple scheme + host + port of a URL; the unit of isolation in the browser. *[HTTP Security Headers and Browser Policies; How the Web Works for Security People]**

Origin validation (R40) — Compare Origin to a strict allowlist; never reflect it blindly, never * with Access-Control-Allow-Credentials: true. *[Browser-Side Web Security Standards]**

Orphan object — Object used in no rule any more after deletions; removed at every cleanup iteration. *[Firewall Policy: Design, Cleanup, Exposed Zone]**

OSE -> EE / EI — operators of essential services under NIS1; NIS2 replaces them with essential and important entities once transposed. The guide still uses OSE. *[Cloud Hosting for Sensitive Systems]**

OSE (opérateur de services essentiels) — organisation designated by the French Prime Minister under the NIS 1 directive because it provides a service essential to society or the economy (energy, transport, health, banking...). *[Protecting Essential IS - PA-085 R1 to R62]**

OSE / SIE — operator of essential services designated by the Prime Minister under NIS 1; its essential information systems (SIE) follow the 23 rules of the arrete; FSN (digital service providers) follow Regulation 2018/151 *[Priority Measures and Essential Systems]**

OSINT (Open-Source Intelligence) — Information gathered from public sources: websites, DNS, social networks, code repositories, breach dumps. *[Pentest Methodologies]**

OSNMA — Galileo Open Service Navigation Message Authentication: signed navigation messages that let a receiver detect spoofed Galileo signals. *[Cyber Security On Board Ships]**

osquery — Open-source agent that exposes a computer's state (processes, users, ports, installed software) as SQLite tables that you query with SQL. *[SQL Basics for Security]**

osquery SQL — SQLite dialect exposing live operating-system state as tables (processes, listening_ports, users); run ad hoc or on a schedule through a fleet manager such as Fleet. *[Query Languages: KQL, SPL, EQL, ES|QL, osquery]**

OSSTMM — Open Source Security Testing Methodology Manual (ISECOM): a measured, repeatable security testing method. *[CompTIA CySA+ CS0-003; CompTIA PenTest+ PT0-003]**

OT — Operational technology: computers that drive physical processes (engines, steering, ballast), as opposed to office IT. *[Cyber Security On Board Ships]**

OT DMZ — Buffer network between enterprise and control networks; IT and OT each talk only to servers in it, never directly to each other. *[OT Architecture and the SP 800-82r3 OT Overlay]*

OT / ICS / SCADA — Operational Technology; Industrial Control Systems; Supervisory Control and Data Acquisition: plant and utility systems where an active scan can stop a process. *[CompTIA CySA+ CS0-003; Vulnerability Scanning Methods]*

OT (operational technology) — Programmable systems that interact with the physical world: they monitor or change physical processes, devices and events. *[NIST OT and IoT Security]*

OT / PLC — Operational Technology (industrial control systems) / Programmable Logic Controller; OT protocols (Modbus, DNP3, S7comm, EtherNet/IP, BACnet) were designed without authentication. *[Networking Ports and Protocols]*

OTA update — over-the-air firmware update; must be signed, verified on the device and protected against rollback to an older vulnerable version. *[IoT/IloT Security and OT Detection]*

OTAA vs ABP (LoRaWAN) — Over-The-Air Activation derives fresh session keys at each join; Activation By Personalisation hard-codes session keys and counters, which weakens replay protection. *[IoT/IloT Security and OT Detection]*

Other HSM schemes — Common Criteria EN 419221-5 protection profile (trust services, eIDAS = EU electronic identification and trust services regulation, qualified signature devices), PCI PTS HSM (payment card industry PIN transaction security, for payment HSMs), ANSSI **qualification** (French state approval: product certified by CC or... *[HSMs, Supply Chain, Physical Security, Decommissioning]*

OTLP — OpenTelemetry Protocol: protobuf messages over gRPC (port 4317) or HTTP (port 4318, paths /v1/traces, /v1/metrics, /v1/logs). *[Observability and Security Telemetry Pipelines]*

OTP / HOTP / TOTP — One-time password; HMAC-based OTP (counter-driven, RFC 4226); time-based OTP (30-second window, RFC 6238), both computed from a shared seed. *[Authentication, MFA and Passwords]*

OU (Organizational Unit) — Folder inside a domain that holds users, groups, computers or other OUs; the unit for Group Policy links and delegated rights. *[Windows Administration and Active Directory Basics]*

OUI — Organizationally Unique Identifier: first 24 bits assigned by IEEE to a vendor (00:50:56 VMware, 00:0c:29 VMware

Workstation, 52:54:00 QEMU/KVM by convention). Fingerprints devices, not proof of identity. *[Ethernet, MAC Tables and ARP]*

Out-of-band communication — Talking over channels the attacker cannot see (phones, a separate chat tenant), never the compromised email. *[Business Continuity and ISO 22301; SANS Incident Handler Checklists and Enterprise IR]*

Out-of-band management — iLO (HPE), iDRAC (Dell), IPMI: server management controllers with full hardware control, to be reachable only from the admin zone. *[Segmentation and IS Mapping; Operations, Security, Troubleshooting: Self-Assessment]*

Out-of-band (OOB) management — A separate network used only to administer devices, isolated from user and production traffic, so an attacker on the data path cannot reach the control plane. *[Classic Enterprise Network Architecture]*

Outcome — A desired result stated without saying how to reach it ("users are authenticated", not "deploy product X"); the unit a Profile scores. *[CSF 2.0 Core: the 106 Outcomes Explained]*

Output drops / discards — Egress queue full: congestion or microbursts, not a cable problem; fix with capacity or QoS. *[Network Troubleshooting: Method, Layers, Tools, Symptoms]*

Overlay — Virtual network built on the underlay by encapsulation; tenant-visible subnets and segments independent of the physical topology. *[Overlay, Data-Centre and Cloud Network Internals; OT Architecture and the SP 800-82r3 OT Overlay]*

Overlay network — Pod packets wrapped in an outer UDP/IP packet between node addresses (VXLAN, Geneve), so the physical network only knows node IPs. *[Kubernetes and Container Networking Explained]*

Overt / covert test — Overt (white hat): IT staff informed. Covert (black hat): only management knows, so detection and response are tested too. *[Security Testing and Assessment in Depth]*

Overt testing — White hat: IT staff know and help, lower impact, doubles as training (SP 800-115 2.4.2). *[PTES Phase Tasks, SP 800-115, Kill Chain Analysis]*

Overt vs covert — Perceptible mark (logo) vs machine-readable perturbation (e.g. least significant bits) that needs a detector with non-zero false positive and false negative rates. *[GenAI Secure Development and Content Transparency]*

OWASP threat modeling — Four questions: what are we working on, what can go wrong, what are we going to do about it,

did we do a good job. Tools: OWASP Threat Dragon, Microsoft Threat Modeling Tool, pytm (threat model as code). *[Compliance, Threat Modeling and AI Security]*

OWASP Top 10 — Top web app risks. OWASP MASVS covers mobile app verification. *[CompTIA PenTest+ PT0-003; CompTIA Security+ SY0-701]*

OWE (Opportunistic Wireless Encryption) — RFC 8110, Wi-Fi Alliance 'Enhanced Open': an open network where client and AP run an unauthenticated Diffie-Hellman exchange inside the association request and response (OWE element), derive a PMK and run the normal 4-way handshake. Result: each client gets its own keys, so passive listeners in the café see only... *[Wi-Fi Security Internals; Wireless Security and IDS/IPS]*

Own build — CGO off, -trimpath, stamped version *[Go for Security Tooling and Safe Code]*

Own team finds more — 42% internal detection (IBM) *[IBM Breach Cost and X-Force Index 2024]*

Own vs shared resources — own: only this domain can act on it (process memory, execution context); shared: several domains can (files, kernel, hardware). The split of resources is the security policy. *[System Partitioning: ANSSI PG-040]*

Owner — Person or organization owning a primitive (operator role included); may be several, anonymous or malicious. *[Networks of Things SP 800-183]*

Owner decides — practitioner advises; owner accepts and treats *[CRISC Exam Strategy]*

Owner reference — Field `metadata.ownerReferences` linking a child to its parent (Pod → ReplicaSet); the garbage collector deletes children of a deleted owner. *[Kubernetes Architecture in Depth]*

P

PAC — Pointer Authentication Codes (ARMv8.3): cryptographic signature on return addresses and pointers against code-reuse attacks. *[Mobile Device Security and MDM]*

Pack — named group of osquery scheduled queries with platform and version filters, shipped as a JSON file (incident-response, ossec-rootkit, it-compliance...). *[osquery and Velociraptor for Fleet Visibility]*

Package — The unit of compilation and import; `package main` with `func main()` builds an executable, any other name builds a library. *[Go Programming from Zero (Part 1: language basics)]*

Package manager — A tool that installs, updates and removes software from signed repositories and tracks which file belongs to which package. *[Operating System Concepts for Beginners]*

Packer — tool that compresses or encrypts an executable and unpacks it in memory at run time (UPX, Themida, VMProtect), hiding strings and imports from static analysis. *[Malware Triage and Analysis]*

Padding oracle — Server reveals whether CBC padding was valid, letting an attacker decrypt data byte by byte without the key. *[WSTG v4.2 - Complete Test Catalogue]*

Page-table entry (PTE) — 8-byte record mapping one virtual page to a physical frame, with permission bits (present, writable, user, no-execute) that transient attacks bypass and Rowhammer flips. *[CPU Side Channels and Memory Attacks]*

Pagefile / hiberfil — pagefile.sys holds pages swapped out of RAM; hiberfil.sys is a compressed RAM copy written at hibernation. Both extend the evidence and are collected with the disk image. *[Memory Forensics with Volatility 3]*

Pairwise pseudonymous identifier (3.4.1) — Different subject identifier per RP, no PII inside, unguessable; shared across RPs only when the trust agreement designates it. Blocks cross-RP tracking. *[Proofing Evidence and FAL Requirements]*

PAKE — Password-authenticated key exchange: lets a password authenticate a key exchange without allowing offline guessing. *[ANSSI Cryptographic Mechanisms and PQC]*

PAM — Privileged access management: vaulting, just-in-time elevation, session recording for admin accounts. *[Linux and Cloud Logging; CISA Domain 5: Protection of Information Assets +4]*

PAM and privileged identity management — Vault with password check-out, session recording, JIT (just-in-time) elevation with approval and expiry, break-glass (emergency) accounts monitored, tiered admin model (Tier 0 = domain controllers, PKI, IdP administered only from dedicated workstations). *[Security Engineering - IAM, Endpoints, Network, Hardware, OT, Automation]*

PAMS — Prestataire d'administration et de maintenance sécurisées: ANSSI qualification scheme for outsourced administration providers. *[ANSSI Secure Administration of IS (PA-022)]*

Parameterised query — A query sent with placeholders and separate values, so input is always treated as data; the standard defence against SQL injection. *[SQL Basics for Security]*

Parameterized query — SQL sent with placeholders (?, \$1, %s, :name); values travel separately, so the database never parses them as SQL. *[Secure Coding Patterns by Vulnerability Class]*

Paranoia level — CRS setting 1-4 that selects how strict and numerous the active rules are; blocking and detection levels can differ. *[WAF and API Gateway Configuration]*

Partitioning (cloisonnement) — Guarantee that a domain cannot reach another domain's resources except through a policy enforced by the **reference monitor** (MAC such as SELinux/AppArmor in the base). *[Multi-Environment Workstation and Refurbishing]*

Partitioning (confinement) — the security function guaranteeing a task can only perform the actions the policy allows on resources. *[System Partitioning: ANSSI PG-040]*

PAS — Plan d'Assurance Securite (security assurance plan): the provider's contractual description of how it meets the client's security requirements. *[IT Usage Charter and Outsourcing Security]*

Pass-the-hash — Authenticating with a stolen NTLM hash instead of the password, which NTLM allows by design. *[Active Directory Security]*

Pass-through audit — a provider's own certification (PCI DSS, SOC 1/2, HIPAA, CCM) that customers inherit for the provider's layers; a form of compliance inheritance. *[CSA Security Guidance v4: the 14 Domains]*

PASSI / PDIS / PRIS — ANSSI-qualified providers of security audits / incident detection (SOC) / incident response. *[IT Usage Charter and Outsourcing Security; Priority Measures and Essential Systems]*

Passive interface — OSPF interface whose subnet is advertised but on which no hellos are sent or accepted, so no adjacency can form there. *[Cisco IOS Configuration Lab]*

Passive scan — Analysis of traffic the proxy already saw (missing security headers, cookies without flags); it sends nothing extra, so it is safe on any target you may browse. *[Web and API Testing Toolkit for Your Own Apps]*

Passive vs active intruder — Passive only listens (eavesdropping, traffic analysis). Active records, replays, injects or modifies messages (Fig. 8-2). Every protocol in ch. 8 is designed

against the active one, called **Trudy**. *[Network Security I - Crypto, PKI, IPsec, Firewalls, Wi-Fi]*

Passkey — FIDO2 discoverable credential bound to an origin; phishing-resistant, replaces the password. *[Authentication, MFA and Passwords; CISSP Domain 5: Identity and Access Management +1]*

Passkey provider — Credential manager that stores and syncs passkeys: iCloud Keychain, Google Password Manager, Microsoft, or third parties such as 1Password, Bitwarden, Dashlane. *[Passkeys and Passwordless Authentication]*

Password dumps — Credential lists from past breaches. A tester checks whether client accounts appear and whether passwords follow a pattern; handle as sensitive personal data and never test them outside scope. *[Reconnaissance and OSINT]*

Password hash / KDF — A password-hashing function (Argon2id, bcrypt, scrypt, PBKDF2) is a deliberately slow, salted one-way function; slowness makes each offline guess expensive. *[Password and Hash Auditing for Defenders]*

Password hashing function — Deliberately slow, salted one-way function (Argon2id, scrypt, bcrypt, PBKDF2) that makes each offline guess expensive. *[Authentication and Session Design]*

Password spraying — Trying a few common passwords against many accounts to avoid lockouts. *[Cyber Crisis Communication; Authentication and Session Design]*

Password vaulting — Privileged and shared credentials stored in a vault; checkout with approval, session brokered and recorded, password rotated after each use so the human never learns it. LAPS does this for local admin passwords. *[Identity and Access Management]*

Passwords — Defaults (admin/admin), .env, web.config, wp-config.php, SAM hive, /etc/shadow. *[Enumeration and Scripting]*

Pastillage — Tagging a ballot with voter attributes (college, site) so one vote also counts in indirect elections. *[Internet Voting for Non-Political Elections]*

Patch — Additional code that changes software to fix a vulnerability or bug, or add a feature; also called update, hotfix, service pack. *[Patch, Configuration and Continuous Monitoring]*

PATH — environment variable listing the directories the shell searches, left to right, for a command typed without a slash; the first match wins. *[Master Any Command-Line Program Fast, on Every OS]*

Path condition — Flexible, survives updates; safe only if the folder and subfolders are writable by Administrators and SYS-

TEM alone (R7). AppLocker variables: %WINDIR%, %SYSTEM32% (includes SysWow64), %OSDRIVE%, %PROGRAMFILES%, %REMOVABLE%, %HOT%. *[Windows Application Control and Endpoint Monitoring]*

pathLenConstraint — basicConstraints field saying how many CA levels may exist below this one; 0 = this CA may only sign end-entity certificates. *[PKI Operations and Key Management]*

Patient zero — The first compromised machine or account; often demanded, but not always reachable or useful (old or destructive attacks). *[Incident Qualification & Remediation Decision Keys]*

PAW — Privileged Access Workstation: hardened workstation dedicated to administering one tier. *[Active Directory Security; Active Directory Tier 0 Remediation +2]*

PAW (Privileged Access Workstation) — A hardened, dedicated device used only for Tier 0/1 administration, never for email or web browsing, so admin credentials are never typed on a risky machine. *[On-Prem Active Directory Architecture]*

Pay transparency — EU Directive (EU) 2023/970 (transposition due 7 June 2026): candidates must receive the initial pay level or range before the interview, and employers may not ask about pay history; several member states transposed late, check national law *[CV, Portfolio and Job Interviews in Security]*

PCA / PRA — Plan de continuité / de reprise d'activité: business continuity plan / disaster recovery plan. *[Start-ups, Municipalities, Teleassistance, Open Source; Firewall Policy: Design, Cleanup, Exposed Zone]*

PCI DSS — Payment Card Industry Data Security Standard (v4.0.1 current): mandatory controls for anyone storing, processing or transmitting card data. *[CompTIA CySA+ CS0-003]*

PCI DSS v4.0.1 — Payment Card Industry Data Security Standard: mandatory contractual rules for anyone storing, processing or transmitting card data. *[CompTIA Security+ SY0-701]*

PCR — Platform Configuration Register: TPM register that can only be extended with hashes of boot components. *[Hardware Roots of Trust and the TPM 2.0]*

PCS — Plan communal de sauvegarde: the mayor's municipal emergency plan for major events, where the guide puts the cyber crisis chapter. *[Start-ups, Municipalities, Teleassistance, Open Source]*

PDC Emulator — The most operationally critical FSMO: it is the forest time root, processes recent password changes first, and is the default target for Group Policy edits. *[On-Prem Active Directory Architecture]*

PDIS — prestataire de détection des incidents de sécurité: SOC provider qualified by ANSSI. *[IoT/IIoT Security and OT Detection]*

PDIS / PRIS — ANSSI-qualified security incident detection / response providers (prestataires de détection / de réponse aux incidents de sécurité). *[ANSSI Logging and Security Supervision]*

PDIS / PRIS / PASSI — ANSSI-qualified providers of incident detection (SOC) / incident response / IS security audit. *[OT Detection Doctrine, Integrators and Training]*

PDMA — Perte de données maximale admissible: recovery point objective (RPO), maximum tolerable data loss. *[Internet Voting for Non-Political Elections]*

PDP (Policy Decision Point) — functions that evaluate access requests, take the decision and define the access conditions between subject and resource; the **control plane** with the PIP. *[ANSSI Zero Trust Model]*

PDU (Protocol Data Unit) — The unit a layer works with: bits (L1), frame (L2), packet (L3), segment or datagram (L4), data above. *[Network Models, Performance and the Physical Layer]*

PE / MZ — Portable Executable, the Windows format for .exe and .dll; every PE starts with the bytes MZ (0x4D 0x5A). *[Malware Triage and Analysis]*

PE (Portable Executable) — Windows format for .exe, .dll, .sys (drivers), .efi, .scr, .cpl; starts with MZ and holds a PE\0\0 signature at the offset stored at 0x3C. *[Executable Formats: ELF and PE]*

PEB — Process Environment Block: user-mode structure with the command line, environment and the loader's module lists; attackers can tamper with it, the VAD cannot lie as easily. *[Memory Forensics with Volatility 3]*

Peer review — A second tester checks each finding's evidence, severity and wording before release; catches false positives and overstatement. *[Engagement Management]*

PEM — Privacy-Enhanced Mail encoding: Base64 of the binary object between -----BEGIN ...----- and -----END ...----- lines; several objects can be concatenated in one file. *[OpenSSL and Certificate Tooling]*

PEN-200 — OffSec's Penetration Testing with Kali Linux course that prepares for the OSCP exam. *[OSCP / OSCP+: Exam Format and Rules]*

Penetration test — Overt, scope-bounded search for as many exploitable weaknesses as possible in named systems; the defenders usually know it is happening. *[Red Team Programme and Rules of Engagement]*

PEP — data plane - enables, monitors, terminates the connection *[Security Architecture - Resilience, Controls, Zero Trust]*

PEP (policy enforcement point) — Component (proxy, gateway, agent) that enables, monitors and terminates connections according to the policy decision. *[ANSSI Zero Trust Model; Secure Architecture Patterns]*

Pepper — Secret key applied to all hashes (HMAC before hashing, or encrypting the hash) and kept outside the database, in a vault or HSM. *[Authentication and Session Design; Password and Hash Auditing for Defenders]*

Performance-based question (PBQ) — A simulated task: classify log lines as prompt-injection attempts, pick gateway settings (rate, token, modality limits) for stated requirements, or match attacks to compensating controls. Practice the mappings, not only the definitions. *[CompTIA SecAI+ CY0-001; CompTIA SecurityX CAS-005 - Exam Overview]*

Perimeter appliances — edge CVEs exploited in days (Fortinet, M-Trends) *[Edge, Readiness and Awareness Reports]*

Permission boundary — AWS managed policy that caps the maximum permissions of a user or role without granting any. *[Cloud Entitlement Management and Least Privilege]*

Permission restrictions — Least privilege through ACLs, RBAC (role-based access control), DLP policies, IRM/DRM (information / digital rights management) on documents: no forward, no print, expiry. *[Data Protection and Resilience]*

Personal data (Art. 4(1)) — any information relating to an identified or identifiable natural person (data subject); identifiers include name, ID number, location data, online identifier (IP address, cookie ID), genetic or biometric factors *[GDPR for Security Teams]*

Personal data breach — GDPR Art. 4(12): breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data; ransomware encryption alone is one (loss of availability). *[Cyber Incident Reporting Obligations]*

Personal data breach (Art. 4(12)) — breach of security leading to accidental or unlawful destruction, loss, alteration, unautho-

rised disclosure of, or access to personal data: **confidentiality, integrity or availability** breach (ransomware without exfiltration is still a breach) *[GDPR for Security Teams]*

PERT — Network technique using optimistic, most likely and pessimistic estimates; expected time = $(O + 4M + P) / 6$. *[CISA Domain 3: IS Acquisition, Development and Implementation]*

PFS — Perfect forward secrecy: ephemeral DH per session, so a leaked long-term key does not decrypt past captures. *[HTTPS Flow Inspection: Proxy and Reverse Proxy; Cryptography Primer]*

PFS (forward secrecy) — Session keys derive from ephemeral DH keys erased after use, so a stolen server key cannot decrypt recorded sessions. *[ANSSI TLS and IPsec Guides: Full R Index]*

PFS (perfect forward secrecy) — Each rekey runs a fresh DH exchange, so stealing one key later does not decrypt earlier traffic. *[TLS, IPsec and SSH Hardening; VPNs in Depth: IPsec/IKEv2, TLS VPN, WireGuard +2]*

pgaudit — PostgreSQL extension writing detailed session and object audit records (statement class, object, command) to the server log. *[Database Security]*

PHB (per-hop behaviour) — The forwarding treatment (priority queue, bandwidth share, drop preference) a router gives to one DSCP class. *[VPN, Firewall Policy, Models, QoS: Self-Assessment]*

Philosophical / political beliefs — Hacktivism: defacement, leaks, DDoS against ideological targets. *[Threat Actors and Threat Vectors]*

Phishing resistance (Sec. 3.2.5) — Formerly verifier impersonation resistance. Two accepted methods: **channel binding** (client-authenticated TLS) and **verifier name binding** (WebAuthn: the browser gives the key the real site origin, so a look-alike domain gets no valid signature). Manually entered OTP or OOB codes are never phishing-resistant. *[Digital Identity Guidelines SP 800-63-4]*

Phishing-resistant — The credential is bound to the real site's origin (FIDO2/WebAuthn) or to a client certificate, so a relayed login on a fake site fails. *[ANSSI Identity: MFA, AD Tiering, OpenID Connect]*

Phishing (T1566) — Email with malicious link or attachment; check SPF (sender IP authorized), DKIM (signature valid), DMARC (From domain aligned), display-name spoofing, ur-

gency, mismatched reply-to. *[Indicators of Malicious Activity]*

Phone + PC — Maximum 2 is the usual minimum (PC data VLAN + phone voice VLAN); 3 covers the phone appearing in both VLANs on some platforms. *[First-Hop Security and Gateway Redundancy]*

Physical partitioning — distinct equipment and cabling per zone or IS (PG-075 R5 and R50, PA-108 R106 physical separation of ICS functional zones); cables of different sensitivity visually distinct, e.g. colours (PG-075 R38). *[Segmentation and IS Mapping]*

Physical vs logical access control systems — Badge systems (PACS = physical access control system) with anti-passback (a badge cannot enter twice without exiting) and mantraps (two-door airlock), integrated with HR and IdP so a leaver loses both badge and account in one workflow. *[Security Architecture - SDLC, IAM Design, Cloud]*

PID 1 (init) — First user-space process; adopts orphans and reaps zombies; if it dies the kernel panics. systemd on almost every modern distribution. *[Linux Boot, Processes and System Calls]*

PID (person identification data) — core identity attributes (name, date of birth, nationality, unique identifier where national law provides it) issued to the wallet by a member-state PID provider at LoA high *[eIDAS 2 and the EU Digital Identity Wallet]*

Pig butchering — long-running fake relationship ('fattening the pig') that ends in a fraudulent crypto investment. *[Industry and Workforce Reports]*

PII — Personally Identifiable Information: data that identifies a person (name, ID number, email, location). *[Attack Mitigation and Vulnerability Response]*

PII / PHI — Personally Identifiable Information (name + ID number, email...); Protected Health Information (medical data, HIPAA). *[CompTIA CySA+ CS0-003]*

Pilot — Deploys to one site or group first to validate before wider rollout. *[CISA Domain 3: IS Acquisition, Development and Implementation]*

PIM (Privileged Identity Management) — Entra ID P2 feature making admin roles eligible rather than permanent: the admin activates the role for a few hours with MFA, justification and optional approval, and every activation is logged. *[Microsoft 365 Hardening]*

PIM (Protocol Independent Multicast) — Routing protocol that builds distribution trees using the unicast table. PIM-SM (RFC 7761) starts from a shared tree rooted at a rendezvous point (RP), then switches to the shortest-path tree from the source. *[QoS, Multicast and WAN Services]*

PIP (Policy Information Point) — the set of attributes used by the PDP: subject, resource, context of the request (time, place, device compliance, threat level). *[ANSSI Zero Trust Model]*

Pipeline — Passes objects, not text: filter with `Where-Object`, pick fields with `Select-Object`, sort with `Sort-Object`. *[PowerShell for Defenders]*

PIR — Priority Intelligence Requirement: a question leadership needs answered to decide, e.g. which ransomware groups target European hospitals this year. *[Cyber Threat Intelligence Lifecycle]*

PIV / CAC — Personal Identity Verification card (civilian) / Common Access Card (defence): smart cards holding a certificate, phishing-resistant. *[CISA Zero Trust Maturity Model v2.0]*

Pivot domain controller — DC used during remediation to replicate the AD data in isolation, clean it, and let the new DCs replicate from it; specifically protected and supervised (no persistence on disk, in-memory operation). *[Active Directory Tier 0 Remediation]*

Pivot point — a known malicious fact (time, file, account) from which you search backwards and forwards in the timeline. *[DFIR Artifacts and Tools]*

PKCE — Proof Key for Code Exchange (RFC 7636): binds an authorization code to the client that requested it. *[ANSSI Identity: MFA, AD Tiering, OpenID Connect; Multi-Cloud Identity Federation +2]*

PKCS#11 SSH — `ssh -I /usr/lib/opensc-pkcs11.so host` uses a PIV/CAC certificate key; `ssh-add -s` loads it into the agent. Combine with `verify-required` FIDO2 keys for admins (ANSSI MFA guide PG-078 favours hardware factors). *[OpenSSH Hardening and Hardware Security]*

PKCS#12 — Public-Key Cryptography Standard 12 (.p12/.pfx): password-protected bundle of a private key, its certificate and the chain, used by Windows, Java keystores and browsers. *[OpenSSL and Certificate Tooling]*

PKI — Public Key Infrastructure: certificate authorities that issue and revoke the certificates behind TLS and signing. *[CompTIA CySA+ CS0-003]*

PKI (public key infrastructure) — The people, policies, software and hardware that create, distribute, validate and revoke digital certificates, so that a public key can be trusted to belong to a named person, server or device. *[PKI and Certificates]*

Plaintext / ciphertext — Readable data before encryption / scrambled output after encryption. *[Cryptography]*

Plan + implement — one step in CompTIA's list *[CompTIA A+ Core 1 - Hardware and Troubleshooting]*

Platform SSO — macOS 13+ (mature in macOS 14 Sonoma) extension that ties the local Mac account to an identity provider (Microsoft Entra ID, Okta, ...): login with the IdP password, a Secure Enclave key or a smart card, then single sign-on to apps. *[macOS Security for Defenders]*

Play App Signing — Google keeps the app signing key and signs the APKs it delivers; the developer keeps only an upload key, which can be reset if lost. *[Android Application Internals and Security]*

Playbook — Scenario-level plan (ransomware, phishing, data leak): decisions, roles, communications and which runbooks to call. *[SOC Operations and SOAR; Writing for Security Work]*

PLC — Programmable Logic Controller: industrial computer driving physical equipment (valves, motors, centrifuges). *[Landmark Incidents and Lessons]*

PLC (programmable logic controller) — Rugged computer that reads sensors and drives actuators in a scan loop, programmed in ladder logic or IEC 61131-3 languages. *[Industrial (OT/ICS) Architecture; NIST OT and IoT Security]*

PLC / RTU / DCS — Programmable Logic Controller (runs the control program) / Remote Terminal Unit (field controller on a remote site, telemetry) / Distributed Control System (plant-wide controllers from one vendor). *[ANSSI ICS/SCADA Security]*

Plugin — Extension the model calls automatically during a conversation (e.g. ChatGPT plugins, 2023) to reach an external API. *[OWASP LLM Top 10 v1.1 (2023) and the 2025 Shift]*

PME / ETI — Small and medium enterprises (under 250 staff) / intermediate-size enterprises (250 to 4 999 staff), the audience of the charter guide. *[IT Usage Charter and Outsourcing Security]*

PMF (802.11w) — Protected management frames: stops forged deauthentication frames used to kick clients onto a rogue AP. *[DNS, Wi-Fi & DDoS Architectures; Wi-Fi and 802.1X: Full Recommendation Sets]*

PMF (protected management frames, 802.11w) — Integrity protection of deauthentication and disassociation frames, which are otherwise forgeable. *[Wireless Security and IDS/IPS]*

PMK — Pairwise Master Key: 256-bit secret shared by client and AP after authentication (from the passphrase, SAE or EAP), input to the 4-way handshake. *[Wi-Fi Security Internals]*

PMTUD — Path MTU Discovery: finds the largest packet size (Maximum Transmission Unit) along a path using ICMP 3/4 replies. *[IP Addressing, ICMP, DHCP and Network Triage]*

PMTUD black hole — A path where a small-MTU link exists but the ICMP 'too big' messages are filtered: small packets pass, large ones vanish silently. *[ICMP, Path MTU, DHCP and DNS Operations]*

PMTUD (path MTU discovery) — Mechanism that finds the largest packet size a path accepts, using ICMP 'fragmentation needed' messages. *[Firewall Policy and IDPS Deployment]*

PNIO-DCP — PROFINET Discovery and Configuration Protocol: unauthenticated layer-2 protocol that can rename or re-address devices. *[OT Switch and Firewall Hardening: Hirschmann, SCALANCE]*

PNT — Positioning, navigation and timing: GNSS time synchronises telecom networks, power grids, finance and data centres, far beyond maps. *[Space and Satellite Security]*

POA&M — Plan of action and milestones: list of weaknesses with tasks, resources, milestones and due dates (defined in SP 800-37). *[Security Testing and Assessment in Depth]*

POA&M (Plan of Action and Milestones) — Tracking document listing each deficiency, tasks, resources, milestones and completion dates. *[PTES Phase Tasks, SP 800-115, Kill Chain Analysis; NIST SP 800-53r5 Controls in Practice +1]*

POC — Point of contact: the person or desk that receives incident reports first (often the IT help desk). *[IR Teams, Playbooks and Lessons Learned]*

Pod — Smallest deployable unit: one or more containers sharing a network namespace and volumes, scheduled on one node. *[Kubernetes Security; Kubernetes hands-on: learn it in your own lab]*

Pod CIDR — Address range for pods, split into one block per node (e.g. 10.244.1.0/24 for node 1); distinct from the Service CIDR (kubeadm default 10.96.0.0/12). *[Kubernetes and Container Networking Explained]*

Point d'insertion de données (PID) — Workstation or server whose removable-media ports are at least partly open to import

data to the operational network. *[Removable Media Airlock and White Station]*

Point-to-point on Ethernet — `ip ospf network point-to-point` on a two-router link: no DR election, no type-2 LSA, faster adjacency. *[Routing I: Routing Table, Static Routes, OSPF]*

Pointer — *T holds the address of a T; &x takes an address, *p dereferences it. Go has no pointer arithmetic, so no buffer overruns from it. *[Go Programming from Zero (Part 1: language basics)]*

Points of focus — Characteristics listed under each criterion (the COSO concept). They help design and evaluate controls, but an auditor does **not** require every point of focus to be addressed; management may tailor them. The criterion is the requirement, the point of focus is guidance. *[SOC 2 Trust Services Criteria, COBIT 2019, CSIRT Services]*

Poisoned pipeline execution (PPE) — Attack class (OWASP CIDC-SEC-4) where an attacker who controls code or configuration read by a pipeline makes a privileged job execute it. *[CI/CD Pipeline Security]*

Poisoning — **availability** (degrade overall), **targeted** (specific samples), **backdoor** (trigger pattern), **model poisoning** (federated learning, tampered checkpoints); defences: data sanitisation, provenance, robust aggregation, trigger reconstruction. *[AI Security Engineering]*

Policing vs shaping — A policer drops (or re-marks) traffic above a rate immediately; a shaper buffers the excess and sends it later, adding delay but avoiding drops. *[QoS, Multicast and WAN Services]*

Policy Administrator (PA) — Executes PE decisions: creates or tears down the session path, issues session-specific tokens or credentials, commands the PEP. *[Zero-Trust Architecture; Zero Trust Architecture SP 800-207]*

Policy as code — Security and compliance rules written as machine-checkable code (Rego, Sentinel, CEL) and run automatically in CI or at admission. *[Infrastructure as Code and Secrets; Kubernetes Admission Control and Policy as Code]*

Policy-based vs route-based VPN — Policy-based: an ACL (crypto map) selects what is encrypted. Route-based: a VTI (virtual tunnel interface) is a normal interface, routing (static or BGP/OSPF over it) decides what enters: easier failover and dynamic routing. *[VPNs in Depth: IPsec/IKEv2, TLS VPN, WireGuard]*

Policy Decision Point (PDP) — PE + PA together (the control plane). The PEP sits on the data plane that carries application traffic. *[Zero Trust Architecture SP 800-207]*

Policy Enforcement Point (PEP) — Enables, monitors and terminates connections between subject and resource; may be split into an agent (client side) and a gateway (resource side). *[Zero-Trust Architecture; Zero Trust Architecture SP 800-207]*

Policy engine — SP 800-207 component that decides to grant or deny access to a resource; with the policy administrator it forms the PDP. *[Secure Architecture Patterns]*

Policy Engine (PE) — The brain: runs the trust algorithm and grants, denies or revokes access to a resource for a subject. It consumes policy plus live inputs; it never touches the traffic. *[Zero-Trust Architecture; Zero Trust Architecture SP 800-207]*

Polyinstantiation — Multiple records with the same key at different classification levels, preventing inference by lower-cleared users. *[CISSP Domain 8: Software Development Security]*

POPC — Poste opérateur sur PC: PC-based switchboard operator console with privileges on the telephony applications. *[ToIP and Virtualization Security]*

Port forwarding / port triggering — Forwarding: static rule sending an external port to one internal IP (e.g. TCP 443 to 192.168.1.10). Triggering: an outbound connection on port X temporarily opens inbound port Y (Sybex ch. 8). *[CompTIA A+ Core 1 - Networking, SOHO, Network Troubleshooting]*

Port priority — of the sender, default 128, steps of 16 *[Switching: VLANs, Trunks, Spanning Tree, EtherChannel]*

Port ranges — 0-1023 well-known (system services, need root to bind on Unix), 1024-49151 registered (IANA-listed applications), 49152-65535 dynamic/ephemeral client ports (IANA; Linux default 32768-60999). *[TCP and UDP Deep Dive]*

Portfolio — public, verifiable evidence of your skills: repositories, write-ups, blog posts, talks, documented home lab *[CV, Portfolio and Job Interviews in Security]*

Positive security model — Everything not explicitly allowed is denied (default deny), the opposite of a blocklist. *[Firewall Policy: Design, Cleanup, Exposed Zone; Firewall Policy Management and IDS/IPS]*

Post-authentication actions — Windows LAPS setting that resets the password and optionally logs off or reboots after the password has been read and used, so a revealed password has a short life. *[Windows Hardening Baseline]*

Post-incident review — Structured, blameless meeting held soon after an incident closes to record the timeline, root cause and improvements, and to assign owners for each action. *[CISM Domain 4: Incident Management]*

Post-incident review (PIR) — Structured, blameless write-up after an incident: timeline, causes, what worked, actions with owners and dates; also called postmortem or lessons learned. *[Writing for Security Work]*

Post-quantum mechanism — Any asymmetric mechanism meeting RèglePQSécuAsym (security rests on a problem presumed quantum-hard, or on a conformant symmetric mechanism). *[ANSSI Crypto Rules Catalogue (PG-083 v3.00)]*

postMessage (R53-R56) — always set the target origin when sending (R54), check event.origin when receiving (R55), complete with CSP (R56). *[Browser-Side Web Security Standards]*

Power factor — Ratio of real power (W) to apparent power (VA); active PFC keeps it near 1. *[Power, Displays, Peripherals and Printers]*

Power problems — **Surge / spike**: brief overvoltage. **Sag**: brief undervoltage. **Brownout**: prolonged undervoltage. **Blackout**: total loss. **Line noise**: EMI/RFI on the circuit. *[CompTIA A+ Core 2 - Threats, Security Symptoms, Safety]*

PPK — Post-quantum preshared key (RFC 8784) mixed into IKEv2 key derivation as an interim quantum-safe measure. *[Emerging Topics: Self-Assessment]*

PPK (post-quantum preshared key) — Secret configured on both IPsec peers and mixed into derived keys (RFC 8784), so a quantum break of DH alone is not enough. *[ANSSI PQC Transition: Positions and Protocols]*

PPK (RFC 8784) — post-quantum preshared key mixed into IKEv2 key derivation; protects confidentiality without new algorithms but needs key distribution *[Quantum-Safe Network Protocols: Status]*

PPL — Protected Process Light: Windows protection level that stops even administrators from opening or injecting into a process (used for lsass with RunAsPPL and for EDR agents). *[Windows Endpoint Telemetry and Sysmon]*

PPL (Protected Process Light) — Process protection level that stops even administrators from opening, injecting into or killing the process unless they run at an equal or higher level; EDR services run as PPL anti-malware. *[EDR Telemetry, Tamper and Evasion Detection; Windows Internals for Defenders]*

PPST — Protection du potentiel scientifique et technique de la nation: French scheme protecting sensitive research and know-how from foreign capture. *[PPST Research Protection and Buying Qualified Security]*

PQ/T hybrid — a scheme combining a post-quantum and a traditional algorithm so that security holds if either one does (IETF terminology) *[Quantum-Safe Network Protocols: Status]*

Practical exercise — hands-on test: analyse logs or a packet capture, triage alerts, exploit a lab machine, review code, or write a short report, live or as a take-home *[CV, Portfolio and Job Interviews in Security]*

Pre-authentication — Proof, in the AS-REQ, that the client knows the user key (encrypted timestamp); disabling it (DONT_REQ_PREAUTH) lets anyone request crackable material. *[Active Directory Tiering and Kerberos in Depth]*

Pre-boot authentication — User authentication performed by a small Cryhod kernel before the operating system loads. *[ANSSI Encryption Tools: Zed! and Cryhod (2/2, Cryhod)]*

Precursor / indicator — Precursor: sign that an incident may happen in the future; indicator: sign that it has happened or is happening now. *[Incident Handling and Response]*

PredAI / GenAI — AI 100-2 splits the taxonomy into predictive AI (classifiers, regressors) and generative AI (LLMs, image generators). *[AI Security Engineering]*

Predisposing condition — Property of the organisation or environment (e.g. single data centre) that raises likelihood or impact (SP 800-30r1 term). *[CRISC Domain 2: IT Risk Assessment]*

Prefix hijack — An AS announces address space it does not own, attracting the victim's traffic. *[BGP, 802.1X & VPN; Routing II: EIGRP, BGP at the Enterprise Edge, Redistribution]*

Prefix / subnet mask — The leading bits that identify the network. Written as a length (/24) or as a dotted mask (255.255.255.0): both say that the first 24 of the 32 bits are the network part, the rest identify the host. *[IPv4 Addressing, Subnetting, VLSM and NAT]*

Preflight — Automatic OPTIONS request a browser sends before a non-simple cross-origin request to ask the target server whether the real request is allowed. *[HTTP Security Headers and Browser Policies]*

Prepare the Organization — requirements, roles, toolchains, criteria, environments *[GenAI Secure Development (SSDF

Profile); Secure Software Development: SSDF and SP 800-160]*

Presentation attack detection — Biometric liveness checks (ISO/IEC 30107) that reject photos, masks or replayed recordings. *[SecurityX Discriminator Pairs and Gap Closers]*

Preservation — Keep originals unaltered: write-once media, evidence locker, tamper-evident bags, hashes recorded, access logged; Faraday bag for phones. *[Incident Response, Forensics, Automation]*

Preservation and legal hold — Suspend retention and deletion for potentially relevant data when litigation or regulatory action is anticipated; notify custodians in writing. *[Incident Response and Management]*

Prestataire — provider; its admins use the **admin APIs** for physical resources, operational and security maintenance (MCO/MCS), creation of domains and projects. Admin APIs must never be exposed on a public network. *[OpenStack and Virtualisation Security]*

Presume breach — operate as if the adversary is already present *[DoD Zero Trust Reference Architecture v1.0]*

Pretest item — Unsourced question under evaluation for future exams, mixed in with scored items. *[CISSP Exam Strategy]*

Pretexting — A fabricated scenario that justifies the request (IT audit, courier, new supplier). *[Breach and Threat Landscape 2024; Social Engineering and Phishing Simulation]*

Primary handler — The single incident lead who coordinates, decides and keeps the journal. *[SANS Incident Handler Checklists and Enterprise IR]*

Primary key (PK) — Column whose value identifies exactly one row of a table (for example id); unique and never NULL. *[SQL Basics for Security]*

Prioritization factors (4.1) — Criticality, impact, asset type, residual risk, data classification, malware presence, known vulnerabilities - a medium alert on a Tier 0 domain controller (identity system that controls everything) outranks a high on a lab VM. *[Security Operations]*

Prioritizing and scheduling (6.2) — By FIPS 199 impact level (Low, Moderate, High) and assessment status: a high-impact system goes before a moderate one, but an overdue moderate system can go first. *[Security Testing and Assessment in Depth]*

Priority (sec. 3) — **High** = core IR activity; **Medium** = directly supports IR; **Low** = indirectly supports IR. A starting

point that each organization customizes. *[SP 800-61r3 Community Profile in Detail]*

PRIS — Prestataire de reponse aux incidents de securite: incident response provider qualified (audited and certified) by ANSSI; the guide encourages contracting one in advance. *[Cyber Crisis Management & Communication]*

Privacy attacks — **membership inference** (was this record in the training set?), **data reconstruction/extraction** (training-data regurgitation from LLMs), **property inference** (global facts about the training data), **model extraction** (functionally equivalent copy via queries); defences: differential privacy, output limiting, ... *[AI Security Engineering]*

Privacy by design — Privacy requirements built into systems from inception rather than added later (GDPR Art. 25). *[CISA Domain 2: Governance and Management of IT; CRISC Domain 4: Information Technology and Security]*

Privacy (confidentiality) — ESP encryption *[Cryptography; NIST Network Security Guides]*

Privacy engineering objectives — **Predictability** (reliable assumptions about data processing), **Manageability** (granular administration: alter, delete, correct), **Disassociability** (process without unnecessary linkage to individuals). Counterpart of C-I-A. *[NIST Privacy Framework 1.0]*

Privacy filter — Screen film that narrows the viewing angle so neighbours cannot read the display (shoulder surfing). *[Business Travel and SME Cybersecurity]*

Privacy risk — Likelihood that a problematic data action occurs x impact on individuals; organizational impact follows (legal, reputational, financial). *[NIST Privacy Framework 1.0]*

Private Link — private endpoint = NIC with a private IP for a PaaS resource; combine with `publicNetworkAccess: Disabled` and a private DNS zone. Service endpoints only extend the VNet identity to the service and still use the public IP. *[Azure and Entra ID Security Essentials]*

Private Sector Offensive Actors (PSOA) — Commercial spyware and hack-for-hire firms, treated by ENISA as a distinct actor category next to state-nexus, cybercrime and hacktivists. *[Breach and Threat Landscape 2024]*

Private VLAN — VLAN whose isolated ports can talk only to the uplink (gateway), not to each other. *[Segmentation and IS Mapping]*

Private VLAN isolated — Hosts in the VLAN talk only to the promiscuous uplink, never to each other (R30). Fallback:

`switchport protected / port isolation (R30-)`. *[Network Equipment Hardening]*

Privilege creep — Gradual accumulation of rights as a user changes jobs without old rights being removed. *[CISSP Domain 5: Identity and Access Management]*

Privilege escalation — Moving from a low-privilege account to administrator or root by abusing a misconfiguration or flaw. *[OSCP / OSCP+: Readiness and Self-Assessment]*

Privilege escalation path — A benign-looking permission (`iam:PassRole`, `lambda:CreateFunction`, `iam:CreatePolicyVersion`) that chains to `admin`. *[Cloud Configuration Review]*

Privilege management infrastructure (PMI) — dynamic assignment and revocation of privileges through attribute or role specification certificates. *[Cloud Reference Architecture and Access Control]*

Proactive posture — The organisation speaks first, fast, with verified facts, to occupy the ground before rumours. *[Cyber Crisis Communication]*

Probe (sonde) — passive network sensor that decodes traffic copied to it and raises alerts; it never sends on the watched network. *[IoT/IloT Security and OT Detection]*

Problem — Cause of one or more incidents; problem management finds the root cause and removes it (known error, workaround). *[CRISC Domain 4: Information Technology and Security]*

Problematic data action — A data action that could cause a problem for individuals (embarrassment, discrimination, economic loss, loss of trust or autonomy). *[NIST Privacy Framework 1.0]*

Procedure — One concrete way of performing a technique; a technique often has dozens, and a rule can catch one procedure and miss the rest. *[Detection Validation and Purple Teaming]*

Process — container for a program: private virtual address space, a handle table, a primary access token and at least one thread; kernel structure `EPROCESS`, user-mode `PEB` (Process Environment Block) holding the command line and loaded modules. *[Windows Internals for Defenders]*

Process assistant — Provides translation or accessibility support, takes no decision. *[Digital Identity Guidelines SP 800-63-4]*

ProcessGuid — Sysmon unique id per process instance; unlike a PID it is never reused, so it links events of one process reliably. *[Windows Endpoint Telemetry and Sysmon]*

Proctor — Remote examiner who watches webcam and screens throughout the exam session. *[OSCP / OSCP+: Exam Format and Rules]*

Produce Well-Secured Software — design, reuse, code, build, review, test, defaults *[GenAI Secure Development (SSDF Profile); Secure Software Development: SSDF and SP 800-160]*

Product with digital elements (PDE) — CRA Art. 3(1): software or hardware product and its remote data processing solutions, placed on the market with a data connection. *[Cyber Resilience Act and AI Act]*

Production vs backup vs baseline config — Production = running now; backup = last saved copy (restore point); baseline (golden) = the approved reference that audits compare against. *[Network Operations: Documentation, Monitoring, Resilience]*

Produit de sécurité / Security product — Hardware or software device designed to protect availability, integrity or confidentiality of stored, processed or transmitted data. *[ANSSI CyberDico FR/EN Glossary]*

Profile — named set of preferences, columns, colouring rules and filter buttons; switch per task (Edit > Configuration Profiles or -C name in tshark). *[AI Compliance Frameworks; Wireshark and tshark for Troubleshooting and Analysis]*

Profile ids — The profile numbers threats M1-M7 (menaces), hypotheses H1-H8, sensitive assets B1-B13 (biens) and security functions FS1-FS15 (fonctions de securite). *[Removable Media Airlock and White Station]*

Program management — 5.0, 20 %: governance, risk, third parties, compliance, audits, awareness *[CompTIA Security+ SY0-701]*

Promiscuous mode — NIC setting that passes every frame on the wire to the capture tool, not only frames addressed to the host. *[Packet Analysis in Practice and the N10-009 Exam Map]*

Prompt firewall — Gateway component that inspects prompts and responses for injection, jailbreak and data-leak patterns before they reach the model or the user. *[CompTIA SecAI+ CY0-001]*

Prompt injection — Attack that places instructions in model input so the application follows the attacker instead of its designer. *[ANSSI Generative AI Security; LLM Application Security Testing +2]*

Proof of deletion — Claim or video from the attacker that stolen data was destroyed after payment; unverifiable, data is often resold or leaked later. *[Ransomware: Respond and Recover]*

Proof of vote (R58-R59) — The voting client generates a proof the voter can keep; the server publishes the list of proof references on a page reachable without authentication, so voters verify presence in the ballot box (2-07). *[Internet Voting for Non-Political Elections]*

proof.txt — Flag file proving administrative or root access on an exam machine. *[OSCP / OSCP+: Exam Format and Rules]*

Protect the Software — code access, release integrity, archives *[GenAI Secure Development (SSDF Profile); Secure Software Development: SSDF and SP 800-160]*

Protected Users — AD security group whose members cannot use NTLM, RC4 or credential caching, limiting credential theft. *[Ransomware: Anatomy, Detection, Prevention]*

Protecting against cyber attack — policies, identity and access, data, systems, resilience, people *[NCSC, BSI and Allied Cyber Authorities]*

Protection devices — Surge suppressor (rated in joules; most power strips do not protect), line conditioner, UPS (standby switches on outage, online double-conversion always on battery path), generator for long outages. *[CompTIA A+ Core 2 - Threats, Security Symptoms, Safety]*

Protection needs (Schutzbedarf) — normal, high or very high, assessed for confidentiality, integrity and availability; high or very high triggers a BSI 200-3 risk analysis. *[NCSC, BSI and Allied Cyber Authorities]*

Protection Profile (PP) — Implementation-independent security requirements for a class of products, written by the customer side. *[CISSP Domain 3: Security Architecture and Engineering]*

Protocol break (rupture de flux) — terminate and re-initiate the session at the boundary (proxy, gateway) so that only application data crosses (PG-075 R14 flow breaker in the class 1 gateway; Rup function of PA-108 inter-class gateways). *[Segmentation and IS Mapping]*

Protocol break (rupture protocolaire) — The jump host terminates the admin session and opens a new one to the target, instead of relaying it end to end. *[ANSSI Secure Administration of IS (PA-022)]*

Protocol vs service — A service is what a layer offers to the layer above; a protocol is the set of rules peers on the same

layer use to implement it (Tanenbaum 1.3). *[Network Models, Performance and the Physical Layer]*

Prototype pollution — JavaScript flaw where writing a key such as `__proto__` through a recursive merge or path setter adds properties to `Object.prototype`, so every object in the process inherits them: authorization flags flip, or a later gadget reaches `child_process`. Node's `--disable-proto=delete` flag removes the `__proto__`. *[Secure Code Review by Language]*

Provenance — Signed statement of who built what, from which source, with which builder (in-toto attestation). *[DevSecOps and Supply-Chain Security; Software Supply Chain Security]*

Provenance data (PS.3.2) — Record of the origin and history of each component of a release, e.g. an SBOM; updated whenever a component changes. *[SSDF v1.1: the 42 Tasks]*

Provenance file (.prov) — A file accompanying a Helm chart that carries its SHA-256 digest and a cryptographic signature for verification. *[Helm, operators and the CRD ecosystem (with security)]*

Provider — Filesystem-like access to other stores: `HKLM:`, `Cert:`, `Env:`, `Variable:`. *[AI Governance Programme; PowerShell for Defenders]*

Provider vs deployer — provider develops or places the system on the market under its name (Art. 16 obligations); deployer uses it under its authority (Art. 26: follow instructions, human oversight, log retention ≥ 6 months, inform workers, fundamental rights impact assessment Art. 27 for public bodies and some private deployers) *[Cyber Resilience Act and AI Act]*

Provisioning profile — Apple-signed file binding a Team ID, an App ID, allowed entitlements, a signing certificate and, for development builds, the device list. *[iOS Application Internals and Security]*

PRT (Primary Refresh Token) — Device-bound Entra ID token on Windows, iOS, macOS and Android that gives single sign-on to all apps; protected by the TPM (Trusted Platform Module) when present. *[Identity Attacks and ITDR: Entra ID and Okta]*

Prudent person rule — Senior management must act as a reasonable person would in similar circumstances; basis of personal liability. *[CISSP Domain 1: Security and Risk Management]*

PSA — Pod Security Admission: built-in Kubernetes controller enforcing the privileged / baseline / restricted Pod Security Standards per namespace. *[Cloud and DevSecOps: Self-Assessment]*

PSCE / PSHE — Prestataire de services de certification électronique (certificate authority) / d'horodatage électronique (time-stamping authority). *[Local Authorities: the Regulatory Security Framework]*

Pseudonymisation (Art. 4(5)) — data can no longer be attributed to a person without additional information kept separately; still personal data. Anonymised data is out of scope (Recital 26) *[GDPR for Security Teams]*

Pseudonymization — Replacing identifiers with tokens that can be re-linked with a separate key; still personal data under GDPR. *[CISSP Domain 1: Security and Risk Management]*

Pseudonyms — users can authenticate with relying-party-specific pseudonyms where identification is not legally required *[eIDAS 2 and the EU Digital Identity Wallet]*

PSH — Push: deliver buffered data to the application now *[TCP and UDP Deep Dive]*

PSI (Pressure Stall Information) — Kernel metric (since 4.20) in `cpu.pressure`, `memory.pressure`, `io.pressure` per cgroup and in `/proc/pressure/`: share of wall time tasks were **stalled** on the resource. `some` = at least one task stalled; `full` = all non-idle tasks stalled at once (lost throughput). `avg10/60/300` in %, `total` in μ s. Better... *[Linux Isolation Primitives and Sandboxes]*

PSID revert — Factory reset of a TCG Opal self-encrypting drive using the Physical Secure ID printed on its label. *[Storage: Interfaces, SSD Internals, RAID, SMART]*

PSK and SSID (annex C.4) — The 256-bit master key is PBKDF2-HMAC-SHA1(passphrase, SSID, 4096 iterations): a default SSID lets attackers reuse precomputed tables, hence R14. *[Wi-Fi and 802.1X: Full Recommendation Sets]*

PSK confidentiality (note to R12) — Any holder of a WPA2-PSK can decrypt other clients' traffic on the same network: no client-to-client confidentiality, use EAP in business. *[Wi-Fi and 802.1X: Full Recommendation Sets]*

PSK (pre-shared key) — Shared secret typed on both peers; only as strong as its entropy. *[VPN and Firewall Security; Wireless Security and IDS/IPS]*

PSK / SAE — Pre-shared key (one passphrase for all, WPA2-Personal) versus Simultaneous Authentication of Equals (WPA3-Personal Dragonfly handshake, resistant to offline guessing). *[DNS, Wi-Fi & DDoS Architectures]*

PSO / PPP — plan de securite d'operateur and plan particulier de protection: the LPM physical-security documents an

OIV maintains besides the SIIV rules *[Priority Measures and Essential Systems]*

PSReadLine — PowerShell module providing line editing, history, prediction and key handlers; Windows edit mode on Windows, Emacs mode on macOS and Linux by default. *[Shell and Terminal Productivity on Every OS]*

PSS (Pod Security Standards) — Kubernetes built-in profiles privileged, baseline and restricted, enforced per namespace by Pod Security Admission. *[Container and Virtualization Security]*

PSSI — politique de securite des systemes d'information: the organisation's IS security policy. *[Remote Work (Digital Nomadism); Multi-Environment Workstation and Refurbishing +3]*

PSSIE — Politique de securite des SI de l'Etat: the State IS security policy (circular of 17 July 2014), binding on ministries. *[PPST Research Protection and Buying Qualified Security; Security Accreditation (Homologation)]*

Psychological safety — Shared belief that the team is safe for interpersonal risk-taking: asking, admitting mistakes, disagreeing without punishment. *[Working Life in Security]*

PTE inversion — L1TF fix in the kernel: a non-present entry keeps its frame bits inverted so they point above installed RAM, and a speculative load finds nothing cached to leak. *[CPU Side Channels and Memory Attacks]*

PTES — Penetration Testing Execution Standard. Seven phases, engagement lifecycle. *[CompTIA PenTest+ PT0-003]*

PTES / OSSTMM — Penetration Testing Execution Standard and Open Source Security Testing Methodology Manual: community methodologies that complement SP 800-115. *[Security Testing and Assessment in Depth]*

PTK — Pairwise Transient Key: per-session key derived from the PMK, both nonces and both MAC addresses; split into KCK, KEK and TK. *[Wi-Fi Security Internals]*

Public information (Art. 23(7)) — the authority may inform the public or require the entity to do so when public awareness is necessary *[NIS2 Directive: EU-wide Obligations]*

Public PPE (3PE) — PPE triggered by anyone on the Internet through a public repository, typically a fork pull request or an issue comment. *[CI/CD Pipeline Security]*

Public vs private — Anyone can detect vs only privileged actors hold the algorithm or key. *[GenAI Secure Development and Content Transparency]*

Publisher condition — Preferred (R3): signer, optionally product, file name, version; updates stay transparent. Breaks when vendors put the version in the product name. *[Windows Application Control and Endpoint Monitoring]*

PUE (Power Usage Effectiveness) — Total facility power divided by IT power; 1.0 is ideal, good modern DCs approach ~1.1-1.2 (illustrative). *[Data-Centre Architecture]*

Pull-through cache — Internal registry that fetches and stores upstream public images on first pull, adding scanning and availability control. *[Container Image and Registry Security]*

Pulled automatically — software agents fetch the desired state; nobody pushes into the cluster *[GitOps and Continuous Delivery Security]*

Purdue model — ICS/OT reference architecture, levels 0-5 (field devices to enterprise). *[CompTIA PenTest+ PT0-003; OT Architecture and the SP 800-82r3 OT Overlay]*

Purge — Physical or logical techniques that defeat laboratory recovery: degaussing (magnetic only), block erase, cryptographic erase (CE). *[NIST Security Operations Guides; Security Operations: Logs, Malware, Servers, Media]*

PURL — Package URL: ecosystem-neutral identifier `pkg:type/namespace/name@version` used by SBOMs, OSV and scanners to match components. *[Software Supply Chain Security]*

Purple team exercise — Collaborative session where attackers run techniques in the open while defenders watch telemetry, tune detections and retest on the spot. *[Red Team Programme and Rules of Engagement]*

Purple teaming — Red (attack simulation) and blue (detection and response) work in the same room, test by test, fixing gaps immediately instead of reporting them weeks later. *[Detection Validation and Purple Teaming]*

Purpose limitation — Art. 5(1)(b): specified, explicit, legitimate purposes; no incompatible reuse *[GDPR for Security Teams]*

Pwn request — A `pull_request_target` or `workflow_run` workflow that checks out and runs fork code while holding secrets and a write token. *[CI/CD Pipeline Security]*

PWS — Performance work statement: like a SoW but states the outcome and quality standard expected rather than the method (common in US government contracts). *[Engagement Management]*

Pxxx policy — Numbered Zed!/Cryhod configuration setting (e.g. P383), pushed by Windows GPO or a local policy file. *[ANSSI Encryption Tools: Zed! and Cryhod (1/2, Zed!)]*

Q

QoD — Quality of Detection: Greenbone's 0-100 % confidence that a finding is real, based on how it was detected (package check 97 %, banner 80 %, unreliable banner 30 %). *[Vulnerability and Configuration Scanners for Your Own Estate]*

QoS (Quality of Service) — Tools that give some traffic better treatment (less delay, jitter, loss) when a link is congested; they reorder and drop, they never create bandwidth. *[QoS, Multicast and WAN Services]*

QSA (Qualified Security Assessor) — PCI SSC-certified external auditor who writes the ROC; an ISA (Internal Security Assessor) is a certified employee. *[PCI DSS v4.0.1, CVSS and FIRST]*

QSCD — Qualified signature creation device: certified smart card, token or remote HSM holding the signer's key. *[Local Authorities: the Regulatory Security Framework; eIDAS 2 and the EU Digital Identity Wallet]*

QTSP — Qualified trust service provider, audited and listed in the national trusted list under eIDAS. *[eIDAS 2 and the EU Digital Identity Wallet; EU Governance and Regulation: Self-Assessment]*

Qualification — ANSSI's strongest product visa (certification plus conformity to French requirements and ANSSI follow-up); asked for C4 products. *[Local Authorities: the Regulatory Security Framework; Incident Qualification & Remediation Decision Keys +3]*

Qualification (ANSSI) — ANSSI label certifying a product after evaluation and recommending it for administration use; levels elementary, standard, reinforced. *[ANSSI Encryption Tools: Zed! and Cryhod (1/2, Zed!)]*

Qualifier — Word in the question stem (BEST, FIRST, MOST cost-effective, LEAST disruptive) that decides between several technically valid options. *[SecurityX Discriminator Pairs and Gap Closers]*

Quantum threat model — **Shor's algorithm** on a large fault-tolerant quantum computer solves factoring and discrete logarithms, breaking RSA, DH and ECC outright. **Grover's algorithm** only speeds up brute force quadratically, so symmetric ciphers and hashes survive with doubled key or output sizes (AES-256, SHA-384). *[NIST Cryptographic Standards]*

Quarantine VLAN — Dead-end VLAN (e.g. 666) for every unused port (R27): no route, no service, no inter-port traffic. Ports also shut down (R34). *[Network Equipment Hardening]*

Quasi-identifier — attribute that is not identifying alone but singles people out in combination (ZIP code, birth date, sex, employer, rare diagnosis) *[Privacy Engineering and PETs]*

Query — One SQL statement; SELECT reads data, INSERT, UPDATE and DELETE change it. *[SQL Basics for Security]*

Query (prompt) — Text instruction sent by the user. May be pre-processed before reaching the model: log **both** the raw query and what was sent (R29). *[ANSSI Generative AI Security]*

Question word — BEST, FIRST, MOST cost-effective, LEAST disruptive, NEXT *[SecurityX Practice Scenarios]*

Queue ID — Identifier a mail server gives each message on acceptance (Postfix: hex string such as 4Q2x1K0ZfBz9sQ); the key for following it through the logs. *[Email Infrastructure Operations]*

R

R / C / N items — **R** recommendation (should do), **C** consideration (consider doing), **N** note (supporting information). Cited as RS.MA-03.R2 or RS.MA-03 R2. *[SP 800-61r3 Community Profile in Detail]*

R+ variant — stronger version to prefer when feasible (R83+ every user named, R116+ two firewalls in series). *[ANSSI ICS Detailed Measures v2 (1/2): organisation and accounts]*

RA Guard — Switch feature that drops Router Advertisements arriving on host-facing ports (RFC 6105). *[IPv6 in Depth: Addressing, NDP, SLAAC, Security]*

RA (Router Advertisement) — ICMPv6 134 sent by routers: prefixes, the M/O/A flags, MTU, router lifetime and DNS servers; its source becomes the default gateway. *[IPv6 in Depth: Addressing, NDP, SLAAC, Security]*

RA-TLS — remote-attestation TLS: the TLS key is embedded in the attestation report, so the client knows it talks to the attested workload. *[Confidential Computing]*

RaaS — Ransomware-as-a-Service: developers rent the encryptor, leak site and negotiation portal to affiliates for a share (often 20-30 %, estimate) of each ransom. *[Threat Actor Profiles]*

RaaS and initial access brokers — Operators rent the encryptor and leak site to affiliates who run the intrusion; access is bought from brokers selling VPN or RDP credentials. *[Ransomware: Anatomy, Detection, Prevention]*

RaaS and the criminal supply chain — **Ransomware-as-a-Service**: developers rent the payload and leak site; **affiliates** run intrusions and take 70-80 % of payments; **initial access brokers (IAB)** sell VPN/RDP credentials and web shells; negotiators, launderers and DDoS services complete the chain. Consequence: the intrusion tradecraft is shared... *[Ransomware Defense End to End]*

Rabbit hole — Promising-looking path that consumes time without leading to access. *[OSCP / OSCP+: Readiness and Self-Assessment]*

Race condition — Two parallel requests pass a check before either updates state (coupon used twice, balance overdrawn). *[Famous Vulnerabilities Explained; WSTG v4.2 - Complete Test Catalogue]*

RACI — Responsible, Accountable (exactly one), Consulted, Informed - responsibility matrix. *[CISM Domain 1: Information Security Governance; SecurityX Practice Scenarios]*

RAG — Retrieval-augmented generation: documents found by similarity search in a vector store are pasted into the prompt. *[OWASP Top 10 for LLM Applications 2025]*

RAG (retrieval-augmented generation) — The application retrieves documents and pastes them into the model's context before it answers. *[AI Security Engineering]*

Rainbow table — A precomputed lookup from hash back to password; salting makes them useless because every hash uses a different salt. *[Password and Hash Auditing for Defenders]*

Range (annex B.2) — Designed for about 100 m line of sight; French limit 100 mW EIRP (equivalent isotropically radiated power) at 2.4 GHz, but a high-gain antenna reads far beyond, hence R19. *[Wi-Fi and 802.1X: Full Recommendation Sets]*

Ransomware — Malware built to obtain a ransom: it makes the victim's computer or IS **reversibly** unusable, in practice by encrypting data, then displays an unencrypted note offering the decryption means against payment. It is a tool of financially motivated cybercriminals. *[Ransomware: Anatomy, Detection, Prevention; Malware, Attacks and Indicators +1]*

Ransomware-as-a-service (RaaS) — developers rent their ransomware to affiliates who break in and share the ransom. *[CISA #StopRansomware Guide]*

Rapid elasticity — provisioned and released elastically, appears unlimited to the consumer *[Cloud Computing Security]*

RASP — Runtime application self-protection: agent in the application that detects and blocks attacks as they execute. *[CISSP Domain 8: Software Development Security]*

RAT / C2 — Remote access trojan and command-and-control - hunted with beacon analysis (RITA), JA3/JA4 TLS fingerprints, DNS anomaly detection. *[CompTIA SecurityX CAS-005 - Exam Overview]*

RBAC — Rights assigned to roles, users assigned to roles; simplifies reviews and SoD. *[CISA Domain 5: Protection of Information Assets]*

RBAC least privilege — no wildcards, no cluster-admin, review escalate/bind/impersonate *[Kubernetes Security]*

RBAC (role-based access control) — Permissions granted to roles, roles bound to users or service accounts. *[Container and Virtualization Security]*

RBI — remote browser isolation: pages execute in a remote container, the user receives only rendered output *[Browser and Extension Security]*

Reactive posture — No public statement unless asked; messages ready and stored off the IS; used when speaking would warn an attacker still inside. *[Cyber Crisis Communication]*

Readily available data — Data Act Art. 2(17): product data the holder can obtain lawfully without disproportionate effort; the scope of the user access right. *[Data Act, Data Governance Act and EHDS]*

Readiness tool (annex A.3) — Microsoft **Device Guard and Credential Guard hardware readiness tool** writes CG_Capable, DG_Capable, HVCI_Capable under HKLM\...\Control\DeviceGuard\Capabilities; use them for GPP item-level targeting (annex C). Version 3.2 needed Enterprise added to \$SKUarray on French systems. *[Windows Privacy GPOs and VBS Deployment]*

Reading an identifier — RS.MA-03.R2 = Function RS (Respond), Category MA (Incident Management), Subcategory 03 (incidents are categorized and prioritized), item R2. A Category row without a number (e.g. RS.MA) holds items that apply to the whole Category. *[SP 800-61r3 Community Profile in Detail]*

Reading rua — Group rows by source IP: legitimate senders failing = fix SPF include or DKIM; unknown IPs with your header_from = spoofing the policy already blocks. *[Email Security: SPF, DKIM, DMARC]*

Reading the ANSSI row — chapters of the 42-measure hygiene guide: I raise awareness and train, II know the information system, III authenticate and control access, IX supervise, audit, react; supply chain has no dedicated chapter. *[NCSC, BSI and Allied Cyber Authorities]*

Reading the CAF row — A1 governance, A2 risk management, A3 assets, A4 supply chain, B2 identity and access, B5 resilience, C1 monitoring, C2 threat hunting, D1 response planning, D2 lessons learned. *[NCSC, BSI and Allied Cyber Authorities]*

Reading the CSF 2.0 refs — function.category-number: GV.RR roles and responsibilities, GV.OV oversight, GV.SC supply chain risk; ID.AM asset management, ID.RA risk assessment, ID.IM improvement; PR.AA identity, authentication and access control, PR.AT awareness and training, PR.DS data security, PR.PS platform security, PR.IR infrastructure... *[CISA Cybersecurity Performance Goals 2.0]*

Reading the CSF row — NIST CSF 2.0 functions GV Govern, ID Identify (ID.AM asset management), PR Protect (PR.AA identity, authentication, access), DE Detect (DE.CM continuous monitoring, DE.AE adverse event analysis), RS Respond, RC Recover, GV.SC supply chain risk. *[NCSC, BSI and Allied Cyber Authorities]*

Reading the NIS2 row — Art. 21(2) letters: (a) risk policies, (b) incident handling, (c) continuity and backups, (d) supply chain, (e) secure development and vulnerability handling, (f) effectiveness assessment, (i) HR, access control, assets, (j) MFA. *[NCSC, BSI and Allied Cyber Authorities]*

Readline — GNU library that gives bash (and gdb, python REPL, sqlite3, psql) emacs- or vi-style line editing, history search and completion; configured in ~/.inputrc. *[Shell and Terminal Productivity on Every OS]*

Reasonable assurance — High but not absolute level of assurance; audits cannot detect every error or fraud. *[CISA Domain 1: Information System Auditing Process]*

Received header — Trace line added by each relay: who handed the message over (from, with the connecting IP seen by the relay), who received it (by), protocol, queue id and timestamp. *[Phishing Analysis and E-mail Header Forensics]*

Recipients of services (Art. 23(1)-(2)) — entities inform recipients of their services likely to be affected by a significant incident without undue delay, and of measures they can take in response to a significant cyber threat *[NIS2 Directive: EU-wide Obligations]*

Reco (recommendation) — State of the art with a substantial security margin; may be waived for major functional, performance or cost constraints. *[ANSSI Crypto Rules Catalogue (PG-083 v3.00)]*

Recommendation (RECO) — respected except in exceptional cases, with a clear and precise justification by the developer. *[C and Rust Secure Coding Rule Catalogue]*

Reconcile interval — How often the agent re-reads the source and compares it with the cluster: Argo CD polls repositories every 3 min by default (timeout.reconciliation), Flux per object (spec.interval, e.g. 1m to 10m); webhooks trigger an immediate refresh. *[GitOps and Continuous Delivery Security]*

Reconciliation loop — Controller routine that repeatedly compares desired and observed state and acts to converge them; idempotent by design. *[Kubernetes Architecture in Depth]*

Reconstruction — Support activity providing the IT means to restore the IS to working and secure condition; may also keep vital activities running; continues after the hot time. *[Managing Cyber Remediation]*

Recoverability — Design to the BIA (business impact analysis): RPO (recovery point objective = acceptable data loss in time) drives replication mode (sync vs async); RTO (recovery time objective = acceptable downtime) drives warm vs hot standby; immutable backups plus tested runbooks. Active-active multi-region = RPO near 0, highest... *[Security Architecture - Resilience, Controls, Zero Trust]*

Recovery — Manual: shutdown then no shutdown. Automatic: errdisable recovery cause psecure-violation. *[First-Hop Security and Gateway Redundancy]*

Recovery operator — Help-desk role that unlocks a user who lost a password or token, by escrow or by a remote challenge-response. *[ANSSI Encryption Tools: Zed! and Cryhod (2/2, Cryhod)]*

Recovery point — One restorable version of a system or dataset at a given time (a snapshot, a backup job result, a database log position). *[Backup and Recovery Engineering]*

Recursive / cache server — Walks the DNS hierarchy for clients and caches answers; the guide merges both roles as *serveur cache*. Poisoning a cache prolongs a compromise. *[DNS, Wi-Fi & DDoS Architectures]*

RED — named recipients only *[IR Exercises and Threat Information Sharing]*

Red / black addresses — IPsec vocabulary: red = clear-text private addresses inside the tunnel; black = public addresses carrying the encrypted packets. *[Stormshield SNS 3.7.17 Hardening by Chapter]*

Red key / black key — A key in clear (red) versus a key encrypted under another key (black), safe to store or transport. **[ANSSI Crypto Rules Catalogue (PG-083 v3.00)]**

Red lines (lignes rouges) — Business thresholds set in advance (e.g. access to the payment system, start of mass encryption) that force a switch to a more drastic strategy such as isolation. **[Incident Qualification & Remediation Decision Keys]**

Red team exercise — Objective-driven, covert, time-boxed simulation of a realistic adversary against people, process and technology, to test whether the organisation can detect and respond, not to list every vulnerability. **[Red Team Programme and Rules of Engagement]**

Redfish — DMTF REST/JSON management API over HTTPS, the modern replacement for IPMI. **[Platform Firmware, BMC, DMA and USB Attacks]**

ReDoS — Denial of service caused by a regex whose matching time grows exponentially with crafted input on backtracking engines. **[Defender Scripting Toolkit]**

Redundant PSU — Servers: two hot-swap PSUs on separate PDUs (power distribution units, rack power strips) and circuits (A+B feeds); one fails, the other carries the load. **[Power, Displays, Peripherals and Printers]**

Redundant rule — Same effect as an upstream rule (identical objects, subset of a wider rule, or network-vs-host overlap): candidate for merge or refinement. **[Firewall Policy: Design, Cleanup, Exposed Zone]**

Ref — Small file (or packed-refs line) holding a commit hash under a human name: refs/heads/main (branch), refs/tags/v1.2 (tag), refs/remotes/origin/main. **[Git Internals and Repository Security]**

Reference cyber scenario — A risk scenario (e.g. ransomware on the whole IS, DDoS on the web shop) rated by severity and likelihood, used to set crisis activation criteria; EBIOS Risk Manager workshop 3 is recommended to build them. **[Cyber Crisis Management & Communication]**

Reference monitor — Abstract machine that mediates every subject-object access; must be tamper-proof, always invoked and verifiable. **[System Partitioning: ANSSI PG-040; CISSP Domain 3: Security Architecture and Engineering +1]**

Referrers (OCI 1.1) — OCI (Open Container Initiative, the image and registry standard) 1.1 lets artefacts (signatures, SBOMs = component lists, attestations, VEX = exploitability statements) attach to an image digest through the subject

field, listed by the referrers API; ORAS, cosign and Notation use it. **[Container Image and Registry Security]**

Reflection — Attacker spoofs the victim's IP as source of small UDP requests to many open servers; their replies all go to the victim. **[DDoS: Protection Options, Response, Non-Participation; DDoS and Edge Protection]**

Reflection attack — Trudy opens a second parallel session and makes the victim answer its own challenge (Fig. 8-34). Real-world echo: NTLM credential reflection over SMB, patched by MS08-068 (Nov 2008). **[Network Security II - Authentication, Email, Web]**

Refresh token — Long-lived secret an app redeems at the IdP for new access tokens without a new sign-in; the prize for token thieves. **[Identity Attacks and ITDR: Entra ID and Okta]**

Register of information — DORA Art. 28(3) inventory of every ICT contract, supplier chain and supported function, filed yearly in ITS 2024/2956 format. **[DORA: Digital Operational Resilience]**

Register of risks and exemptions — List of accepted risks and security exceptions granted during the crisis, with owner and end date; reviewed before the crisis exit. **[Cyber Crisis Management & Communication]**

Registered MFA — new authentication methods after the compromise **[Microsoft 365 Hardening]**

Registration authority — Verifies the requester's identity on behalf of the CA before issuance. **[CISA Domain 5: Protection of Information Assets; NIST Cryptography, TLS and PKI]**

Registration Authority (RA) — Vets the identity of a requester (domain control, org validation, employee identity) and tells the CA to issue; it never holds the CA signing key. **[PKI and Certificate Architecture]**

Registry — Server that stores and distributes images (Docker Hub, ECR, Harbor). **[Docker and Containers Hands-On; Container and Virtualization Security]**

Règle (rule) — Necessary condition for a mechanism to be recognised at the right security level; a mechanism meeting all rules is 'conforme au référentiel'. Not sufficient: only a specific analysis proves robustness. **[ANSSI Crypto Rules Catalogue (PG-083 v3.00)]**

RègPQ / RecoPQ — Extra conditions applying only when post-quantum security is targeted; a PQ rule is necessary to claim protection against a quantum adversary. **[ANSSI Crypto Rules Catalogue (PG-083 v3.00)]**

Regression test — Re-runs earlier tests to confirm a change did not break working functions. **[CISA Domain 3: IS Acquisition, Development and Implementation]**

Reinforcements — Business and cyber needs centralised by one unit or person, which also welcomes the experts; needs reviewed at regular intervals during investigation and reconstruction. **[Cyber Crisis Management & Communication]**

Relay (forwarder) — Forwards client queries to a cache without resolving itself; used for hosts that need both internal and Internet names. **[DNS, Wi-Fi & DDoS Architectures]**

Release — One installed instance of a chart in a namespace, with a numbered revision history kept as Secrets in the cluster. **[Helm, operators and the CRD ecosystem (with security)]**

Release (CPRT) — Since 2023 SP 800-53 evolves by numbered releases (5.1.1, 5.2.0) published in the Cybersecurity and Privacy Reference Tool, without a new revision number. **[NIST Cyber Publications 2024-2026 Roundup]**

Relocated Subcategory — Gap in numbering (ID.AM-06, DE.CM-04, RS.AN-01...): the CSF 1.1 outcome was moved elsewhere or merged; numbers are never reused. **[CSF 2.0 Core: the 106 Outcomes Explained]**

Relocation — Record telling the loader which address fields to patch when the image is not loaded at its preferred base (PE .reloc) or when symbols are resolved (ELF .rela.*). **[Executable Formats: ELF and PE]**

Relying party ID (rpId) — The domain a credential is bound to (e.g. example.com); the browser refuses to use it on any other origin, which is what defeats phishing. **[Authentication and Session Design]**

Relying party / key broker — the party that acts on the attestation result, typically a KMS (Key Management Service) that releases a decryption key only to a passing TEE **[Confidential Computing and Remote Attestation]**

Relying party (RP) — Organisation that requests and verifies wallet data or signatures to deliver a service; must register and state its purpose. **[eIDAS 2 and the EU Digital Identity Wallet]**

Remediation — Operations aiming at recovering control of a compromised IS and restoring it to a sufficient operational status. Begins once the intruder is contained; lasts weeks or months; touches many business units. **[Incident Qualification & Remediation Decision Keys]**

Remediation plan — List of actions bringing the IS in line with the operational objectives, split into sub-projects per operational objective. *[Managing Cyber Remediation]*

Remédiation / Reconstruction — Remediation: regaining control of a compromised IS and restoring sufficient service, alongside investigation and crisis management, starting at containment and lasting months. Rebuilding (reconstruction) supplies the IT means for it. *[ANSSI CyberDico FR/EN Glossary]*

Remote access (sec. 6.2.10) — Justified and limited to the business need, never bypassing safety or security controls, MFA considered. For temporary vendor access: unique accounts, no default credentials, current firmware, automatic removal timers, monitoring, operations informed, **connection initiated from the OT side**, remote devices labeled... *[OT Architecture and the SP 800-82r3 OT Overlay]*

Remote attestation — a hardware-signed report containing measurements of the workload, hardware model, firmware/microcode version and a unique identifier; the signing key is certified by the processor vendor. *[Confidential Computing]*

Remote IP — ping 8.8.8.8 / tracer: routing and ISP *[CompTIA A+ Core 1 - Networking, SOHO, Network Troubleshooting]*

Rendered manifests — Final Kubernetes YAML after Helm templating or Kustomize overlays; what the agent really applies and what reviewers should see in the pull request. *[GitOps and Continuous Delivery Security]*

Replication factor — Number of copies of each piece of data kept in a cluster so that losing a node loses no data; multiplies storage. *[SIEM Architecture and Sizing]*

Reported distance (RD / AD) — The neighbour's own metric to the destination, as it advertised it (older Cisco texts call it 'advertised distance', not to be confused with administrative distance). *[Routing II: EIGRP, BGP at the Enterprise Edge, Redistribution]*

Reporting — Facts, methods, tools and versions, findings, timeline, limitations; written so a non-technical reader and a court can follow; separate opinion from evidence. *[Incident Response, Forensics, Automation]*

Repository — An index of packaged charts served over HTTP or as OCI artifacts in a registry (found via Artifact Hub). *[Helm, operators and the CRD ecosystem (with security)]*

repository_owner_id — Immutable numeric owner id; trusting it instead of the owner name defeats re-registration of a deleted or renamed organisation. *[CI/CD Pipeline Security]*

Representative period — The log window used for the usage indicators (R7): long enough to contain all current flows (monthly batch jobs, quarter closing), short enough to be processed in reasonable time, without incidents or migrations that skew the counts. Rules used only in rare situations (PCA) must be marked, not judged on hits. *[Firewall Policy: Design, Cleanup, Exposed Zone]*

Reproducible build — Same source + same toolchain = bit-identical artifact; lets a third party detect a tampered build. *[DevSecOps and Supply-Chain Security; Go for Security Tooling and Safe Code]*

Reproducible builds — Same source and toolchain give bit-identical binaries, so a published binary can be checked against the source. *[Start-ups, Municipalities, Teleassistance, Open Source]*

Repudiation → non-repudiation — central logging, session recording (bastion), signed logs *[Secure Architecture Patterns]*

Request smuggling — Proxy and server disagree on where a request ends (Content-Length vs Transfer-Encoding: CL.TE, TE.CL). *[OWASP Web Security Testing Guide v4.2]*

Require MFA — phishing-resistant (FIDO2) where possible *[Network and Authentication Attacks]*

Requirement levels — Basic (MUST), Standard (SHOULD) and requirements for elevated protection in each module; Basic protection implements only the MUST items as a first milestone. *[NCSC, BSI and Allied Cyber Authorities]*

Réseau d'anonymisation / Anonymisation network — Network of compromised machines an attacker group relays through to stay stealthy. *[ANSSI CyberDico FR/EN Glossary]*

Reserved L2 groups — 01:80:c2:00:00:00 STP BPDUs, 01:80:c2:00:00:03 802.1X PAE (Port Access Entity), 01:80:c2:00:00:0e LLDP, 01:00:0c:cc:cc:cc Cisco CDP/VTP (VLAN Trunking Protocol)/DTP (Dynamic Trunking Protocol). The 01:80:c2:00:00:0X block is never forwarded by 802.1D bridges; the Cisco group is flooded by non-Cisco switches. *[Ethernet, MAC Tables and ARP]*

Resident key — FIDO2 key stored on the token itself (ssh-keygen -O resident) and recoverable on a new machine with ssh-keygen -K; protect it with the token PIN. *[SSH in Depth]*

Residual risk — Risk remaining after management responses are implemented as planned. *[CISM Domain 2: Information Security Risk Management; CRISC Domain 2: IT Risk Assessment +6]*

Resource — Any data source or computing service the enterprise protects (database, API, SaaS tenant, sensor). *[Zero Trust Architecture SP 800-207]*

Resource-based policy (function policy) — Policy on the function listing who may invoke it (another account, S3, API Gateway); lambda:AddPermission edits it. *[Serverless and Runtime Security]*

Resource / kind — A REST object type (Pod, Deployment, Node); its short name (po, deploy, no) and API group come from kubectl api-resources. *[kubectl and Cluster Operations Mastery]*

Resource pooling — multi-tenant model, location independence (country/region/datacenter at best) *[Cloud Computing Security]*

resourceVersion — Object version derived from the etcd revision; a write carrying a stale one gets 409 Conflict (optimistic concurrency); also used to resume a watch. *[Kubernetes Architecture in Depth]*

Respond to Vulnerabilities — identify, remediate, root cause *[GenAI Secure Development (SSDF Profile); Secure Software Development: SSDF and SP 800-160]*

Responsibility matrix — Table of which security tasks the CSP owns and which the customer owns for each service model (the shared responsibility model). *[Security Architecture Models]*

restore errors — restores tested and verified *[Emerging Topics: Self-Assessment]*

Retention — how long each backup generation is kept; guide example: 15 days for dailies, 1 year for monthlies, 5 years for yearlies. *[IT Backup - ANSSI BP-100 R1-R32]*

RETEX — Retour d'expérience: lessons-learned process after the crisis (FS18); blame-free, completed at most 30 days after the end of the crisis. *[Cyber Crisis Management & Communication]*

Reusable secret — A credential an attacker can replay: password, NTLM hash, Kerberos ticket or key, API key, certificate private key. *[ANSSI Active Directory Recommendation Catalogue]*

Revenge — Disgruntled employee or ex-partner deletes data, plants a logic bomb, leaks secrets. *[Threat Actors and Threat Vectors]*

Reversible vs irreversible — Original recoverable from the mark and key, or not. Marks applied during generation cannot be reversible: there is no original. *[GenAI Secure Development and Content Transparency]*

Review and update — mature the program *[Patch, Configuration and Continuous Monitoring]*

Revocation — CRL (periodic signed list), OSCP (online query, RFC 6960), OSCP stapling. Let's Encrypt ended OSCP in 2025 in favour of CRLs; short lifetimes are the real fix: CA/B Forum ballot SC-081 cuts TLS certs to 200 days (Mar 2026), 100 (Mar 2027), 47 (Mar 2029). *[Network Security I - Crypto, PKI, IPsec, Firewalls, Wi-Fi]*

RFB — Remote Framebuffer, the protocol under VNC; no encryption of its own. *[Start-ups, Municipalities, Teleassistance, Open Source]*

RFC 1087 — IAB 1989 'Ethics and the Internet': unethical to seek unauthorized access, disrupt intended use, waste resources, destroy integrity or compromise user privacy. *[CISSP Domain 1: Security and Risk Management]*

RGS — Référentiel général de sécurité: French government security framework that sets the admissible cryptographic algorithms. *[IT Usage Charter and Outsourcing Security; Local Authorities: the Regulatory Security Framework +2]*

RGS annex B1 — Référentiel Général de Sécurité, annex B1: ANSSI rules for cryptographic mechanisms (algorithms and key sizes, e.g. RSA $\geq$ 2048 bits until 2030, SHA-2, AES). *[Access Switch Audit Grid: DAT-NT-025 R1-R71]*

RIA policy — Rich Internet Application cross-domain files (crossdomain.xml, clientaccesspolicy.xml) that grant Flash/Silverlight access. *[OWASP Web Security Testing Guide v4.2]*

Risk — Likelihood that a threat uses a vulnerability, times the resulting impact. *[CEH v13: Core Concepts, Phases and Legal Framework; CISM Domain 2: Information Security Risk Management +1]*

Risk acceptance — documented, time-limited decision by the asset owner not to remediate yet, with compensating controls *[CRISC Domain 3: Risk Response and Reporting; Vulnerability Management Programme]*

Risk aggregation — Combining related risks across units to see an enterprise exposure that single entries hide. *[CISM Domain 2: Information Security Risk Management; CRISC Domain 2: IT Risk Assessment]*

Risk appetite — The amount and type of risk an organization is willing to pursue or retain, set by the board. *[Digital Risk Governance - ANSSI-AMRAE 15 Steps; CISM Domain 1: Information Security Governance +6]*

Risk appetite vs tolerance — Appetite = amount of risk the organization is willing to pursue (strategic; CSF 2.0 GV.RM-02 asks for appetite and tolerance statements); tolerance = acceptable deviation per objective (operational thresholds, e.g. at most 4 h ERP outage per quarter). *[Governance and Risk Management]*

Risk capacity — The maximum loss the organization can absorb before it fails; appetite must sit below it. *[CISM Domain 2: Information Security Risk Management; CRISC Domain 1: Governance]*

Risk culture — Shared values and behaviours that determine how people identify, discuss and act on risk, starting with the tone at the top. *[CRISC Domain 1: Governance]*

Risk evaluation factors — RS.MA N2: asset criticality, functional impact, data impact, stage of observed activity, threat actor characterization, recoverability; they drive triage, escalation and recovery timing. *[Incident Handling and Response]*

Risk event — Occurrence or change of circumstances that, if it happens, affects an objective (a loss event when the effect is negative). *[CRISC Domain 2: IT Risk Assessment]*

Risk executive (function) — Individual or group at Tier 1 that provides organization-wide risk oversight so that system-level authorization decisions are consistent with the risk tolerance. *[NIST Risk Management: SP 800-39 and SP 800-30]*

Risk first — prioritise by risk; the first step is to understand the business and assess risk *[CISA Exam Strategy]*

Risk framing — Establishes the context: risk assumptions, constraints, tolerance, priorities. Output feeds every other component; it is where trust relationships with external providers are defined. *[NIST Risk Management: SP 800-39 and SP 800-30]*

Risk owner — business manager who accepts or funds treatment of a risk; security advises, the owner decides *[CRISC Domain 1: Governance; ISO/IEC 27001:2022 and 27002:2022 +2]*

Risk owner (propriétaire) — person who accepts residual risks at the end of the study; identified in the RACI (who is Responsible, Accountable, Consulted, Informed) of workshop 1 *[EBIOS Risk Manager]*

Risk practitioner — The CRISC role: facilitates identification, analysis, response and monitoring, and advises owners; does

not accept risk on their behalf. *[CRISC Domain 1: Governance]*

Risk prioritization inputs — Severity impact, exploitability, asset criticality, existing controls; then remediation → validation (re-test proves the control works). *[Governance and Risk Management]*

Risk profile — Overall portfolio of identified risk to which the enterprise is exposed at a point in time, with its current levels versus appetite. *[CRISC Domain 1: Governance]*

Risk (R.x) — a bad outcome for the cloud customer, rated by probability and impact; the numbered rows of the register. *[ENISA Cloud Computing Risk Register (2009)]*

Risk register — Central record of identified risks with owner, rating, treatment, status and review date. *[CISM Domain 2: Information Security Risk Management; CRISC Domain 2: IT Risk Assessment]*

Risk taxonomy — Common classification of risk categories (strategic, operational, IT, compliance, third party) so risks are named and aggregated consistently. *[CRISC Domain 1: Governance]*

Risk threshold — Operational trigger value, often on a KRI, that forces escalation or action before tolerance is breached. *[CRISC Domain 1: Governance]*

Risk threshold vs tolerance vs appetite — Appetite = overall willingness (expansionary, conservative, neutral); tolerance = acceptable deviation for a given risk; threshold = the KRI value that triggers escalation. *[Governance, Risk and Third-Party Management]*

Risk tolerance — Acceptable deviation from the appetite for a given objective or metric. *[CISM Domain 2: Information Security Risk Management; CRISC Domain 1: Governance +3]*

Risk universe — Complete set of risk categories and scenarios that could affect the enterprise, from which the register is populated. *[CRISC Domain 1: Governance]*

RITA / Zeek — Beacon and long-connection analytics / open-source network monitor that turns traffic into logs. *[SecurityX Practice Scenarios]*

Rn / Rn+ / Rn- — Baseline recommendation / reinforced variant for high security needs (*renforce*) / degraded fallback when the baseline is impossible (*degrade, a default*). *[Remote Work (Digital Nomadism)]*

ROA — Route Origin Authorisation: RPKI object signed by the prefix holder stating which AS may originate a prefix and up

to which maximum length. *[BGP, 802.1X & VPN; BGP and Internet Routing in Practice]*

RODC — Read-Only Domain Controller: holds a read-only copy and caches only chosen passwords, for sites without physical security. *[ANSSI Active Directory Recommendation Catalogue; Active Directory Security +1]*

RODC (Read-Only Domain Controller) — A DC for branch/untrusted sites that holds a read-only copy and caches only selected passwords, so its theft exposes far less. *[On-Prem Active Directory Architecture]*

RoE — Rules of engagement: the operational limits of the test (what, when, how, who to call). *[Security Testing and Assessment in Depth; Engagement Methodology and Reporting]*

RoE (Rules of Engagement) — How testing is done: scope, windows, allowed techniques, contacts, stop conditions. *[Pen-test Methodologies]*

Role in the stem — risk practitioner, risk owner, senior management or auditor: the answer is what that role should do *[CRISC Practice Scenarios]*

Role of automation (2.3) — Automate what is machine-checkable (inventory, configuration, vulnerabilities, via SCAP machine-readable checklists); manual assessment stays for policy, training, physical controls. Automation feeds dashboards, not decisions. *[Log Management and ISCM in Depth]*

Role (the what) — Protection acts before the attack stage, defence during it, resilience after it. *[Defence in Depth & Secure Internet Gateway]*

Role (Windows Server) — A major server function installed with `Install-WindowsFeature` or Server Manager, such as AD DS, DNS Server or DHCP Server. *[Windows Administration and Active Directory Basics]*

Roles (sec. 3) — Program managers, CIO, system owner, information owner, senior agency information security officer (SAISO), system security officer, property management officer, records management officer, privacy officer, users: property and records officers ensure media is sanitized before disposal. *[Malware, Servers and Media in Depth]*

Rolling release — A distro (Arch/BlackArch, Kali) that updates continuously rather than in fixed versions; you update often, not every few years. *[Kali Linux and Security Distros: Orientation for Learners]*

Root cause — The underlying condition that allowed the incident (missing patch, no MFA, flat network), as opposed to

the trigger (the exploit or the phishing email). *[Landmark Incidents and Lessons]*

Root cause analysis — Explaining why a flaw exists (missing patch process, no secure SDLC) so the fix addresses the cause, not one instance. *[Engagement Management]*

Root-cause category — Category named after why the flaw exists (e.g. Insecure Design) rather than its symptom (e.g. a specific attack). *[OWASP Top 10 - Web (2021 and 2025)]*

Root guard / BPDU Guard — STP protections: Root Guard blocks a port that receives a better (superior) BPDU; BPDU Guard err-disables an edge port that receives any BPDU. *[Switching, Routing, Wireless, Fabrics: Self-Assessment]*

Root of trust — Component trusted by design (boot ROM, fuses, TPM) that anchors verification or measurement of everything above. *[Hardware Security: Self-Assessment]*

Root path cost — Sum of the port costs from a switch to the root bridge; speed-based (1 Gb/s = 4 short, 20 000 long). *[Switching: VLANs, Trunks, Spanning Tree, EtherChannel]*

Rooting — Obtaining UID 0 and usually an unrestricted SELinux domain on a device, which removes the sandbox guarantees for every app on it. An app cannot prevent it; it can only detect some signs and let the backend decide (see Play Integrity below). *[Android Application Internals and Security]*

Rootkit — Hides at kernel, bootloader or firmware level to conceal processes and files; survives reinstall if in firmware. Detect from a clean boot medium or with measured boot. *[Malware, Attacks and Indicators]*

ROSI — Return on security investment: (loss avoided per year - control cost) / control cost. *[EU Governance and Regulation: Self-Assessment]*

Route leak — Advertising routes learned from one provider to another provider, turning your network into unintended transit. *[BGP, 802.1X & VPN; Routing II: EIGRP, BGP at the Enterprise Edge, Redistribution +1]*

Route leak vs hijack — Leak: legitimate route re-announced outside policy (customer to provider). Hijack: origin AS forged. Both fixed by RPKI/ROV plus ASPA and IRR filtering (MANRS). *[Networking Fundamentals II - Routing, L2, IPv6, Wi-Fi, Tools]*

Route types — EVPN route types: 1 Ethernet auto-discovery, 2 MAC/IP advertisement, 3 inclusive multicast (BUM peer list), 4 Ethernet segment (DF, designated forwarder, election), 5 IP prefix. *[Wireless, Data-Center Fabrics and Cloud Networking]*

Routed (native) mode — No encapsulation: the underlay routes pod ranges directly, learned by BGP (Calico) or programmed into the cloud route table or VPC (AWS VPC CNI). *[Kubernetes and Container Networking Explained]*

ROV — Route Origin Validation: routers mark each route valid, invalid or not-found (RFC 6811) from validator data received over RTR (RFC 8210). *[BGP, 802.1X & VPN]*

Row-level security — Engine policy filtering which rows a user can read or change, enforced whatever the query. *[Database Security]*

Rowhammer — Repeated DRAM row activation that flips bits in neighbouring rows, breaking memory integrity. *[CPU Side Channels and Memory Attacks]*

RPDB — Routing Policy DataBase: ordered ip rule list; each rule selects a routing table (local, main, default or a numbered one) by source, destination, mark, incoming interface or user id. *[Linux Networking Toolbox]*

RPF check — Reverse Path Forwarding: a router accepts multicast from source S only on the interface it would use to reach S; prevents loops, and explains why asymmetric routing breaks multicast. *[QoS, Multicast and WAN Services]*

RPKI — Resource Public Key Infrastructure: certificates issued by the regional internet registries (RIRs) proving who holds which prefixes and AS numbers. *[BGP, 802.1X & VPN]*

RPKI ROV — Resource Public Key Infrastructure Route Origin Validation: routers check each announcement against signed ROAs and drop 'invalid' origins (RFC 6811). *[Routing II: EIGRP, BGP at the Enterprise Edge, Redistribution]*

RPO — Maximum acceptable data loss measured in time; drives backup frequency. *[CISA Domain 4: IS Operations and Business Resilience; CISSP Domain 1: Security and Risk Management]*

RPO (Recovery Point Objective) — Maximum acceptable data loss, measured in time back from the incident; drives backup frequency and replication. *[Hybrid, Multi-Cloud and Connectivity Architecture; CISM Domain 4: Incident Management +3]*

RRM (Radio Resource Management) — Cisco controller function: DCA (dynamic channel assignment), TPC (transmit power control), coverage hole detection. Aruba ARM / Air-Match and Mist RRM do the same. *[Wireless, Data-Center Fabrics and Cloud Networking]*

RRSet signing (Fig. 8-48) — The bob.com RRSet carries its A records, the zone KEY and a SIG over the set; the resolver

checks it with the key vouched for by the parent zone. Test: `dig +dnssec example.com, delv example.com` (AD flag = validated). *[Network Security II - Authentication, Email, Web]*

RSAT (Remote Server Administration Tools) — Admin consoles and PowerShell modules (ActiveDirectory, GroupPolicy, DnsServer) installed on an admin workstation to manage servers remotely. *[Windows Administration and Active Directory Basics]*

RSSI — Responsable de la securite des SI: the information security officer (CISO). *[PPST Research Protection and Buying Qualified Security]*

RST — Reset: abort the connection (closed port, crash, firewall) *[TCP and UDP Deep Dive]*

RTBH (remotely triggered black hole) — Asking the ISP, usually with a BGP community, to drop all traffic to the attacked address: stops collateral damage but completes the denial of service for that address. *[L2/L3 Attacks: Detection and Mitigation]*

RTBH (RFC 7999) — Remotely triggered blackhole: tag a /32 with community 65535:666 so the upstream drops traffic to it; stops collateral damage but completes the DoS for that address. *[BGP, 802.1X & VPN]*

RTM (CRTM / S-CRTM) — Root of trust for **measurement**: first code that hashes the next stage before running it (CRTM = core RTM). Static (S-CRTM) at power-on, in boot ROM or a block verified by Intel Boot Guard / AMD PSB (Platform Secure Boot). *[Hardware Roots of Trust and the TPM 2.0]*

RTO — Retransmission TimeOut: time a TCP sender waits for an acknowledgement before resending; starts at 1 s (RFC 6298) and doubles after each timeout. *[CISA Domain 4: IS Operations and Business Resilience; CISSP Domain 1: Security and Risk Management +1]*

RTO (Recovery Time Objective) — Maximum acceptable time from disruption to service restored; drives restore throughput, standby capacity and runbooks. *[Hybrid, Multi-Cloud and Connectivity Architecture; CISM Domain 4: Incident Management +3]*

RTO + WRT ≤ MTPD — the time budget must close *[Business Continuity and ISO 22301]*

RTS on TLPT — Delegated Regulation (EU) 2025/1190 (OJ 18 June 2025, applies from 8 July 2025): criteria to designate entities, tester requirements, use of internal testers, pooled tests for shared providers *[DORA: Digital Operational Resilience]*

RTS / RTR — Roots of trust for **storage** (shielded locations: PCR = platform configuration registers holding boot hashes, NV = non-volatile memory, keys) and **reporting** (signs what the RTS holds, e.g. a TPM quote). The TPM provides both; it does not measure anything itself. *[Hardware Roots of Trust and the TPM 2.0]*

RTU (remote terminal unit) — Field controller at a remote site (substation, pump station) that reports to SCADA over a WAN or radio. *[Industrial (OT/ICS) Architecture; NIST OT and IoT Security]*

Rubeus — Kerberoast, AS-REP roast, ticket manipulation, delegation abuse. *[Host and Web Application Attacks]*

Rug pull (MCP) — A server silently changing its tool definitions after the user approved it. *[Agentic AI and MCP Security]*

Rules of engagement — Document setting what, when, how and by whom testing may be done. *[CEH v13: Practice Scenarios; Governance, Risk and Third-Party Management]*

Rules of the exercise — Rules of the game, e.g. players may not use a communication means declared unavailable by the scenario. *[Organising a Cyber Crisis Management Exercise]*

Ruleset — Ordered list of allow and deny rules; most engines apply the first rule that matches a packet. *[Firewall Policy and IDPS Deployment]*

Run-to-run totals — Totals carried from one processing stage to the next to prove nothing was lost in between. *[CISA Domain 3: IS Acquisition, Development and Implementation]*

Runbook — Step-by-step procedure for one known technical task (rotate a key, isolate a host), exact commands and expected output. *[Writing for Security Work]*

Running-config — Configuration active in RAM on a Cisco device; lost at reload unless copied to startup-config in NVRAM with `copy running-config startup-config` (or `write memory`). *[Cisco IOS Configuration Lab]*

Runs / giants — Runs < 64 bytes (collisions, duplex mismatch); giants > 1518 bytes (MTU or jumbo mismatch between neighbours). *[Network Troubleshooting: Method, Layers, Tools, Symptoms]*

Rup / Inno — protocol break and data transformation (e.g. Modbus to BACnet gateway) / anti-malware check of transferred data, ideally with the same policies as the OT SOC. *[ANSSI ICS/SCADA Security]*

Rup (protocol break) — the session is terminated and data rebuilt in another format, e.g. a Modbus-to-BACnet gateway, so

no attacker packet crosses as is. *[ANSSI ICS Detailed Measures v2 (2/2): technical measures]*

RVA (Relative Virtual Address) — PE address counted from the image base in memory, not from the file start; the loader adds the actual base chosen by ASLR. *[Executable Formats: ELF and PE]*

S

S.M.A.R.T. — Self-Monitoring, Analysis and Reporting Technology: reallocated sectors (05), pending sectors (C5), uncorrectable (C6), power-on hours, SSD wear/TBW. `smartctl -a /dev/sda, wmic diskdrive get status`. *[CompTIA A+ Core 1 - Hardware and Troubleshooting]*

S/MIME — End-to-end email signing and encryption with X.509 certificates; PGP is the web-of-trust alternative. *[CISSP Domain 4: Communication and Network Security]*

S0 / conn_state — Zeek connection state; S0 = originator sent SYN, no reply seen - the dominant state in a filtered-port scan. *[Network Scanning and Enumeration Reference (Authorized Labs)*]

SA — Security association: one-way agreement on keys and algorithms, identified by the SPI. *[CISSP Domain 4: Communication and Network Security]*

SA keys — user-managed JSON keys never expire and end up in repos: block with `iam.disableServiceAccountKeyCreation`, alert on `CreateServiceAccountKey`; prefer **impersonation** (`gcloud --impersonate-service-account`, needs `roles/iam.serviceAccountTokenCreator`, logged with the caller's identity). *[GCP Security Essentials]*

SA / SAD / SPI — Security Association: unidirectional context (peers, mode, protocol, algorithms, keys, lifetime) stored in the SAD and identified by its SPI carried in every AH/ESP header. *[ANSSI TLS and IPsec Guides: Full R Index]*

SA (security association) — One-way agreement between two peers on keys, algorithms and lifetime; identified by an SPI (security parameter index) carried in each packet. *[VPNs in Depth: IPsec/IKEv2, TLS VPN, WireGuard; VPN and Firewall Security]*

SA / SP (IPsec) — Security Association: the keys and algorithms for one direction of a tunnel; Security Policy: the rule saying which traffic must be protected, bypassed or dropped. *[TLS, IPsec and SSH Hardening]*

SaaS / PaaS / IaaS — Software, Platform or Infrastructure as a Service: the consumer rents a finished application, a man-

aged runtime, or raw virtual machines, storage and networks. *[\[Cloud Computing Security\]](#)*

SABSA — Sherwood Applied Business Security Architecture: layered model that derives security architecture from business requirements (contextual, conceptual, logical, physical, component, operational). *[\[CISM Domain 3: Information Security Program\]](#)*

SACL — System Access Control List: the part of an object's security descriptor that says which accesses are audited (events 4663, 4662). *[\[Windows and AD Logging: ANSSI PB-090; Windows Audit Policy and Event ID Reference\]](#)*

SAD (security association database) — Kernel table of active SAs: SPI, keys, algorithms, counters and lifetimes. *[\[VPN Planning, Design and Operations\]](#)*

SAE / DAJ — Service des achats de l'Etat (State purchasing service) / Direction des affaires juridiques of the finance ministries: co-authors of the purchasing guide. *[\[PPST Research Protection and Buying Qualified Security\]](#)*

SAE (Simultaneous Authentication of Equals) — WPA3-Personal password handshake (Dragonfly) that resists offline password guessing and gives forward secrecy. *[\[Wireless Security and IDS/IPS\]](#)*

Safe harbour — A promise, usually in a vulnerability disclosure policy, that the organisation will not take legal action against good-faith researchers who follow its rules. *[\[Law and Ethics for Security Practitioners\]](#)*

Safe method — HTTP method that must not change server state (GET, HEAD, OPTIONS, TRACE), so browsers and caches may send it freely. *[\[How the Web Works for Security People\]](#)*

Safeguard vs Benchmark — A safeguard says what outcome to reach (4.1 secure configuration process); a CIS Benchmark gives product settings to reach it (Level 1, Level 2). *[\[CIS Controls v8.1: All 153 Safeguards\]](#)*

Safety Instrumented System (SIS) — A separate, independent system (IEC 61511) that trips the process to a safe state if the normal control (the Basic Process Control System) fails - e.g. slams a valve shut on over-pressure. It is rated by Safety Integrity Level (SIL 1-4). Design rule: the SIS must be independent from control, so a compromise of the... *[\[Industrial \(OT/ICS\) Architecture\]](#)*

Sag / brownout — Momentary / prolonged low voltage. *[\[CISSP Domain 3: Security Architecture and Engineering\]](#)*

SAIV — secteurs d'activités d'importance vitale: state civil and military activities, justice, space and research, health, water, food, energy, electronic communications and media, transport, finance, industry *[\[Priority Measures and Essential Systems\]](#)*

Salt — Random per-account value mixed into a password hash so identical passwords give different hashes. *[\[Authentication, MFA and Passwords; Authentication and Session Design +1\]](#)*

Salt / pepper — Salt: per-password random value stored next to the hash, defeats rainbow tables. Pepper: secret value kept outside the database. *[\[Cryptography Primer\]](#)*

Salting — Random per-user value stored with the hash; identical passwords give different hashes and precomputed rainbow tables become useless. A pepper is a secret site-wide value kept outside the database. *[\[Cryptography\]](#)*

SAM — Software asset management: tracks installed software and licences to prevent both unlicensed use and unknown software. *[\[CISSP Domain 2: Asset Security\]](#)*

SAM (Secure Access Module) — Smart-card-sized secure chip in readers or UTLs that stores master keys and computes with them, so keys never sit in firmware. *[\[Physical Access Control and CCTV \(ANSSI PA-72\)\]](#)*

Same-Origin Policy — scheme + host + port. Everything below relaxes (CORS) or reinforces (COOP/CORP) it. *[\[Browser-Side Web Security Standards\]](#)*

SAML attacks — XML signature wrapping, unsigned/altered assertions, IdP-initiated replay. Defend by validating the full signed assertion, audience/recipient and clock skew. *[\[Network and Authentication Attacks\]](#)*

SAMM — Software Assurance Maturity Model: OWASP model to score and improve a secure development programme. *[\[CISSP Domain 8: Software Development Security; OWASP Secure Coding Practices and Developer Guide\]](#)*

SAN — Subject Alternative Name extension: the list of DNS names and IPs the certificate is valid for; browsers ignore the CN (Common Name) for host matching. *[\[OpenSSL and Certificate Tooling\]](#)*

SAN vs NAS — A Storage Area Network serves block volumes (LUNs) over Fibre Channel or iSCSI; Network-Attached Storage serves files over NFS/SMB. *[\[Data-Centre Architecture\]](#)*

Sandboxed iframes (R50-R52+) — sandbox attribute or CSP sandbox directive; strongest isolation is an iframe on a second origin (R52+). *[\[Browser-Side Web Security Standards\]](#)*

Sandboxing — Run untrusted code in an isolated environment: malware detonation (Cuckoo, ANY.RUN, vendor cloud sand-

boxes), browser site isolation, iOS/Android app sandboxes, Windows Sandbox, containers for CI jobs. Evasive malware checks for VM artefacts and sleeps. *[\[Security Operations - Baselines, Wireless, Mobile, Assets\]](#)*

Sanitizer — Function after which data is considered safe for a given sink (escaping, allow-list check, parameter binding). *[\[Secure Code Review by Language; Static Analysis and Code Scanning in Practice +1\]](#)*

SAQ (Self-Assessment Questionnaire) — Reduced self-attestation for smaller merchants, one variant per payment channel. *[\[PCI DSS v4.0.1, CVSS and FIRST\]](#)*

SAR (Security Assessment Report) — Assessor's findings per control after testing with SP 800-53A procedures. *[\[NIST SP 800-53r5 Controls in Practice; Risk Management Framework \(RMF\)\]](#)*

SARIF — JSON format (OASIS SARIF 2.1.0) that every modern scanner emits and GitHub, GitLab and Azure DevOps ingest. *[\[Static Analysis and Code Scanning in Practice\]](#)*

SAS token — Azure Shared Access Signature: signed URL granting time-limited access to storage without an identity. *[\[Cloud Configuration Review\]](#)*

SASE — Secure Access Service Edge: networking (SD-WAN) and security delivered together as a cloud service close to the user. *[\[CompTIA CySA+ CS0-003; Security Operations Architecture\]](#)*

SASE (Secure Access Service Edge) — A cloud-delivered bundle of SD-WAN plus security services (SWG, CASB, ZTNA, FWaaS) applied at the edge close to the user. *[\[Classic Enterprise Network Architecture; Secure Enterprise Network Landscape SP 800-215\]](#)*

SAST — Static Application Security Testing: analysis of source or byte code without running it. *[\[OWASP Top 10 2017 and Risk Rating\]](#)*

Satellite — High latency (GEO) or LEO constellations; encrypt links, treat as untrusted backhaul. *[\[CISSP Domain 4: Communication and Network Security\]](#)*

SBAT — Secure Boot Advanced Targeting: generation numbers in EFI binaries, revoked by raising one small UEFI variable. *[\[UEFI, Secure Boot and Bootkits\]](#)*

SBC — Session border controller: VoIP-aware border device that terminates external SIP, hides internal topology and filters attacks. *[\[ToIP and Virtualization Security\]](#)*

SBOM — Software bill of materials: machine-readable list of components and versions (SPDX, CycloneDX). *[\[Start-ups,](#)

Municipalities, Teleassistance, Open Source; IoT/IIoT Security and OT Detection +5]*

SBOM and the CRA — EU Cyber Resilience Act (Regulation 2024/2847): in force 10 Dec 2024, vulnerability and incident reporting from 11 Sep 2026, main obligations 11 Dec 2027; an SBOM is part of the technical documentation. *[Industry and Workforce Reports]*

SBOM minimum elements — NTIA 2021 baseline: supplier, component name, version, unique identifier (PURL, CPE), dependency relationship, SBOM author, timestamp; the August 2025 CISA draft *2025 Minimum Elements for an SBOM* adds component hash, license, tool name and generation context. *[Software Supply Chain Security]*

SBOM (software bill of materials) — Machine-readable list of every package and version inside an image (CycloneDX, SPDX). *[Container and Virtualization Security]*

SCA — Software composition analysis: inventory of third-party packages checked against vulnerability databases. *[OWASP Secure Coding Practices and Developer Guide]*

SCA and SBOM — Software composition analysis finds vulnerable and mis-licensed dependencies (Dependency-Track, Snyk, Trivy); the software bill of materials lists every component, in SPDX (ISO/IEC 5962) or CycloneDX format; a VEX (Vulnerability Exploitability eXchange) document states whether a CVE in a component is actually... *[Security Architecture - SDLC, IAM Design, Cloud]*

SCADA / DCS — Supervisory control and data acquisition (wide-area, e.g. pipelines, grids) / distributed control system (one plant, e.g. refinery). *[NIST OT and IoT Security]*

SCADA / HMI — Supervisory Control And Data Acquisition servers that collect data and send commands / Human-Machine Interface, the operator screen. *[ANSSI ICS/SCADA Security]*

SCADA (Supervisory Control and Data Acquisition) — Level 2 supervisory layer that collects data from and sends commands to controllers spread over a wide area. *[Industrial (OT/ICS) Architecture]*

Scale-out backup repository — Veeam construct grouping several repositories (performance tier) with object storage (capacity and archive tiers) under one target. *[Backup and Recovery Engineering]*

Scaled score — Raw points converted to a fixed scale so exam forms of different difficulty are comparable; ISACA 450/800

and ISC2 700/1000 are not percentages. *[Security Certification Landscape]*

Scan continuously — registry rescans, VEX for decisions, KEV first *[Cloud and DevSecOps: Self-Assessment]*

Scan vulns — govulncheck on every PR *[Go for Security Tooling and Safe Code]*

SCAP — Security Content Automation Protocol (NIST): standard formats (CVE, CPE, CVSS, XCCDF, OVAL) that let scanners exchange checks and results. *[CISSP Domain 6: Security Assessment and Testing; DISA STIG Viewer 3 and STIG Checklists +1]*

SCAP 1.3 (SP 800-126r3) — Suite of specs for automated checking: **XCCDF** checklist format, **OVAL** state tests, **OCIL** questionnaires, **CPE** platform names, **CCE** configuration ids, **CVE** vulnerabilities, **CVSS**, **ARF** asset reporting format for results, **AI** asset identification. SCAP = Security Content Automation Protocol. *[CIS Controls v8.1 and NIST SP 800-171r3]*

SCAP / XCCDF / OVAL — Security Content Automation Protocol; its checklist format; its test language - automated compliance scanning. *[SecurityX Practice Scenarios]*

SCCM / GPO — System Center Configuration Manager (now Microsoft Configuration Manager, MECM) for patching and software deployment; Group Policy Objects for AD-joined configuration baselines - both are 3.2 configuration management answers. *[CompTIA SecurityX CAS-005 - Exam Overview]*

SCCs — Standard contractual clauses: EU-approved contract terms that legitimize transfers to a country without an adequacy decision. *[CISSP Domain 1: Security and Risk Management]*

SCHANNEL — Secure Channel - the Windows TLS/SSL provider; protocol and cipher enablement lives under HKLM\SYSTEM\CurrentControlSet\Control\Security Providers\SCHANNEL; handshake errors are logged with source Schannel (e.g. event 36874/36888). *[CompTIA SecurityX CAS-005 - Exam Overview]*

Schema — The declared structure of a database: tables, columns, types, keys and constraints. *[SQL Basics for Security]*

Schema-on-read — Raw text stored, fields extracted at search time (Splunk search-time extraction): flexible, costlier per query. *[SIEM Architecture and Sizing]*

Schema-on-write — Fields extracted and typed at ingest (Elastic, Sentinel tables): fast queries, but a parsing error is stored forever. *[SIEM Architecture and Sizing]*

SCIM — System for Cross-domain Identity Management: API that creates and removes accounts in SaaS apps from the identity provider. *[SecurityX Practice Scenarios; Identity Protocols: OAuth, OIDC, SAML, FIDO2]*

SCIM 2.0 (RFC 7643/7644) — REST provisioning of users and groups from the IdP to AWS Identity Center, Entra, Google; deprovisioning at the source removes access everywhere. JIT (just-in-time) provisioning creates accounts at first login but never deletes them. *[Multi-Cloud Identity Federation]*

SCIP (PACS) — security continuous improvement plan (plan d'amélioration continue de la sécurité): list of measures per risk scenario with leader, cost, time frame. *[Digital Risk Governance - ANSSI-AMRAE 15 Steps]*

Scope — The exact list of assets, techniques, times and source addresses covered by the authorisation; anything outside is unauthorised even for the same client. *[Law and Ethics for Security Practitioners]*

Scope creep — Unapproved growth of the targets or activities during an engagement. *[CEH v13: Practice Scenarios; CISA Domain 3: IS Acquisition, Development and Implementation +1]*

Scope first — is the target, time window and technique inside the signed rules of engagement? *[PenTest+ Practice Scenarios]*

Scope limitation — Restriction that prevents the auditor gathering enough evidence; must be disclosed and may prevent an opinion. *[CISA Domain 1: Information System Auditing Process]*

Scope vocabulary — **PAN** primary account number (the 15-19 digit card number). **CHD** cardholder data = PAN + name, expiry, service code. **SAD** sensitive authentication data (full magnetic-stripe track, CVV2 card verification code, PIN) never stored after authorisation. **CDE** cardholder data environment: every system that... *[PCI DSS v4.0.1, CVSS and FIRST]*

Scope vs claim — Scope = what the client asks for (openid profile api:read); claim = a fact about the subject inside a token (email, groups). *[Identity Protocols: OAuth, OIDC, SAML, FIDO2]*

Scoping and tailoring — Scoping selects which baseline controls apply to a system; tailoring modifies the selected controls (parameters, compensating controls) to fit the mission. Both

start from a standard baseline such as NIST SP 800-53B, which gives low, moderate and high control baselines matched to the FIPS 199 impact level. Example: a... [*\[CISSP Domain 2: Asset Security\]*](#)

Score-based trust algorithm — Each data source gives a weighted value; the total confidence is compared with a per-resource threshold; below it, access is denied or reduced (read but not write). [*\[Zero Trust Architecture SP 800-207\]*](#)

SCP / RCP — AWS Organizations service control policy (caps what your principals may do) and resource control policy (caps what anyone may do to your resources). [*\[Cloud and DevSec-Ops: Self-Assessment\]*](#)

SCP (Service Control Policy) — AWS Organizations policy that caps the permissions available in member accounts; it grants nothing, it only limits. [*\[Designing a Secure SME Network and Cloud Landing Zone\]*](#)

SCRAM-SHA-256 — Salted challenge-response password authentication used by PostgreSQL and MongoDB; the password never crosses the network. [*\[Database Security\]*](#)

Screened subnet — Modern name for a DMZ built between two firewall interfaces (outer and inner), so inbound and outbound are filtered separately. [*\[Classic Enterprise Network Architecture\]*](#)

Screened subnet (DMZ) — Network zone between two firewalls hosting internet-facing servers, so a compromise there does not reach the internal LAN. [*\[Security Operations Architecture; Firewall Policy Management and IDS/IPS\]*](#)

Scrubbing — Diverting traffic (by BGP or DNS) through a provider's filtering centres, which drop attack packets and return clean traffic by tunnel. [*\[DDoS: Protection Options, Response, Non-Participation; L2/L3 Attacks: Detection and Mitigation\]*](#)

Scrubbing centre — Provider data centre that receives diverted traffic, drops the attack and returns clean traffic to the customer over GRE tunnels or direct interconnects. [*\[DDoS and Edge Protection\]*](#)

Scrutinize explicitly — multiple dynamic and static attributes build a confidence level per access [*\[DoD Zero Trust Reference Architecture v1.0\]*](#)

SD-WAN (software-defined WAN) — Overlay that steers branch traffic over any transport (MPLS, broadband, 4G/5G) from a central controller. [*\[Secure Enterprise Network Landscape SP 800-215\]*](#)

SDDL — Security Descriptor Definition Language: text form of permissions; used to restrict who can read a log channel. [*\[Windows and AD Logging: ANSSI PB-090\]*](#)

SDN — Software-Defined Networking: control plane separated from data plane; the controller (OpenFlow, NSX) pushes rules programmatically - protect the controller API. [*\[Security Operations Architecture\]*](#)

SDO — Service delivery objective: level of service to be delivered during alternate processing mode. [*\[CISA Domain 4: IS Operations and Business Resilience\]*](#)

SDO (Service Delivery Objective) — Level of service to be reached during the alternate-processing mode until full recovery. [*\[CISM Domain 4: Incident Management\]*](#)

SDP (software-defined perimeter) — Access model where a controller authenticates the subject before a gateway opens a tunnel to the resource; ports stay closed by default. [*\[ANSSI Zero Trust Model\]*](#)

Sealed Secrets — Controller plus kubeseal CLI: secrets encrypted with the cluster controller's public key, safe to commit, decryptable only in that cluster. [*\[GitOps and Continuous Delivery Security\]*](#)

Sealing — Encrypting data so the TPM releases it only when selected PCRs match expected values. [*\[ANSSI GNU/Linux Hardening Deep Dive \(BP-028 R1-R49\); Hardware Roots of Trust and the TPM 2.0\]*](#)

Sealing (scellement) — Cryptographic fingerprints of files and configuration recorded before opening, re-checked to detect tampering. [*\[Internet Voting for Non-Political Elections\]*](#)

seccomp — Kernel filter restricting which system calls a process may make; Docker's default profile blocks about 44 of 300+. [*\[Docker Container Security\]*](#)

seccomp-BPF — Kernel filter restricting which system calls a process may make. [*\[GNU/Linux BP-028: Kernel Build, Files and Services; Linux Isolation Primitives and Sandboxes\]*](#)

SecNumCloud — French ANSSI (national cybersecurity agency) qualification for trusted cloud providers; version 3.2 (2022) adds immunity from non-EU laws such as the US CLOUD Act. [*\[Cloud Outsourcing and Virtualization Lifecycle\]*](#)

SecOC (Secure Onboard Communication) — AUTOSAR module adding a truncated MAC and freshness value to selected PDUs so receivers can reject forged or replayed messages on CAN, CAN FD, FlexRay or Ethernet. [*\[Automotive and Embedded Security\]*](#)

Secret — Like a ConfigMap but for sensitive values; only base64-encoded, NOT encrypted, unless encryption-at-rest is enabled on the cluster. [*\[Kubernetes hands-on: learn it in your own lab\]*](#)

Secret at rest — base64 only. Enable Encryption Configuration on the API server (kms v2 provider with the cloud KMS, else aescbc/secretbox) then rewrite: `kubectl get secrets -A -o json | kubectl replace -f -`. Managed: EKS envelope encryption, GKE application-layer secrets encryption, AKS KMS. [*\[Kubernetes Security\]*](#)

Secrets encrypted and external — KMS v2 at rest, External Secrets Operator / CSI driver, never in git or env vars [*\[Kubernetes Security\]*](#)

Secrets management — Tokens, certificates, passwords, keys: central vault (HashiCorp Vault, AWS Secrets Manager, Azure Key Vault), dynamic short-lived secrets, rotation on schedule and on incident, deletion at decommission, no secrets in code or CI logs. [*\[Security Engineering - IAM, Endpoints, Network, Hardware, OT, Automation\]*](#)

Secrets Store CSI driver — mounts secrets from the backend as files at pod start, optional sync to a Secret; Vault Agent injector does the same with a sidecar. [*\[Kubernetes Security\]*](#)

Section — Named region of the file for the linker and tools (.text code, .data, .rodata/.rdata, .bss); ELF may strip the section table, PE loads sections directly. [*\[Executable Formats: ELF and PE\]*](#)

Section 8 open issues — computing performance (latency, off-line sync), reliability (network dependence, provider outages, safety-critical processing), economic goals (business continuity, SLA evaluation, portability, interoperability, DR), compliance (visibility, physical data location, jurisdiction, forensics), information security... [*\[Cloud Computing Security\]*](#)

Section (manual) — one of the numbered groups (1-9) a manual is split into, so the same name can document a command and a file format separately (passwd(1) the command, passwd(5) the file). [*\[Read the Manual: man, help, tldr and info\]*](#)

Secure baseline for cloud — CIS Foundations Benchmarks for AWS/Azure/GCP; landing zones with guardrails enforcing them (AWS service control policies SCPs, Azure Policy, GCP organization policies). [*\[NIST Cloud, Virtualization, and Container Security\]*](#)

Secure baseline (PW.9.1) — Every security-relevant setting chosen so that defaults are secure and do not weaken platform, network or service security functions. [*\[SSDF v1.1: the 42 Tasks\]*](#)

Secure Boot vs Measured Boot — Secure Boot **blocks** unsigned code; Measured Boot **records** hashes into TPM PCRs for attestation (Windows Defender System Guard). *[CompTIA A+ Core 1 - Hardware and Troubleshooting]*

Secure distribution — Reports and evidence travel encrypted to named recipients only (client portal or encrypted archive, key sent out of band), with a retention and destruction date. *[Engagement Management]*

Secure element — Tamper-resistant chip that stores keys and performs crypto without exposing them (SIM, payment chip, Titan M2). *[Laptops, Mobile Devices, Virtualization Hardware]*

Secure Enclave — Apple coprocessor inside the SoC holding biometric templates and data-protection keys. *[macOS Security for Defenders; Laptops, Mobile Devices, Virtualization Hardware +1]*

Secure processing environment (EHDS) — controlled environment operated by or for a Health Data Access Body where permit holders process pseudonymised data; access control, logging, no download of personal data *[Data Act, Data Governance Act and EHDS]*

Secured comms — network location gives no trust *[Zero Trust Architecture SP 800-207]*

Secured-core — OEM class with TPM 2.0, Secure Boot, DRTM (System Guard), Kernel DMA Protection, HVCI, SMM protection enabled at the factory; ANSSI favours it for Server 2022+ (Back to basics). *[ANSSI Endpoint Security: Overview and Windows]*

Security accreditation (homologation) — formal decision by a business authority to accept the residual risks of a system before and during its use. *[Local Authorities: the Regulatory Security Framework; Digital Risk Governance - ANSSI-AMRAE 15 Steps]*

Security architecture — The structured design of controls and their relationships across the enterprise, aligned with business architecture. *[CISM Domain 3: Information Security Program]*

Security baseline — Minimum mandatory configuration or control set for a class of assets. *[CISM Domain 3: Information Security Program]*

Security baseline scanning — Compare configuration to a hardened baseline (CIS Benchmark, DISA STIG = US Defense Security Technical Implementation Guide) with SCAP content (tree below). Tools: OpenSCAP, Nessus compliance audits,

Microsoft Security Compliance Toolkit. *[Vulnerability Scanning Methods]*

Security baseline (socle de securite) — applicable references (ANSSI hygiene guide, internal security policy PSSI, government framework RGS, NIS / LPM regulatory rules, ISO 27002 controls) and the identified gaps with justification *[EBIOS Risk Manager]*

Security by design / by default — Requirements from day one; defaults are the most restrictive settings that remain usable *[OWASP Developer Guide v4.2 - Chapter by Chapter]*

Security champion — Developer in each team trained to be the first point of contact for security questions. *[OWASP Secure Coding Practices and Developer Guide]*

Security charter — board- or CEO-signed document granting the CISO mandate, scope, authority (stop a go-live, access to all data for investigation) and reporting line *[Building a Security Program]*

Security class agreement (SCA) — mutual agreement between a data provider and the PaaS provider fixing the security class of the data; every replica of the data inherits the same class; hosts qualified by class decide access (Bell-LaPadula model, 'no read up': a report written at *confidential* is readable only by subjects and hosts cleared at... *[Cloud Reference Architecture and Access Control]*

Security component — Tamper-resistant chip (smart card, TPM, secure enclave, token) that stores keys and performs crypto without exporting them. *[Authentication, MFA and Passwords]*

Security control — Any safeguard or countermeasure that reduces risk to an asset. The exam classifies every control twice: by **category** (who or what implements it: technical, managerial, operational, physical) and by **type** (what it does to the threat: preventive, deterrent, detective, corrective, compensating, directive). *[Security Controls]*

Security coprocessors and CPU extensions — Apple T2/Secure Enclave, Google Titan, Microsoft Pluton; CPU extensions AES-NI (hardware AES acceleration), SGX/TDX, ARM Pointer Authentication, Intel CET (control-flow enforcement: shadow stack against ROP = return-oriented programming exploits). *[Security Engineering - IAM, Endpoints, Network, Hardware, OT, Automation]*

Security culture — the shared beliefs, norms and habits that decide what people do about security when no one is watching *[Security Awareness and Culture Programme]*

Security data lake — Cheap, large, columnar store (object storage + query engine) holding full-fidelity logs for long retention and ad-hoc hunting, separate from the SIEM's hot index. *[Security Operations Architecture]*

Security distribution — A Linux OS bundling assessment, forensics and reversing tools ready to use; examples: Kali, Parrot, BlackArch. *[Kali Linux and Security Distros: Orientation for Learners]*

Security event — Any observable occurrence in a system or network; most are benign. *[CISM Domain 4: Incident Management]*

Security group — Cloud virtual firewall attached to instances; automation keeps its rules consistent and reviewed. *[Incident Response, Forensics, Automation]*

Security group / NSG — Stateful virtual firewall attached to a cloud instance or subnet (AWS security group, Azure network security group). *[Cloud Configuration Review]*

Security incident — An event that jeopardizes confidentiality, integrity or availability or violates policy, and needs a response. *[CISM Domain 4: Incident Management]*

Security kernel — Hardware, firmware and software that implement the reference monitor. *[CISSP Domain 3: Security Architecture and Engineering; CISSP Domain 5: Identity and Access Management]*

Security officer — Person in charge of IT security in the organisation (RSSI, responsable de la securite des systemes d'information); first contact for loss, theft or seizure. *[Business Travel and SME Cybersecurity]*

Security operations — 33 % - logs, indicators, tools, threat intel, efficiency *[CompTIA CySA+ CS0-003]*

Security target — Document describing a product's security functions, assumptions and threats, against which it is evaluated (Common Criteria, CSPN). *[PPST Research Protection and Buying Qualified Security]*

Security Target (ST) — Vendor's claims for a specific product, evaluated against a PP or standalone. *[CISSP Domain 3: Security Architecture and Engineering]*

Security visa (Visa de securite) — umbrella term for an ANSSI certification or qualification of a product or provider. *[ANSSI ICS Detailed Measures v2 (1/2): organisation and accounts]*

Security zones — Internet (untrusted), screened subnet (DMZ, demilitarised zone), internal, guest, management, OT (operational technology). Default deny between zones; each crossing logged. Screened subnet = public services that must never

reach the internal zone directly. **[Securing Enterprise Infrastructure]**

Segment / datagram — A TCP unit of data is a segment; a UDP unit is a datagram. Both travel inside IP packets. **[TCP and UDP Deep Dive]**

Segment (ELF program header) — Run-time view: a contiguous range the loader maps with one set of permissions (PT_LOAD R E); several sections fit in one segment. **[Executable Formats: ELF and PE]**

Segmentation — Keep sensitive data in its own zone, database or tenant so a breach elsewhere does not reach it. **[Data Protection and Resilience]**

Segregation of duties (SoD) — Splitting critical tasks (develop, approve, deploy) among different people so that one person cannot commit and hide an error or fraud. **[CRISC Domain 4: Information Technology and Security]**

Selecting techniques (6.3) — Objectives first, then classes, then techniques and viewpoint (internal/external, overt/covert). Weigh impact on production, presence of PII, personally identifiable information (test on non-production with fake data), and how closely test mirrors production. **[Security Testing and Assessment in Depth]**

Selective disclosure — present only the needed attributes or predicates (e.g. `age_over_18 = true`) instead of the whole credential; salted-hash disclosures in SD-JWT, per-element digests in mdoc **[eIDAS 2 and the EU Digital Identity Wallet]**

Selective vs full wipe — Selective removes managed apps and data (BYOD); full wipe factory-resets the device (corporate owned). **[Hardware: Self-Assessment]**

Self-encrypting drive (SED) — Drive following the TCG (Trusted Computing Group) Opal spec encrypts everything with an internal key; unlock at pre-boot; crypto-erase in seconds; pair with TPM to avoid a pre-boot password. Host-based encryption (BitLocker, LUKS) is the software alternative. **[Security Engineering - IAM, Endpoints, Network, Hardware, OT, Automation]**

Self-heal — Argo CD option that re-syncs automatically when live objects drift from git, not only when git changes. **[GitOps and Continuous Delivery Security]**

Self-healing hardware / virtual hardware — Firmware resilience (NIST SP 800-193): automatic recovery to a golden firmware image; vTPM and virtual HSM give VMs the same root-of-trust APIs. **[Security Engineering - IAM, Endpoints, Network, Hardware, OT, Automation]**

SELinux — Label-based MAC from the NSA, default on RHEL, Fedora, Rocky, Alma, Android: every file, process and port carries a context `user:role:type:level` and the policy lists which type may do what to which type (type enforcement). **[Linux Hardening in Practice]**

Semantic conventions — Standard OTel attribute names (`service.name`, `http.request.method`, `user.id`, `k8s.pod.name`) so every source describes the same thing the same way. **[Observability and Security Telemetry Pipelines]**

Sensitivity label — Purview classification tag (for example Confidential) stored in the file metadata that can encrypt the content and restrict who opens it, wherever the file goes. **[Microsoft 365 Hardening; Data Security Posture in the Cloud]**

Sensor / agent — Component that collects and analyses traffic (sensor, network) or host events (agent); reports to a management server with a database and consoles. **[Firewall Policy Management and IDS/IPS]**

Server security principles (sec. 2.4) — Simplicity, fail-safe, complete mediation, open design (security must not rely on secrecy of the design), separation of privilege, least privilege, psychological acceptability (controls users will actually follow), least common mechanism, defense in depth, work factor, compromise recording. **[Security Operations: Logs, Malware, Servers, Media]**

Server-side apply — `kubectl apply --server-side`: the API server merges your fields and tracks per-field ownership, replacing the older client-side three-way merge that stored the last-applied config in an annotation. **[kubectl and Cluster Operations Mastery]**

Service — A stable virtual IP and DNS name load-balancing across a Deployment's Pods (types: ClusterIP internal, NodePort, LoadBalancer). **[Kubernetes hands-on: learn it in your own lab]**

Service account (Kubernetes) — Namespaced identity for pods; its token authenticates the pod to the API server. **[Kubernetes Security]**

Service account (SA) — Non-human Google identity used by workloads; also a resource on which others can be granted impersonation. **[GCP Security Essentials]**

Service agreement — Contract plus SLA that fixes what the cloud provider promises, its limits and the customer's obligations. **[Cloud Outsourcing and Virtualization Lifecycle]**

Service agreement (SP 800-146 §3) — **Promises** (availability, remedies, security), **limitations** (scheduled outages, force ma-

jeure, service changes), **obligations** (acceptable use, licensed software), and recommendations: negotiate, log SLA breaches, keep an exit plan. **[Cloud Computing Security]**

Service (daemon) — A background program started by the OS without a logged-in user, often with high privileges (sshd, the Windows Print Spooler, launchd daemons). **[Operating System Concepts for Beginners]**

Service discovery — A registry (e.g. Consul, DNS-based) where services register and look each other up, so instances can come and go behind a stable name. **[Web Application and Microservices Architecture]**

Service disruption — DDoS, wiper malware, ransomware without decryption intent. **[Threat Actors and Threat Vectors]**

Service manager — The component that starts, restarts and supervises services: systemd on most Linux, the Service Control Manager (services.exe) on Windows, launchd on macOS. **[Operating System Concepts for Beginners]**

Service mesh — Sidecar proxies (e.g. Envoy) beside each service giving automatic mutual TLS, retries, timeouts and traffic telemetry without changing app code. **[Web Application and Microservices Architecture]**

Service partitioning — Running each service under its own account with minimal capabilities and kernel isolation (namespaces, seccomp, cgroups), e.g. `systemd NoNewPrivileges=yes, ProtectSystem=strict, PrivateTmp=yes` (BP-028 R64-R66). **[ANSSI GNU/Linux Hardening Deep Dive (BP-028 R1-R49)]**

Service perimeter — VPC Service Controls boundary: Google API calls crossing it are denied unless an access level or ingress/egress rule allows them. **[GCP Security Essentials]**

Service principal — The identity of an application inside one Entra tenant, holding its role assignments and credentials. **[Azure and Entra ID Security Essentials]**

Service principals — consent grants and new app credentials **[Microsoft 365 Hardening]**

Session — isolated logon workspace: session 0 hosts services only (since Windows Vista, so services cannot draw on the user's desktop), sessions 1+ host interactive users. **[Windows Internals for Defenders]**

Session cookie — token set after login that proves an authenticated session on each request; a bearer secret until it expires **[Identity Attacks and ITDR: Entra ID and Okta; Browser and Extension Security]**

Session fixation — Attacker plants a known session id in the victim's browser before login, then reuses it once the victim authenticates. *[Authentication and Session Design]*

Session management — Controls on an authenticated session: timeouts, re-authentication, token binding, logout. *[CISSP Domain 5: Identity and Access Management]*

Session puzzling — Two flows reuse the same session variable, so setting it in one (e.g. password reset) grants access in the other. *[WSTG v4.2 - Complete Test Catalogue]*

Session tokens — Capture via proxy; check predictability; decode JWT, test alg confusion (none, HS256 vs RS256). *[Enumeration and Scripting]*

SET — Social-Engineer Toolkit: site cloning, credential harvest, payload delivery. *[Cloud, Wireless, Social Eng and Specialized Attacks]*

set -e (erexit) — exit when a command fails, instead of carrying on with bad data *[Bash Scripting from Zero]*

set -o pipefail — a pipe fails if ANY stage fails, not only the last one *[Bash Scripting from Zero]*

set -u (nounset) — an unset variable is an error, not an empty string (no more `rm -rf /*`) *[Bash Scripting from Zero]*

Setup mode / user mode — No PK enrolled = **setup mode**, variables writable without signature and Secure Boot not enforced. Enrolling a PK switches to **user mode**. UEFI 2.5 adds **audit** and **deployed** modes (deployed cannot fall back without a platform-specific action). *[UEFI, Secure Boot and Bootkits]*

Severe incident — CRA Art. 14(5): an incident that harms or can harm the product's ability to protect data or functions, or that led to malicious code in the product or its update channel. *[Cyber Resilience Act and AI Act]*

SGDSN / AIST — Secretariat general de la defense et de la securite nationale (Prime Minister's defence secretariat) / its directorate for protection of scientific and technical assets. *[PPST Research Protection and Buying Qualified Security]*

Shadow admin — account with admin-equivalent rights obtained indirectly (nested groups, delegated permissions) that does not appear in admin group lists. *[Industry and Workforce Reports]*

Shadow AI — AI tools and features used without approval or inventory: browser chatbots, SaaS copilots switched on by default *[AI Governance Programme]*

Shadow API — Endpoint running in production that is missing from the inventory and the gateway (old version, debug route). *[OWASP API Security Top 10 - 2023]*

Shadow data — Copies of sensitive data outside governed stores: snapshots, exports, dev databases restored from production, CSVs in buckets. *[Data Security Posture in the Cloud; IBM Breach Cost and X-Force Index 2024]*

Shadow IT — IT systems or cloud services used without IT approval, outside inventory and controls. *[CISA Domain 4: IS Operations and Business Resilience; CISSP Domain 2: Asset Security +1]*

Shadow SaaS — SaaS apps used without IT approval, often signed up with a corporate email and a personal password, outside SSO and offboarding. *[SaaS Security and Google Workspace]*

Shadowed / redundant rule — Shadowed: never matched because an earlier rule catches the same traffic. Redundant: duplicates what another rule already allows. *[Firewall Policy Management and IDS/IPS]*

Shadowed rule — Never matched because a broader rule above already decides; a broad ALLOW above a specific DENY silently voids the restriction. *[Firewall Policy: Design, Cleanup, Exposed Zone; Operations, Security, Troubleshooting: Self-Assessment]*

Shared fate — Newer framing promoted by some providers (Google Cloud from 2021): the provider also ships secure defaults, blueprints and guidance so the customer's part is easier to get right, instead of only drawing a responsibility line. *[CSA Cloud Controls Matrix and Guidance]*

Shared signaling (Sec. 4.8) — IdP notifies RPs of account events (credential change, compromise): CAEP (continuous access evaluation) / RISC (risk incident sharing) profiles of the OpenID Shared Signals Framework. *[Digital Identity Guidelines SP 800-63-4]*

Shebang — The `#!` interpreter first line of a script; the kernel runs that interpreter with the script's path as argument. *[Bash Scripting from Zero]*

Shell builtin — command implemented inside the shell itself (`cd`, `export`, `history`, `set`); it has no file on disk and no own man page, so `man cd` fails and `help cd` works (`bash`). *[Master Any Command-Line Program Fast, on Every OS]*

Shim — Small Microsoft-signed EFI program that then verifies the distribution's own key, so each distro does not need Mi-

crosoft to sign every kernel. *[ANSSI GNU/Linux Hardening Deep Dive (BP-028 R1-R49)]*

SI maitrise (controlled IS) — system whose components are known, configured and maintained by the operator or a contracted provider, so its security level can be guaranteed; excludes BYOD. *[Protecting Essential IS - PA-085 R1 to R62]*

SID filtering — A control on inter-forest trusts that strips foreign security identifiers (SIDs) so a compromised trusted forest cannot inject privileged SIDs (SID history abuse). *[On-Prem Active Directory Architecture]*

SID / RID — Security Identifier of an account (`S-1-5-21-
<domain>-<RID>`); the Relative ID 500 = built-in Administrator, 512 = Domain Admins, 544 (in `S-1-5-32-544`) = local Administrators. *[Windows and Active Directory for Defenders]*

SID (Security Identifier) — Unique, never reused number identifying a user, group or computer, e.g. `S-1-5-21-...-1104`; permissions store SIDs, not names. *[Windows Administration and Active Directory Basics]*

Side-channel attack — Recovers secrets from indirect effects of computation (timing, power, EM, cache state) instead of breaking the algorithm. *[CPU Side Channels and Memory Attacks]*

SIE (système d'information essentiel) — information system an OSE declares to ANSSI because the essential service depends on it; the 23 rules of the arrete apply to it. *[Protecting Essential IS - PA-085 R1 to R62]*

SIEM — Security Information and Event Management: central log platform that collects, normalizes, correlates and alerts. *[SIEM and Detection Engineering; Security Tools and Techniques +1]*

SIEM / EDR / FIM — Security Information and Event Management (central log correlation); Endpoint Detection and Response (host agent); File Integrity Monitoring (alerts on changed files). *[Attack Mitigation and Vulnerability Response]*

SIEM (security information and event management) — Platform that collects, normalizes, stores and correlates logs from every source to raise alerts and support investigations. *[Security Operations]*

SIEM / SOAR — Security information and event management (central log correlation and alerting) / security orchestration, automation and response (playbooks that act on alerts). *[Incident Handling and Response]*

SIEM / SOAR / EDR — Security Information and Event Management (collect, correlate, alert); Security Orchestration, Automation and Response (playbooks); Endpoint Detection and Response. *[CompTIA CySA+ CS0-003]*

SIF — Situation information file: concise 'state of the world' document handed to players at the start. *[Organising a Cyber Crisis Management Exercise]*

Sighting — Record that an indicator was seen (or is a false positive) by an organisation; feeds decay and confidence. *[Cyber Threat Intelligence Lifecycle]*

Sigma — open, vendor-neutral YAML format for detection rules, converted by sigma-cli into the query language of each SIEM. *[SIEM and Detection Engineering]*

Sigma / YARA / MISP — generic log-detection rule format / pattern rules for files and memory / open threat-intelligence sharing platform and its JSON format. *[Security Supervision: ANSSI GP-112 and PG-113]*

Signalling firewall — GSMA category 1-3 filtering on SS7, Diameter, GTP; SEPP for 5G *[Telecom and 5G Security]*

Significant incident (Art. 23(3)) — has caused or is capable of causing severe operational disruption of the services or financial loss for the entity, **or** has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage *[NIS2 Directive: EU-wide Obligations]*

Significant incident (NIS2) — Incident that caused or can cause severe operational disruption or financial loss to the entity, or considerable material or non-material damage to others. *[Cyber Incident Reporting Obligations]*

SIIV — système d'information d'importance vitale, declared to ANSSI, accredited, audited by PASSI LPM every 3 years, incidents notified to ANSSI *[Priority Measures and Essential Systems; Security Supervision: ANSSI GP-112 and PG-113]*

SIIV / SIE — Information system of vital importance (OIV, LPM) / essential information system (OSE, NIS). Both are declared to ANSSI. *[Local Authorities: the Regulatory Security Framework]*

SILL — Socle interministeriel de logiciels libres: the French administration's catalogue of recommended open-source software, cited as a maturity signal. *[Start-ups, Municipalities, Teleassistance, Open Source]*

Silly window syndrome — Tiny window updates → tiny segments. Fixed by Clark's receiver rule and Nagle's sender rule (Tanenbaum 6.5.8). *[TCP and UDP Deep Dive]*

Silver ticket — Forged TGS for one service, signed with that service account hash; quieter than golden. *[Identity and Active Directory Assessment]*

SIM swap — Fraudulent transfer of a victim's phone number to a SIM or eSIM controlled by the attacker, obtained by social engineering or bribing carrier staff, or by a fraudulent **port-out** (number moved to another operator). From then on, every call and SMS OTP (one-time password) goes to the attacker. No protocol weakness... *[Authentication, MFA and Passwords; Telecom and 5G Security]*

Simple vs complex signature — simple: a technical marker (IP, domain, firmware hash, URL part); complex: an attack scenario, heuristic or statistical operation, rule language or script. *[OT Detection Doctrine, Integrators and Training]*

Single sign-on — One authentication session reused by many applications: Kerberos inside the domain, SAML/OIDC on the web. Risk: one compromised session opens everything, so protect it with MFA and short token lifetimes. *[Identity and Access Management]*

Singling out — isolating the record of one person in a dataset; first of the three anonymisation tests of Article 29 Working Party Opinion 05/2014 *[Privacy Engineering and PETs]*

Sink — Dangerous API where untrusted data causes harm: SQL execute, shell, file open, HTML output, deserializer. *[Secure Code Review by Language; Static Analysis and Code Scanning in Practice]*

SIP / RTP / SRTP — Session Initiation Protocol (call signalling) / Real-time Transport Protocol (voice media) / its encrypted and authenticated version (RFC 3711). *[ToIP and Virtualization Security]*

SIP (System Integrity Protection) — kernel-enforced policy (since OS X 10.11 El Capitan, 2015) that stops even root from modifying /System, /usr (except /usr/local), /bin and /sbin, from attaching a debugger to Apple processes and from loading unsigned kernel extensions; only changeable from Recovery with csrutil. *[macOS Security for Defenders]*

SIP trunk — Connection to the operator carried over IP with SIP instead of TDM lines. *[ToIP and Virtualization Security]*

SIR — Specific Intelligence Requirement: a narrower subquestion of a PIR that one collection effort can answer. *[Cyber Threat Intelligence Lifecycle]*

SIRR — IS giving direct access to unprotected IRR: laptop, USB key, file server. **Not** a SIRR: physical-security systems (cameras, access control, fire detection, SCADA), nor a mail server

carrying only encrypted IRR. *[PPST Research Protection and Buying Qualified Security]*

SIS / BPCS — Safety Instrumented System, independent controllers that bring the process to a safe state / Basic Process Control System, the normal control PLCs. *[ANSSI ICS/SCADA Security]*

SIS (Safety Instrumented System) — Independent controller that brings the process to a safe state when limits are exceeded, engineered to a SIL (Safety Integrity Level 1-4, IEC 61511). *[OT/ICS Network Security; NIST OT and IoT Security]*

Site — Scheme + registrable domain (eTLD+1, e.g. example.co.uk), ignoring subdomains and port; used by SameSite cookies and Fetch Metadata. *[How the Web Works for Security People]*

site: / inurl: / intitle: — Restrict results to a domain, a URL substring (e.g. admin, login) or a page title - surfaces admin panels and exposed listings that were never meant to be indexed. *[Reconnaissance and OSINT]*

Site (same-site) — Scheme + registrable domain (eTLD+1 from the Public Suffix List): app.example.com and api.example.com are same-site but cross-origin. *[HTTP Security Headers and Browser Policies]*

Site survey — Physical recon: entry points, cameras, guard rotation, dumpsters, smoking areas. *[Vulnerability Discovery and Analysis]*

Skill (S) — The capacity to perform an observable action: "Skill in analyzing network traffic". Statement starts with **Skill in**. Rev. 1 merged the 2017 Ability statements into Skills. *[NICE Workforce Framework for Cybersecurity]*

SL (Security Level) — IEC 62443 level 0-4 of protection against an attacker of growing capability; SL-T target, SL-C capability, SL-A achieved. *[ANSSI ICS/SCADA Security]*

SL-T / SL-C / SL-A — Target security level required for a zone after risk assessment, Capability level a product or system can reach, Achieved level measured in operation. *[OT/ICS Network Security]*

SLA — Agreement between provider and customer defining service levels, measurement and remedies. *[CISA Domain 4: IS Operations and Business Resilience]*

SLA (service level agreement) — Contract terms that fix availability, support times and penalties for the provider. *[Cloud Computing Security]*

SLA / SLO — Service Level Agreement (contractual, with penalties) / Service Level Objective (internal target). **[CySA+ Practice Scenarios]**

SLAAC (Stateless Address Autoconfiguration) — The host builds its own address from the prefix announced in a Router Advertisement plus an IID it generates (RFC 4862); no server keeps a lease. **[IPv6 in Depth: Addressing, NDP, SLAAC, Security]**

Slack space — Unused bytes between the end of a file and the end of its last allocation unit (cluster); may hold residue of earlier files. **[Forensics by Data Type]**

SLAT — Second-level address translation (EPT/NPT): hardware-walked guest page tables, needed for fast virtualization. **[Windows Privacy GPOs and VBS Deployment; CPUs, Memory, Motherboards and Buses]**

SLAT (second level address translation) — Hardware GPA to HPA translation: Intel EPT (extended page tables), AMD NPT (nested page tables, marketed RVI). **[Virtualization Internals and VM Isolation]**

SLH-DSA (FIPS 205) — stateless hash-based signatures - backup family **[Cryptography Engineering and PQC]**

Slice — A descriptor (pointer, length, capacity) over a backing array; passed cheaply, grown with `append()`; the nil slice behaves like an empty one. **[Go Programming from Zero (Part 1: language basics)]**

SLM — Small language model: compact model that runs locally or at the edge, cheaper and more private than an LLM. **[SecAI+ Discriminators and Practice Scenarios]**

SLSA — Supply-chain Levels for Software Artifacts: framework for build integrity and provenance. **[CISSP Domain 8: Software Development Security]**

SLSA (Supply-chain Levels for Software Artifacts) — OpenSSF framework grading how trustworthy the build and its provenance (signed record of source, builder and inputs) are. **[Security Architecture - SDLC, IAM Design, Cloud]**

SLSA v1.0 (2023) — Supply-chain Levels for Software Artifacts, Build track: L0 none, L1 provenance exists, L2 signed provenance from a hosted build, L3 hardened build platform, non-falsifiable provenance. **[Secure Software Development: SSDF and SP 800-160]**

Smart contract — program stored on-chain and executed by every node; immutable unless built behind an upgradeable proxy **[Blockchain and Smart-Contract Security]**

Smart setpoint (consigne intelligente) — setpoint computed outside the ICS (statistics, AI, cloud) and sent back to a PLC, e.g. production line reconfiguration from predicted orders or energy optimisation from market forecasts. **[ANSSI IoT and IIoT Recommendations]**

SMB signing — Cryptographic signature on each SMB (Windows file sharing) message; when required, relayed authentication fails. **[Network and Infrastructure Assessment]**

SMM — System Management Mode: most privileged x86 firmware mode, invisible to the OS; SMRAM must be locked. **[OpenSSH Hardening and Hardware Security; UEFI, Secure Boot and Bootkits]**

Snap length (snaplen) — Bytes kept per packet (-s); 0 = whole packet, small values keep headers only for privacy and disk space. **[Packet Analysis in Practice and the N10-009 Exam Map]**

Snaplen — maximum bytes saved per packet; a short snaplen (-s 128) keeps headers only and shrinks files, but payload-based fields become empty. **[Wireshark and tshark for Troubleshooting and Analysis]**

Snapshot — An instant in time; data without an agreed timestamping mechanism has reduced value; recorded times can be tampered with and malicious latency can delay decision triggers. **[Networks of Things SP 800-183]**

Snapshot query — scheduled query that logs the full result set every time (`snapshot: true`), for inventories. **[osquery and Velociraptor for Fleet Visibility]**

SNi — Server Name Indication: the hostname a client sends in clear in the TLS ClientHello; lets defenders see the destination site of encrypted traffic (hidden only with Encrypted Client Hello, ECH). **[Network Traffic Analysis: Zeek and Suricata]**

SNi / ALPN — Server Name Indication (hostname the client wants) and Application-Layer Protocol Negotiation (e.g. h2 for HTTP/2), both ClientHello extensions. **[ANSSI TLS and IPsec Guides: Full R Index]**

SNi / ECH — Server Name Indication: the site name sent in clear in the TLS ClientHello; Encrypted Client Hello hides it. **[HTTPS Flow Inspection: Proxy and Reverse Proxy]**

SNMP / IPMI / BMC — Simple Network Management Protocol (device monitoring; v3 adds auth and encryption) / Intelligent Platform Management Interface on the Baseboard Management Controller (out-of-band server management: iLO, iDRAC). **[Networking Ports and Protocols]**

SNMP (Simple Network Management Protocol) — Manager polls agents on UDP 161 (Get, GetNext, GetBulk, Set); agents push traps and informs to UDP 162. **[Network Operations: Documentation, Monitoring, Resilience]**

SoA — Statement of Applicability: ISO 27001 list of every Annex A control, included or excluded with justification. **[EU Governance and Regulation: Self-Assessment]**

SOAR — Security Orchestration, Automation and Response: playbooks that act on alerts automatically. **[Security Operations Architecture; SIEM and Detection Engineering +2]**

SOAR (security orchestration, automation and response) — Workflow engine that runs playbooks (enrich, decide, contain, ticket) through the APIs of other security tools. **[Security Operations]**

SOC — Security Operations Centre: the team and tools that run security supervision. **[Security Supervision: ANSSI GP-112 and PG-113; SIEM and Detection Engineering]**

SOC 2 Type II — Independent auditor report on how a provider's controls operated over a period (typically 6-12 months). **[Cloud Outsourcing and Virtualization Lifecycle]**

SOC / MDR — Security Operations Centre (team watching alerts 24/7) / Managed Detection and Response (the same service bought from a provider). **[Ransomware: Anatomy, Detection, Prevention]**

Sociability test — Confirms the new system coexists with others in the target environment without harm. **[CISA Domain 3: IS Acquisition, Development and Implementation]**

Social engineering — fluent, personalised phishing, vishing (voice phishing) with voice clones **[AI-Assisted Security]**

Socket / 4-tuple — Source IP, source port, destination IP, destination port (plus protocol = 5-tuple): uniquely identifies one TCP connection or UDP flow. **[TCP and UDP Deep Dive]**

Solicited-node multicast — Group `ff02::1:ffXX:XXXX` derived from the last 24 bits of an address; NDP queries go there instead of a broadcast, so only 1-2 hosts process them. **[IPv6 in Depth: Addressing, NDP, SLAAC, Security]**

SOME/IP — Scalable service-Oriented MiddlewarE over IP: AUTOSAR service protocol on automotive Ethernet (service discovery, remote procedure calls); unauthenticated unless protected by SecOC, TLS/DTLS or MACsec. **[Automotive and Embedded Security]**

SOPS — Secrets OPerationS: encrypts values inside YAML/JSON files with age, PGP or cloud KMS keys, leaving

keys readable for review. **[GitOps and Continuous Delivery Security]**

Source — Where untrusted data enters: HTTP parameters, headers, message queues, files uploaded by users. **[Secure Code Review by Language; Static Analysis and Code Scanning in Practice]**

Source code escrow — A neutral third party holds the vendor's source code and releases it to the customer if the vendor fails or stops support. **[CISA Domain 3: IS Acquisition, Development and Implementation]**

Source de risque — who attacks: rated motivation, resources, activity **[EBIOS Risk Manager]**

Source map — File mapping minified JavaScript back to the original source; shipped to production it leaks code and comments. **[WSTG v4.2 - Complete Test Catalogue]**

Source of truth — The system (NetBox, Nautobot) from which configs are generated and pushed by automation (Ansible, Nornir); the device is never edited by hand. **[Network Operations: Documentation, Monitoring, Resilience]**

Source of truth (SoT) — Authoritative database of what the network should be (sites, devices, IPs, VLANs, circuits), e.g. NetBox or Nautobot; configurations are rendered from it, never edited by hand. **[Network Automation and Observability]**

SoW — Statement of work. Deliverables, timeline, cost, methodology. **[Engagement Management; Engagement Methodology and Reporting]**

SOW (Statement of Work) — This engagement's deliverables, timeline, price and acceptance criteria. **[Penetration Methodologies]**

SP 800-125A Rev. 1 (2018) — Security recommendations for hypervisor deployment on servers, grouped by five hypervisor baseline functions (HY-BF1 to HY-BF5, table below). **[Container and Virtualization Security]**

SP 800-125B (2016) — Secure virtual network configuration for VM protection: segmentation with VLANs/overlays, virtual firewalls, traffic monitoring of intra-host flows. **[Container and Virtualization Security]**

SP 800-193 beyond the BIOS — NIC, SSD, GPU, dock and BMC firmware are also persistence points (Equation group HDD firmware implants, 2015); inventory them with their versions, as PG-067 3.1.1 asks every supplier to declare. **[Platform Firmware, BMC, DMA and USB Attacks]**

SP 800-218A — Secure Software Development Framework (SSDF) community profile for generative AI and dual-use foun-

dation models: development-time practices (protect training data and weights, sign models, verify acquired models) mapped to AI RMF subcategories and OWASP LLM items. **[AI Compliance Frameworks]**

SP 800-61r3 (2025) — Recasts incident response around the NIST CSF 2.0 functions (Govern, Identify, Protect, Detect, Respond, Recover) instead of the four r2 phases; emphasises continuous improvement over a linear cycle. **[SANS Incident Handling]**

SP / RP / client — Service provider (SAML) / relying party (OIDC) / client (OAuth): the application consuming the identity. **[Identity Protocols: OAuth, OIDC, SAML, FIDO2]**

SP / SPD — Security Policy (per flow: bypass, discard or protect) collected in the Security Policy Database; acts like a firewall rule set. **[ANSSI TLS and IPsec Guides: Full R Index]**

SPA — Single-page application: JavaScript front end in the browser calling a back-end API. **[OWASP ASVS 5.0 - Application Security Verification Standard]**

SPA / DPA — Simple / differential power analysis: reading keys from one or many power-consumption traces of a device. **[CPU Side Channels and Memory Attacks]**

SPAN port — Switch port that receives a copy of traffic from other ports (port mirroring); may drop packets under load. **[Wireless Security and IDS/IPS]**

SPAN / TAP — Switch port mirroring (can drop under load) versus a passive hardware tap (copies everything, invisible to the network). **[Packet Analysis in Practice and the N10-009 Exam Map]**

SPAN vs TAP — A SPAN port mirrors traffic from a switch (can drop under load); a network TAP is a passive splitter that copies every bit. Use a TAP for reliable monitoring. **[Classic Enterprise Network Architecture]**

Spatial safety — Every access stays within the bounds of its object; violated by buffer overflows and out-of-bounds reads. **[Memory Safety and Fuzzing]**

SPD — Serial presence detect: EEPROM on each DIMM holding its JEDEC timings and XMP/EXPO profiles. **[CPUs, Memory, Motherboards and Buses]**

SPD (security policy database) — Kernel table saying, per traffic selector, whether a packet is protected by IPsec, bypassed in clear or discarded. **[VPN Planning, Design and Operations]**

Spear phishing vs whaling — Targeted mail to an individual vs targeted mail to an executive with signing authority. **[Social Engineering and Phishing Simulation]**

Special categories (Art. 9) — racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic, biometric (for identification), health, sex life or orientation; processing prohibited unless an Art. 9(2) exception applies. Criminal data: Art. 10 **[GDPR for Security Teams]**

SpEL — Spring Expression Language: evaluating user input with it (or eval()) is code injection. **[ASVS 5.0 - Chapter Highlights and 4.0.3 Delta]**

SPF — Sender Policy Framework: DNS record listing the servers allowed to send mail for a domain. **[CISSP Domain 4: Communication and Network Security; Social Engineering and Deepfakes +2]**

SPI flash — Serial flash chip on the motherboard holding the UEFI firmware, ME/PSP firmware and NVRAM variables. **[Platform Firmware, BMC, DMA and USB Attacks]**

SPIFFE ID — Workload identity URI carried in a certificate, e.g. spiffe://cluster.local/ns/shop/sa/api (namespace + service account). **[Kubernetes and Container Networking Explained]**

SPIFFE / SVID — vendor-neutral workload identity spiffe://trust-domain/path issued by SPIRE as short-lived X.509 or JWT SVIDs; a SPIRE server can expose OIDC discovery so clouds trust it like any IdP. **[Multi-Cloud Identity Federation]**

Spike / surge — Momentary / prolonged high voltage. **[CISSP Domain 3: Security Architecture and Engineering]**

Spine-leaf (Clos) fabric — A two-layer fabric where every leaf switch connects to every spine switch, so any two servers are at most two hops apart and bandwidth scales by adding spines. **[Data-Centre Architecture]**

Spine switch — The backbone. Connects only to leaves; adds bandwidth and paths when you add one. Never carries a directly-attached server. **[Data-Centre Architecture]**

SPL / KQL / EQL — query languages: Splunk Search Processing Language, Kusto Query Language (Microsoft Sentinel and Defender), Event Query Language (Elastic, for event sequences). **[SIEM and Detection Engineering]**

SPL (Search Processing Language) — Splunk pipeline language; starts with an implicit search over indexes, then | commands such as stats, eval, rex. **[Query Languages: KQL, SPL, EQL, ES|QL, osquery]**

Split / full tunnel — Split: only corporate prefixes enter the tunnel. Full: all traffic, including Internet browsing, goes through it and the corporate security stack. **[VPNs in Depth: IPsec/IKEv2, TLS VPN, WireGuard]**

Split horizon — Never advertise a route back out of the interface it was learned on; poison reverse advertises it back with an infinite metric instead. *[Routing I: Routing Table, Static Routes, OSPF]*

Split-horizon DNS — The same zone name serves different records to internal and external clients. *[ICMP, Path MTU, DHCP and DNS Operations]*

Split knowledge / dual control — Master key components held by n custodians (SP 800-57 Section 8); no single person can reconstruct the key. *[NIST Cryptographic Standards]*

Split tunnel — VPN mode where only corporate prefixes go through the tunnel and Internet traffic leaves directly from the device. *[Operations, Security, Troubleshooting: Self-Assessment]*

Split tunnelling — Only traffic for the entity goes into the VPN, the rest goes straight to the local network or Internet; full tunnelling sends everything into the VPN. *[Remote Work (Digital Nomadism)]*

SPN — Service Principal Name: registers a service on an account; any user can ask a ticket for it. *[SecurityX Practice Scenarios; Windows and Active Directory for Defenders +1]*

SPN (service principal name) — Name binding a Kerberos service (e.g. MSSQLSvc/db01) to the account whose key encrypts its tickets. *[Active Directory Security; Active Directory Tiering and Kerberos in Depth]*

Spoofing → authentication — zero trust access, mTLS, FIDO2 *[Secure Architecture Patterns]*

Spyware — Covertly collects browsing, credentials, screenshots; often bundled with free software; stalkerware on phones. *[Malware, Attacks and Indicators]*

SQLi — SQL injection: input changes the structure of a database query. *[Web Application Assessment]*

SR-IOV — Single-root I/O virtualization: a physical function (PF) spawns virtual functions (VFs), each a PCIe function with its own queues. *[Virtualization Internals and VM Isolation]*

SRG — Security Requirements Guide: technology-class requirements (operating system, application server, network device) from which product STIGs are derived. *[DISA STIG Viewer 3 and STIG Checklists]*

SRI in practice (R11, R12) — integrity="sha384-..." on scripts and stylesheets, internal and third-party; with crossorigin="anonymous" (R43) so no credentials leak. *[Browser-Side Web Security Standards]*

SRI (Subresource Integrity) — Hash in a script or link tag; the browser refuses the file if its content differs. *[Browser-Side Web Security Standards]*

SSDF task id — The Secure Software Development Framework (SP 800-218, version 1.1) groups practices as **PO** Prepare the Organization, **PS** Protect the Software, **PW** Produce Well-Secured Software, **RV** Respond to Vulnerabilities. PS.1.3 = group PS, practice 1, task 3. SP 800-218A adds AI items per task: PS.1.3.R4 is its... *[GenAI Secure Development and Content Transparency]*

SSE — Security Service Edge: the security half of SASE (SWG + CASB + ZTNA), without the WAN part. *[CompTIA CySA+ CS0-003; Security Operations Architecture]*

SSE-C — S3 server-side encryption with a customer-provided key sent in each request; AWS does not keep the key. *[Cloud and DevSecOps: Self-Assessment]*

SSH certificate — Public key signed by an SSH CA with principals and a validity period; servers trust the CA instead of every user key. *[OpenSSH Hardening and Hardware Security]*

SSH / RDP / VNC — Secure Shell (encrypted remote terminal and file copy) / Remote Desktop Protocol (Windows graphical session) / Virtual Network Computing (cross-platform screen sharing). *[Networking Ports and Protocols]*

SSI injection — Server-Side Includes: <!--#exec ... --> directives in input executed by the web server. *[OWASP Web Security Testing Guide v4.2]*

SSID / BSSID — SSID: the network name users see; BSSID: the MAC address of one AP radio broadcasting it. *[Wireless Security and IDS/IPS]*

SSID / BSSID / ESS — SSID = network name; BSSID = MAC of one AP radio serving it; ESS (Extended Service Set) = all APs sharing one SSID so clients roam between them. *[Wireless, Data-Center Fabrics and Cloud Networking]*

SSO — One authentication gives access to many systems; single point of failure and of compromise, so MFA is required. *[CISA Domain 5: Protection of Information Assets]*

SSO / federation — Single Sign-On: one login gives access to many apps; federation = trusting identities asserted by another organisation's IdP. *[Identity Protocols: OAuth, OIDC, SAML, FIDO2]*

SSO (single sign-on) — One authentication gives access to many systems in one trust domain; larger blast radius if the credential leaks. *[CISSP Domain 5: Identity and Access Management]*

SSP (System Security Plan) — Document describing the system boundary and how each selected control is implemented, with all ODP values (control PL-2). *[NIST SP 800-53r5 Controls in Practice; Risk Management Framework (RMF)]*

SSPM (SaaS Security Posture Management) — Tool that connects by API to SaaS tenants (M365, Google Workspace, Salesforce, Slack, GitHub...) and continuously checks settings, users, OAuth grants and sharing against a baseline. *[SaaS Security and Google Workspace]*

SSRF — Server-Side Request Forgery: the server is made to send a request to a URL chosen by the attacker. *[Famous Vulnerabilities Explained; Web Application Assessment +1]*

SSRF / CSRF — Server-Side Request Forgery makes the server fetch an attacker-chosen URL; Cross-Site Request Forgery makes a victim's browser send an authenticated action. Fixes: egress allow-lists vs anti-CSRF tokens + SameSite cookies. *[Host and Web Application Attacks]*

SSRF / IMDS — Server-Side Request Forgery (making a server fetch a URL of the attacker's choice) / Instance Metadata Service at 169.254.169.254 that hands cloud credentials to the VM; IMDSv2 requires a session token. *[IP Addressing, ICMP, DHCP and Network Triage]*

SSRM ownership types (CCM v4) — for each control, who implements it: CSP-owned (cloud service provider), CSC-owned (cloud service customer), third-party outsourced, shared-independent (each side does its own part), shared-dependent (the customer part relies on the provider part). Both parties fill it per control. *[CSA Cloud Controls Matrix and Guidance]*

SSTI — Server-side template injection: input is evaluated by the template engine, often leading to code execution. *[Web Application Assessment]*

SSTI / LFI / RFI — Server-Side Template Injection executes template syntax; Local/Remote File Inclusion loads a local or remote file into execution. Fixes: no user-controlled templates; disable remote include; canonicalize paths. *[Host and Web Application Attacks]*

SSV (Signed System Volume) — since macOS 11 Big Sur the system volume is a read-only APFS snapshot sealed by a hash tree; any modified byte breaks the seal and the Mac refuses to boot it in Full Security. *[macOS Security for Defenders]*

SSVC — **SSVC** (Stakeholder-Specific Vulnerability Categorization) - CISA's decision tree replacing CVSS-only triage: Exploitation (none / proof of concept / active), Technical impact (partial / total), Automatable (can an attacker exploit it at scale without human steps: yes / no), Mission prevalence and

Public well-being. . . *[Vulnerability Tools, CVSS and Prioritization; Vulnerability Management Programme +1]*

SSVC and KEV — Stakeholder-Specific Vulnerability Categorization - decision tree (exploitation, automatable, technical impact, mission prevalence) → Track, Track*, Attend, Act; CISA KEV (Known Exploited Vulnerabilities) catalog = exploited in the wild, US federal agencies must fix by the listed due date (Binding Operational. . . *[Security Operations]*

SSVC (CISA, 2022) — Stakeholder-Specific Vulnerability Categorization: decision tree over exploitation status, automatable (can attackers script it), technical impact, mission and well-being impact; outcomes Track (routine), Track* (routine, watch closely), Attend (faster, supervisors informed), Act (immediately, leadership involved). *[Vulnerability Management and Security Testing]*

Stack buffer overflow — write past a stack array, overwriting the return address; mitigated by stack canaries (C rule R43), PIE address randomisation (R45) and a non-executable stack (R42). *[Secure Coding in C and Rust, CMS and JRE Hardening]*

STAD — Système de traitement automatisé de données (automated data processing system): the French legal term for any computer system protected by Code pénal articles 323-1 and following. *[Law and Ethics for Security Practitioners]*

Stage gate — Formal review point at which the steering committee decides to continue, change or stop a project. *[CISA Domain 3: IS Acquisition, Development and Implementation]*

Stakeholder alignment — Agreeing goals, success criteria and communication cadence with every party (sponsor, IT, SOC, legal) before and during the test. *[Engagement Management]*

Standing privilege — Privileged access that is active all the time, whether or not it is being used; the opposite of just-in-time access. *[Cloud Entitlement Management and Least Privilege]*

STAR — Security, Trust, Assurance and Risk registry: public listing of provider assessments. Level 1 = self-assessment (CAIQ); Level 2 = third-party audit (STAR Certification on top of ISO/IEC 27001, STAR Attestation on top of SOC 2). *[CCSP and CCSK: Cloud Security Certifications]*

STAR method — structure for behavioural answers: Situation, Task, Action, Result; the Action part (what *you* did) should take most of the time *[CV, Portfolio and Job Interviews in Security]*

STARTTLS — command that upgrades a cleartext connection to TLS on the same port; see implicit vs explicit TLS below. *[Networking Ports and Protocols]*

STARWatch — CSA SaaS tool to manage CCM/CAIQ assessments and mappings. *[CSA Cloud Controls Matrix and Guidance]*

State exhaustion — Floods that fill connection tables of firewalls, load balancers and IDS: the in-line security box is often the first to fall. *[DDoS: Protection Options, Response, Non-Participation]*

state / nonce — Random values: *state* ties the callback to the browser session (anti-CSRF), *nonce* ties the ID Token to the request (anti-replay). *[ANSSI Identity: MFA, AD Tiering, OpenID Connect]*

State-sponsored actor — Group working for a government, typically running long APT (advanced persistent threat) campaigns. *[CEH v13: Exam Blueprint and Module Map]*

Stateful return — Reply packets are accepted by the connection table; writing a second rule in the reverse direction opens an unsolicited path. *[Firewall Policy: Design, Cleanup, Exposed Zone]*

Statement of Applicability (SoA) — Clause 6.1.3(d) document listing every Annex A control as included or excluded, with justification and implementation status. *[ISO/IEC 27001:2022 and 27002:2022]*

Statement of volatility — Vendor document listing which components of a device retain data after power-off; also used for media sanitization (SP 800-88). *[Digital Forensics in Incident Response]*

Static analysis — examining a file without running it: hashes, file type, strings, imports, embedded macros. *[Malware Triage and Analysis]*

Static pod — Pod defined by a file in `/etc/kubernetes/manifests`, run by the kubelet without scheduler or API; kubeadm runs the control plane this way (the API shows a read-only mirror pod). *[Kubernetes Architecture in Depth]*

Static vs dynamic analysis — static inspects formats and content (hidden elements, exploit code); dynamic replays files or sessions in a supervised sandbox. *[OT Detection Doctrine, Integrators and Training]*

Station blanche / White station — Workstation or server isolated from the operational network, dedicated to anti-malware analysis of removable media and their data. Gives

reasonable assurance of harmlessness. *[Removable Media Airlock and White Station]*

Statistical learning — Regression, Bayesian and decision-tree methods with explicit assumptions; explainable, cheap, still the backbone of spam and fraud scoring. *[AI Fundamentals for Cybersecurity]*

Status / Sub Status — NTSTATUS hexadecimal codes in failure events (4625, 4776) giving the exact reason: wrong password, unknown user, locked, disabled. *[Windows Audit Policy and Event ID Reference]*

Stem — The scenario and question text of a multiple-choice item. *[CISA Practice Scenarios]*

Sticky — Learned MACs are written as `mac-address sticky H.H.H` into the running-config; `write memory` makes them survive reload. *[First-Hop Security and Gateway Redundancy]*

STIG — Security Technical Implementation Guide: DISA configuration standard for one product (e.g. Windows Server 2022, RHEL 9), each rule with discussion, check and fix text; mandatory for DoD systems, free at public.cyber.mil. *[SANS Incident Handling; DISA STIG Viewer 3 and STIG Checklists]*

STIX 2.1 — Structured Threat Information Expression: OASIS JSON format for intel objects (indicator, malware, threat-actor, attack-pattern, relationship). *[Malware Triage and Analysis; Threat Intelligence, Hunting and SOC Efficiency]*

STIX / TAXII / TLP — Threat-intel data format / its HTTPS transport / Traffic Light Protocol sharing labels (RED, AMBER, GREEN, CLEAR). *[SecurityX Practice Scenarios]*

Stop-or-go sampling — Attribute variant that stops early when few or no errors appear, avoiding oversampling. *[CISA Domain 1: Information System Auditing Process]*

Storage limitation — Art. 5(1)(e): identifiable no longer than necessary (retention schedules) *[GDPR for Security Teams]*

STP / BPDU — Spanning Tree Protocol breaks layer-2 loops; switches exchange Bridge Protocol Data Units to elect a root. *[OT Switch and Firewall Hardening: Hirschmann, SCALANCE]*

STP (Spanning Tree Protocol) — IEEE 802.1D protocol that blocks redundant switch links so the L2 topology is a loop-free tree; Ethernet frames have no TTL, so a loop circulates broadcasts forever (broadcast storm). *[Switching: VLANs, Trunks, Spanning Tree, EtherChannel]*

Strategic alignment — Security objectives derived from, and traceable to, business objectives. *[CISM Domain 1: Information Security Governance]*

Strategic scenario — path from a risk origin to its target objective through business values and possibly an ecosystem stakeholder, rated in severity. *[EBIOS Risk Manager]*

Stratified sampling — Divide the population into homogeneous strata and sample each; reduces sample size for a given precision. *[CISA Domain 1: Information System Auditing Process]*

Stream (stdin/stdout/stderr) — the three default channels every program has: standard input (data in), standard output (results out), standard error (messages/errors out). Pipes connect one program's stdout to the next program's stdin. *[Text Processing and Data Toolkit Reference]*

Strict KEX — OpenSSH 9.6 countermeasure to Terrapin: sequence numbers reset after each NEWKEYS and any unexpected message during key exchange aborts the connection; both sides must support it. *[SSH in Depth]*

String ops — parse and filter output *[Enumeration and Scripting]*

Strip 2G — disable legacy fallback on managed devices *[Telecom and 5G Security]*

Strong authentication — Authentication relying on cryptographic mechanisms conforming to RGS annexes B1-B3 (PG-078 R2), e.g. a smart card or FIDO2 key signing a challenge. *[ANSSI Identity: MFA, AD Tiering, OpenID Connect]*

Strong authentication (authentification forte) - R2 — Authentication relying on a **cryptographic protocol** (a challenge signed or MACed with a secret key) resistant to eavesdropping, replay and man-in-the-middle. R2 asks for mechanisms conform to the **RGS** (Referentiel General de Securite, the French government security framework) and its annexes **B1** (approved...). *[Authentication, MFA and Passwords]*

Strong unforgeability — No new valid signature even on an already-signed message. ECDSA lacks it: Bitcoin double-spend (transaction malleability) and incompatibility with SSH, which requires it. *[ANSSI Crypto Rules Catalogue (PG-083 v3.00)]*

StrongBox — Android Keystore backend hosted in a discrete secure element instead of the TEE. *[Laptops, Mobile Devices, Virtualization Hardware]*

Structured and comprehensive — consistent, comparable results *[CRISC Domain 1: Governance]*

Stub / recursive / authoritative — the client's minimal resolver / the server that walks the hierarchy and caches answers / the server that holds the zone and answers for it. *[DNS Security in Practice]*

sub claim (GitHub) — Token subject: repo:ORG/REPO:ref:refs/heads/main, ...:environment:prod, ...:pull_request or ...:ref:refs/tags/v1; the key field of every trust rule. *[CI/CD Pipeline Security]*

Sub-interface — Logical interface on a physical router port (Gi0/0/0.10) bound to one 802.1Q VLAN id; the gateway of that VLAN in router-on-a-stick. *[Cisco IOS Configuration Lab]*

Subcategory — Specific technical or management outcome (PR.AA-03 = users, services and hardware are authenticated). Identifier = Function.Category-NN. *[Windows Audit Policy and Event ID Reference; NIST Cybersecurity Framework 2.0]*

Subdomain takeover — DNS record still points to a deleted cloud or SaaS resource that anyone can re-register. *[DNS Security in Practice; OWASP Web Security Testing Guide v4.2]*

Subject — Active entity (user, process, service) that requests access to an object. *[Zero-Trust Architecture; CISSP Domain 5: Identity and Access Management +1]*

Subject access control (3.1) — Subjects are users, processes, devices and services - each needs its own identity; service accounts get a gMSA (group managed service account, auto-rotated password) or cloud workload identity, not shared passwords. *[Security Engineering - IAM, Endpoints, Network, Hardware, OT, Automation]*

Subject Alternative Name (SAN) — The names a certificate is valid for; browsers ignore the CN. Wildcard *.example.com covers one label only. *[TLS and Certificates in Practice]*

Subprocessor — GDPR (General Data Protection Regulation) term: a processor engaged by your processor to process personal data you control *[Third-Party Risk Management (TPRM)]*

Subscriber / applicant / claimant — Applicant = person being proofed; subscriber = enrolled account holder; claimant = someone trying to authenticate as a subscriber. *[Digital Identity Guidelines SP 800-63-4]*

Subsequent system impact — 4.0 splits impact between the vulnerable component and downstream systems (replaces 3.1 Scope). *[Report Templates and Severity Rating]*

SUC — System Under Consideration: the perimeter of the risk assessment, decomposed into zones and conduits (62443-3-2). *[ANSSI ICS/SCADA Security]*

Successor — Next hop of the best path, installed in the routing table. *[Routing II: EIGRP, BGP at the Enterprise Edge, Redistribution]*

SUCI — Subscription Concealed Identifier: the SUPI encrypted by the SIM with the home network's public key (ECIES) so it never crosses the radio in clear. *[Telecom and 5G Security]*

Sufficient evidence — conclusions only on reliable, relevant, sufficient evidence *[CISA Exam Strategy]*

SUID / SGID / sticky bit — special mode bits: run a program with the file owner's (SUID) or group's (SGID) rights; sticky on a directory = only a file's owner may delete it. *[Linux Security Command Line]*

Summary black hole — The summarizing router installs a route to Null0 (a discard interface); if one component subnet fails, traffic is dropped there instead of looping. Intentional, but hides partial outages from upstream. *[IPv4 Addressing, Subnetting, VLSM and NAT]*

Super-timeline — one chronological table merging file-system, registry, event log, browser and other artefacts (built by plaso / log2timeline). *[DFIR Artifacts and Tools]*

Supervised / fully managed — Company-owned enrolment mode (iOS supervision, Android Enterprise fully managed) giving the MDM the widest control. *[Mobile Device Security and MDM]*

Supervision strategy — internal document of the supervision team linking security objectives (from governance, PSSI), data families and collection points, and detection rules; also means, architecture, governance and outsourcing level per process. Revised often at first, then yearly. Not the same as a provider's service agreement. *[Security Supervision: ANSSI GP-112 and PG-113]*

Supplementary groups — Extra groups a process belongs to, read from /etc/group at login; any of them can match a file's group. *[Linux Users, Groups, Permissions and ACLs]*

Suppliant — Software on the device (built into the OS) that answers the 802.1X authentication. *[BGP, 802.1X & VPN]*

Supply chain attack — Compromising a supplier (software vendor, service provider, open source library) to reach its customers through a trusted channel. *[Landmark Incidents and Lessons]*

Support domain (domaine support) — VM or sandbox hosting a base function: VMM per user domain, CRYPTO (vTPM), JOURNALISATION, ADMIN, AUDIT, MISE_A_JOUR, file-analysis domain per diode. *[Multi-Environment Workstation and Refurbishing]*

Support period — CRA Art. 13(8): time during which the manufacturer must handle vulnerabilities and ship free security

updates, normally at least 5 years. *[Cyber Resilience Act and AI Act]*

Supporting asset (bien support) — component the business value relies on: hardware, software, network, people, premises, organisation *[EBIOS Risk Manager]*

Suricata / Snort — Signature IDS/IPS. Rules like the classic 'sfPortscan' or ET SCAN signatures alert on many connections from one source in a window. *[Network Scanning and Enumeration Reference (Authorized Labs)]*

SVI — Switched Virtual Interface: routed interface of a VLAN inside a multilayer switch (interface Vlan10). *[Cisco IOS Configuration Lab]*

SVI (Switched Virtual Interface) — interface vlan N, the L3 gateway of a VLAN on a multilayer switch. Up/up only if the VLAN exists, at least one port in that VLAN is up and STP-forwarding (or a trunk carries it), and the SVI is not shut. *[Switching: VLANs, Trunks, Spanning Tree, EtherChannel]*

sVirt — libvirt feature that confines each VM's QEMU process with a unique SELinux MCS label or AppArmor profile. *[Virtualization Internals and VM Isolation]*

SVP — Shortest Vector Problem in a lattice; ANSSI sizes lattice schemes by the dimension of the equivalent SVP instance. *[ANSSI Cryptographic Mechanisms and PQC]*

SWG — Secure Web Gateway: cloud or on-prem proxy that filters users' web traffic (URL categories, malware). *[CompTIA CySA+ CS0-003]*

switch_root — Replaces the initramfs root with the real root filesystem and executes the real init, freeing the RAM filesystem. *[Linux Boot, Processes and System Calls]*

Switching — Data Act Art. 2(34): moving from one cloud or edge provider to another (or on-premises) with exportable data and digital assets. *[Data Act, Data Governance Act and EHDS]*

Symbol table (ISF) — Intermediate Symbol Format JSON describing kernel structure layouts for one exact OS build; Volatility 3 downloads Windows ones from Microsoft PDB servers and needs them built for Linux and macOS. *[Memory Forensics with Volatility 3]*

Symmetric vs asymmetric — Symmetric: fast, bulk data, key distribution problem (AES, ChaCha20); asymmetric: key exchange, signatures, slow, PKI needed (RSA, ECC, ML-KEM/ML-DSA). Real systems combine both (TLS). *[Cryptography Engineering and PQC]*

SYN — Synchronize sequence numbers: opens a connection *[TCP and UDP Deep Dive]*

SYN scan (-sS) — Half-open probe; sends SYN, reads the reply, never completes the handshake. Fast, needs root. *[Reconnaissance and OSINT]*

Synced passkey — Private key backed up end-to-end encrypted to the provider's cloud and usable on all the user's devices; the key is exportable by design. *[Passkeys and Passwordless Authentication]*

SYNOPSIS — the usage line at the top of a man page or --help output, written in a small notation: [] optional, ... repeatable, | alternatives. *[Master Any Command-Line Program Fast, on Every OS]*

Synthetic data — Artificially generated records that mimic the statistics of real data (GAN, LLM or simulation). Used for augmentation, balancing rare classes and privacy (no real PII). Risk: model collapse when models train repeatedly on their own outputs, and hidden bias copied from the generator. *[AI Data Security and Lifecycle]*

sysdiagnose — Apple diagnostic bundle (logs, process list, shutdown.log, crash reports, network state) generated on demand on macOS and iOS; the main iPhone evidence source for defenders. *[macOS and iOS Forensics for Defenders]*

Sysmon — free Microsoft Sysinternals driver that writes detailed process, network and file events to the Windows event log (event 1 = process created, 10 = process accessed another process). *[SIEM and Detection Engineering]*

System call (syscall) — The controlled doorway from user space into the kernel, for example open, read, write, fork, execve on Linux or NtCreateFile on Windows. *[Operating System Concepts for Beginners]*

System for — RFC 7643/7644 - REST + JSON *[Security Architecture - SDLC, IAM Design, Cloud]*

System owner — Owns the system that processes data; ensures it meets security requirements (system security plan). *[CISSP Domain 2: Asset Security]*

System prompt — Hidden instructions the application sends before the user's message to set role, rules and tools. *[OWASP Top 10 for LLM Applications 2025]*

System test — Tests the whole system against functional and non-functional requirements (performance, security, recovery). *[CISA Domain 3: IS Acquisition, Development and Implementation]*

T

TA numbers — Proofpoint names criminal groups 'Threat Actor' plus a number (TA542 = Emotet operators, TA569 = SocGholish); other vendors use other names for the same groups. *[Industry and Workforce Reports]*

Tabletop exercise (TTX) — discussion-based exercise where decision-makers talk through a scenario delivered as injects, without touching real systems *[Crisis Communication and Tabletop Exercises]*

Tag — mutable pointer to a manifest; latest or 1.2 can be repointed by anyone with push rights. Deploy by **digest**, or enforce immutable tags in the registry. *[Container Image and Registry Security]*

Tail sampling — Keeping or dropping a whole trace after it completes, based on errors, latency or attributes; requires all spans of a trace on one collector. *[Observability and Security Telemetry Pipelines]*

Tailgating — Follow an authorized person through a controlled door. Tests whether staff challenge strangers. *[Vulnerability Discovery and Analysis]*

Tailgating / piggybacking — Following an authorized person through a door; piggybacking implies they consent. *[Social Engineering and Phishing Simulation]*

Taint analysis — Tracking data from sources to sinks through the code; what CodeQL, Semgrep Pro and Psalm do automatically. *[Secure Code Review by Language]*

Taint tracking — Data-flow analysis that follows values from sources through assignments and calls to sinks, stopping at sanitizers. *[Static Analysis and Code Scanning in Practice]*

Take-Grant — Directed graph with take, grant, create and remove rules to track how rights propagate. *[CISSP Domain 3: Security Architecture and Engineering]*

Tamper detection and countermeasures — Chassis intrusion switches, epoxy potting, mesh sensors that zeroise (erase) keys when drilled (FIPS 140-3 level 4 HSM), tamper-evident seals, EMI (electromagnetic interference) shielding and EMP (electromagnetic pulse) protection (Faraday cage, surge protection) for critical sites. *[Security Engineering - IAM, Endpoints, Network, Hardware, OT, Automation]*

Tampering → **integrity** — signed artefacts, immutable infra, WAF, input validation *[Secure Architecture Patterns]*

TAP / SPAN — Network test access point (hardware copy of every packet) vs switch port mirroring (SPAN, may drop packets

under load); both feed passive sensors. *[Security Architecture - Resilience, Controls, Zero Trust]*

TAP (test access point) — Passive hardware device that copies every packet on a link; no loss, no impact if the sensor fails. *[Wireless Security and IDS/IPS]*

TAP vs SPAN — A network TAP copies traffic passively at line rate; a SPAN/mirror port on a switch can drop frames under load. Prefer TAPs on high-value links. *[IoT/IloT Security and OT Detection; Network Traffic Analysis: Zeek and Suricata]*

Target of Evaluation — The system or product being assessed (TOE). *[CEH v13: Core Concepts, Phases and Legal Framework]*

Target value and tolerance range — value to approach, e.g. monthly antivirus update; once reached, a tolerance range triggers alerts on drift *[SSI Maturity and Security Dashboards]*

Targeted policy — Default SELinux policy: network daemons run in confined domains (httpd_t, sshd_t), user shells run unconfined (unconfined_t). *[Linux Hardening in Practice]*

Targeted risk analysis (TRA, 12.3.1) — Written analysis the entity performs wherever a requirement says 'periodically' or 'at the frequency defined in the entity's TRA' (the list is in the cadence table below); each TRA reviewed at least every 12 months. *[PCI DSS v4.0.1 Requirement by Requirement]*

Task / domain — a task is the logical entity being confined; its domain is the set of software and hardware resources it can act on. A resource outside the domain is out of reach. *[System Partitioning: ANSSI PG-040]*

Task (T) — An activity directed toward achieving organizational objectives: "Identify anomalous network activity". What the work is. *[NICE Workforce Framework for Cybersecurity]*

TAXII 2.1 — Trusted Automated eXchange of Intelligence Information: HTTPS API that serves STIX objects in collections (MISP, OpenCTI, vendor feeds). *[Malware Triage and Analysis; Threat Intelligence, Hunting and SOC Efficiency]*

TCB — Trusted computing base: all protection mechanisms that enforce policy; its boundary is the security perimeter. *[CISSP Domain 3: Security Architecture and Engineering]*

TCB recovery — vendor process after a TEE vulnerability: new microcode/firmware raises the security version number (SVN) and verifiers start rejecting reports with the old one *[Confidential Computing and Remote Attestation]*

TCB (trusted computing base) — All code whose compromise breaks isolation; smaller is safer. *[Multi-Environment Work-

station and Refurbishing; Virtualization Internals and VM Isolation +1]*

TCC.db — SQLite database of Transparency, Consent and Control decisions: which app got Full Disk Access, camera, screen recording, and when. *[macOS and iOS Forensics for Defenders]*

TCC (Transparency, Consent, and Control) — framework that asks the user before an app reaches protected resources (camera, microphone, Desktop and Documents folders, Full Disk Access, Accessibility, Screen Recording, Input Monitoring) and records the answer in TCC.db. *[macOS Security for Defenders]*

TCN — Topology Change Notification: makes switches flush their MAC tables; a flood of TCNs causes traffic storms. *[OT Switch and Firewall Hardening: Hirschmann, SCALANCE]*

TCP/IP model — Four layers: application (OSI 5-7), transport, internet, network access (link, OSI 1-2). *[CISSP Domain 4: Communication and Network Security]*

tcp.stream — index Wireshark gives each TCP connection (0, 1, 2...); tcp.stream == 7 isolates one conversation exactly, unlike an address and port filter. *[Wireshark and tshark for Troubleshooting and Analysis]*

TCP three-way handshake — SYN, SYN-ACK, ACK; connection-oriented, reliable, ordered. UDP is connectionless and best effort. *[CISSP Domain 4: Communication and Network Security]*

TDBSSI — Tableaux de bord de la SSI: DCSSI method (2004) to build security dashboards, i.e. sets of indicators that tell each audience (management, steering, operations) whether security objectives are met. Section 1 is the methodology; section 2 a worked example; section 3 blank templates. *[SSI Maturity and Security Dashboards]*

TDE (Transparent Data Encryption) — Engine-level encryption of data and log files at rest, invisible to applications; protects files and backups, not live queries. *[Database Security]*

TDM — Time-division multiplexing: classic digital phone lines (ISDN T0 basic, T2 primary) that are not IP, giving a protocol break with the operator. *[ToIP and Virtualization Security]*

TDP / PL1 / PL2 — Thermal design power sizes the cooler; Intel PL1 = sustained, PL2 = turbo burst. Undersized cooler = thermal throttling at Tjmax (maximum junction temperature of the die, ~95-105 C): the CPU lowers its clock to protect itself. *[CPUs, Memory, Motherboards and Buses]*

Team — A set of Work Roles or Competency Areas assembled for a mission; Section 3.5 shows how to build teams from either. *[NICE Workforce Framework for Cybersecurity]*

Team ID — Ten-character identifier of an Apple developer account; prefixes App IDs and Keychain groups and limits sharing to one developer. *[iOS Application Internals and Security]*

Technical control vs security function — One product can host several controls: an NGFW (next-generation firewall) filters (preventive), logs (detective) and blocks C2 (command-and-control) traffic after a match (corrective). Classify the *function* the scenario describes. *[Security Controls]*

Technical debt — Future cost of quick, undocumented or outdated automation that someone must later fix or replace. *[CRISC Domain 4: Information Technology and Security; Incident Response, Forensics, Automation]*

Technique data items — Id, tactic(s), platforms, permissions required, data sources, detection, mitigations, procedure examples, CAPEC ids, contributors, version. Every technique must be backed by public reporting or MITRE research, never theory. *[MITRE ATT&CK]*

TEE — Hardware-isolated enclave protecting data in use (Intel SGX/TDX, AMD SEV-SNP, Arm TrustZone). *[CISSP Domain 3: Security Architecture and Engineering; Laptops, Mobile Devices, Virtualization Hardware]*

TEE (Trusted Execution Environment) — hardware-isolated execution context whose memory is encrypted and integrity-protected by the CPU against all other software, including the hypervisor *[Confidential Computing and Remote Attestation]*

Teleassistance — Remote help on a user's workstation, in the user's session and with the user watching; distinct from tele-administration, done with a dedicated privileged account. *[Start-ups, Municipalities, Teleassistance, Open Source]*

Telemetry pipeline (observability pipeline) — Broker/router between sources and the SIEM that filters, reduces, reshapes, enriches and tees data to more than one destination (Cribl Stream, Logstash, Vector, Kafka). *[Security Operations Architecture]*

Telemetry source — Any system that emits security-relevant records: OS audit logs, EDR events, network flows, application and cloud audit trails, identity provider logs. *[Security Operations Architecture]*

Teleservice (teleservice) — Any IS letting users complete administrative formalities online: school or canteen enrolment, water bill payment, public procurement platform, social bene-

fit request, transmission to the prefecture (controle de legalite).
[Local Authorities: the Regulatory Security Framework]

TEMPEST — NATO/US name for protection against compromising electromagnetic emanations of IT equipment. *[CPU Side Channels and Memory Attacks]*

Template — A Kubernetes manifest with Go-template placeholders (`{{ .Values.x }}`) filled in at render time. *[Helm, operators and the CRD ecosystem (with security)]*

Temporal metrics — Exploit Code Maturity (E), Remediation Level (RL), Report Confidence (RC) - lower the score as patches and doubts appear. *[Vulnerability Tools, CVSS and Prioritisation]*

Temporal safety — An object is only used while alive; violated by use-after-free, double free and returning pointers to stack variables. *[Memory Safety and Fuzzing]*

Temporary pass (laissez-passer temporaire) — One-time recovery ticket limited in days and number of uses (P842). *[ANSSI Encryption Tools: Zed! and Cryhod (2/2, Cryhod)]*

Terraform state — JSON file mapping code to real resources, including their attributes and often secrets; whoever reads it reads those secrets. *[Infrastructure as Code and Secrets]*

Test — Exercise the mechanism under specified conditions and compare actual with expected behaviour; the strongest evidence. *[SP 800-53r5 Key Controls Explained; IR Exercises and Threat Information Sharing]*

Test the theory — confirmed: next step; not: new theory or escalate *[Hardware: Self-Assessment]*

Tête de lecture (reader) — Badge reader at the door, on the uncontrolled side; ideally 'transparent' (passes data, holds no secrets). *[Physical Access Control and CCTV (ANSSI PA-72)]*

TEVV — test, evaluation, verification and validation; performed throughout the lifecycle, with independent (third-party) assessors where impacts are high (MEASURE 1.3). *[AI Risk Management Framework]*

TGT / TGS — Kerberos ticket-granting ticket (proves who you are, from the KDC) / service ticket (grants one service, encrypted with that service account's key). *[Identity and Active Directory Assessment]*

Theory of probable cause — question the obvious, research *[Hardware: Self-Assessment]*

Third party — any external entity you have a business relationship with: supplier, SaaS, outsourcer, consultant, partner *[Third-Party Risk Management (TPRM)]*

Third-party audit — Audit of a vendor or of the organisation on behalf of another party (customer, regulator). *[CISSP Domain 6: Security Assessment and Testing]*

Third-party authorization — Written consent from hosting or SaaS provider when their assets are touched. *[Engagement Methodology and Reporting]*

Thread — the unit the scheduler runs: own stack and registers, belongs to one process; can temporarily carry an impersonation token to act as a client. *[Windows Internals for Defenders]*

Threat — A potential event or actor that can cause harm to an asset. *[CEH v13: Core Concepts, Phases and Legal Framework; CISM Domain 2: Information Security Risk Management +3]*

Threat actor — A person or group that carries out intrusions, described by sponsor, motive, targets and a repeatable way of operating. Defenders profile actors to decide which techniques to detect first, not to name and shame. *[Threat Actor Profiles; Threat Actors and Threat Vectors]*

Threat community — group of threat agents sharing capability and motive: cybercriminals, insiders, nation-states, hacktivists; TEF and TCap are estimated per community *[Risk Quantification and Cyber Insurance]*

Threat hunting — Proactive, human-led search for attackers already inside the environment that automated detections missed, starting from a hypothesis rather than from an alert. *[Threat Hunting Playbooks]*

Threat intelligence — Evidence-based knowledge about adversaries (strategic, tactical, operational, technical) used to anticipate and detect attacks. *[CEH v13: Core Concepts, Phases and Legal Framework]*

Threat landscape — Current set of threat actors, techniques and trends relevant to the enterprise, fed by threat intelligence. *[CRISC Domain 2: IT Risk Assessment]*

Threat modeling — Structured analysis of a system's design to find what can go wrong (threats), decide which matter (risk) and choose controls before or while building it. *[CEH v13: Core Concepts, Phases and Legal Framework; Compliance, Threat Modeling and AI Security]*

Threat Modeling Manifesto — 2020 community statement of values and principles: people and collaboration over tools, a journey of understanding over a snapshot, doing it early and often. *[Threat Modeling Methods]*

Threat type — malicious, accidental, error, failure, natural, external requirement *[CRISC Domain 2: IT Risk Assessment]*

Three-tier campus — A LAN design split into access (user ports), distribution (aggregation and Layer-3 boundary) and core (high-speed backbone) tiers. *[Classic Enterprise Network Architecture]*

Threshold — KRI value that triggers escalation; changed only by the owner after reassessment, never to silence an alert. *[CRISC Exam Strategy]*

Threshold key sharing (1-08, annex A) — The ElGamal private key is split among electoral board members; k of n shares are needed to decrypt, none can alone. Centralised or distributed generation, maximal or lower threshold. *[Internet Voting for Non-Political Elections]*

Threshold value — bound not to cross, e.g. network availability of 99.95 % a year *[SSI Maturity and Security Dashboards]*

TIBER-EU — Threat Intelligence-based Ethical Red Teaming framework of the ECB (2018, revised February 2025 to align with DORA); national implementations TIBER-FR, TIBER-DE, TIBER-NL; phases preparation, testing, closure *[CompTIA PenTest+ PT0-003; DORA: Digital Operational Resilience]*

Tier 0 — The assets that control identity itself (domain controllers, ADCS, directory-sync servers and their admins); compromise there means the whole forest is lost. *[ANSSI Active Directory Recommendation Catalogue; Incident Qualification & Remediation Decision Keys +3]*

Tier 0 / 1 / 2 — Trust zones of the privileged access model: identity control plane, business servers, user workstations; an admin account of one tier never logs on to a lower tier. *[Active Directory Security]*

Tier 0 asset — Any account, group, computer, service or data whose compromise gives control of the identity system itself. Hidden tier 0 paths found in audits: GPOs linked to the Domain Controllers OU editable by a server team, an SCCM/Intune or EDR console that runs code on DCs, the Entra Connect server's sync account (it holds... *[Active Directory Tiering and Kerberos in Depth]*

Tiering / PAW — Tier 0 (DCs, PKI, identity), Tier 1 (servers), Tier 2 (workstations): admin credentials never log on to a lower tier; privileged access workstations for Tier 0/1, as required by ANSSI PA-022 (recommendations for secure administration of information systems). *[ANSSI Endpoint Security: Overview and Windows]*

Time to exploit — Days between public disclosure of a vulnerability and the first observed exploitation in the wild. At about 5

days, a monthly patch cycle leaves internet-facing systems exposed for weeks. [*\[Edge, Readiness and Awareness Reports\]*](#)

Timebox — Fixed period and budget in which scope flexes; typical of agile and RAD. [*\[CISA Domain 3: IS Acquisition, Development and Implementation\]*](#)

Timely patching — KEV first, rings, verify [*\[Mitigation Techniques\]*](#)

Timetable (chronogramme) — Line-by-line table of the whole exercise from START EX to END EX: each inject, its channel and the reaction expected from players. [*\[Organising a Cyber Crisis Management Exercise\]*](#)

TLP — Traffic Light Protocol (FIRST standard, version 2.0 since 2022): a label telling recipients how far they may share a piece of information. [*\[Malware Triage and Analysis\]*](#)

TLP (Traffic Light Protocol) — FIRST sharing label, version 2.0 (2022): TLP:RED (named recipients only), TLP:AMBER (organisation and clients need-to-know; AMBER+STRICT = organisation only), TLP:GREEN (community), TLP:CLEAR (public). [*\[Writing for Security Work\]*](#)

TLPT — Threat-led penetration testing: red team exercise on live production systems driven by threat intelligence, attested by the authority (Art. 26). [*\[Detection Validation and Purple Teaming; CompTIA PenTest+ PTO-003 +1\]*](#)

TLS 1.3 — RFC 8446 (2018): 1-RTT handshake, forward secrecy only (ephemeral DH), AEAD ciphers only, no RSA key transport. [*\[CISSP Domain 4: Communication and Network Security\]*](#)

TMA / ASP — Tierce maintenance applicative (outsourced application maintenance) / application service provider, the fore-runner of SaaS. [*\[IT Usage Charter and Outsourcing Security\]*](#)

TOCTOU — Time-of-check to time-of-use race: a condition checked, then changed by another thread or request before it is used. [*\[Secure Code Review by Language\]*](#)

TOCTTOU — Time Of Check To Time Of Use: a race where the resource changes between the access check and its use. [*\[System Partitioning: ANSSI PG-040\]*](#)

TOE — Target of evaluation: the product and configuration actually evaluated. [*\[CISSP Domain 3: Security Architecture and Engineering\]*](#)

TOFU — Trust On First Use: the first certificate or key seen is accepted without verification. [*\[OT Switch and Firewall Hardening: Hirschmann, SCALANCE\]*](#)

TOGAF — The Open Group Architecture Framework: enterprise architecture method (ADM cycle) into which security architec-

ture is integrated. [*\[CISM Domain 3: Information Security Program\]*](#)

ToIP — Telephony over IP: the whole phone system (handsets, call servers, gateways) runs on an IP network, unlike VoIP which only carries voice over IP. [*\[ToIP and Virtualization Security\]*](#)

Token binding / proof of possession — Tying a token to a key held by the device so a copy is useless elsewhere; Entra **token protection** and Okta **FastPass** device binding do this. [*\[Identity Attacks and ITDR: Entra ID and Okta\]*](#)

Token exchange (RFC 8693) — `grant_type=urn:ietf:params:oauth:grant-type:token-exchange`: a subject token from one domain is swapped at an STS for a token of another; GCP STS and Entra federated credentials implement this pattern. [*\[Multi-Cloud Identity Federation\]*](#)

Token replay — Using a stolen token or cookie from another machine; the IdP sees a valid token from an unexpected IP, device or ASN (Autonomous System Number, the network owner). [*\[Identity Attacks and ITDR: Entra ID and Okta\]*](#)

Token theft after MFA — Infostealers or AiTM steal the post-auth session cookie/token; MFA already passed. Mitigate with token binding, short sessions and impossible-travel alerts. [*\[Social Engineering and Phishing Simulation\]*](#)

Tokenization — Replace the value with a random surrogate; mapping lives in a separate token vault. Takes systems out of PCI DSS scope. [*\[Data Protection and Resilience; Privacy Engineering and PETs\]*](#)

Tokenization vs encryption — tokenization swaps data for a random value kept in a vault (format preserved); format-preserving encryption keeps structure with a key but may be weaker. [*\[Cryptography Engineering and PQC; CSA Security Guidance v4: the 14 Domains\]*](#)

Tolerable error — Maximum error the auditor accepts while still concluding the control or balance is acceptable. [*\[CISA Domain 1: Information System Auditing Process\]*](#)

Tone at the top — The attitude of the board and executives toward risk and control, which staff imitate. [*\[CRISC Domain 1: Governance\]*](#)

Tool poisoning — Hidden instructions in a tool's description or schema that the model reads as trusted context. [*\[Agentic AI and MCP Security\]*](#)

Tools server (serveur outils) — Server in an admin zone hosting vendor consoles and admin tools, reached only from admin workstations. [*\[ANSSI Secure Administration of IS \(PA-022\)\]*](#)

Top-of-rack (ToR) — An access switch placed at the top of each server rack; servers cable up to it, and it uplinks to the spines/aggregation. [*\[Data-Centre Architecture\]*](#)

Top packages (Census III) — npm direct: **react-dom**; non-npm direct: **spring-boot-starter-web** (Maven); non-npm direct and indirect: Google **google-cloud-go**; log4j-core ranked #51 non-npm direct. [*\[Industry and Workforce Reports\]*](#)

Topology change (TC) — Event flooded after a port moves to forwarding or fails; switches age their MAC tables quickly and flood until they relearn. [*\[Switching: VLANs, Trunks, Spanning Tree, EtherChannel\]*](#)

ToS — Terms of service. Constraints imposed by third-party/cloud providers. [*\[Engagement Management\]*](#)

TOTP — Time-based one-time password (RFC 6238): 6 digits derived from a shared secret and the current 30 s window. [*\[ASVS 5.0 - Chapter Highlights and 4.0.3 Delta\]*](#)

Toxic combination — Set of individually harmless permissions that together allow escalation, e.g. `iam:PassRole` plus `lambda:CreateFunction`. [*\[Cloud Entitlement Management and Least Privilege\]*](#)

TP / IVP — Transformation procedure (the only way to change a CDI) / integrity verification procedure (checks CDI consistency). [*\[CISSP Domain 3: Security Architecture and Engineering\]*](#)

TPE / PME — Tres petite entreprise (micro-business, under 10 staff) / petite et moyenne entreprise (SME, under 250 staff). [*\[Business Travel and SME Cybersecurity\]*](#)

TPM — Trusted Platform Module: chip on the motherboard that stores keys and records boot measurements in PCRs (Platform Configuration Registers). [*\[Remote Work \(Digital Nomadism\); CISSP Domain 3: Security Architecture and Engineering\]*](#)

TPM (Trusted Platform Module) — Discrete or firmware chip storing keys and PCR measurements; seals BitLocker VMK to boot state. Clearing the TPM erases keys: have the recovery key. [*\[CompTIA A+ Core 1 - Hardware and Troubleshooting\]*](#)

TRA (targeted risk analysis) — Documented analysis the entity performs to set its own frequency for flexible requirements (Req. 12.3.1). [*\[PCI DSS v4.0.1, CVSS and FIRST\]*](#)

Traffic selector — The pair of source and destination subnets an IPsec Child SA protects; both peers must propose matching selectors. [*\[VPN, Firewall Policy, Models, QoS: Self-Assessment\]*](#)

Training — Teaching personnel their roles and responsibilities in an IT plan (IR, contingency, COOP) so they can take part in exercises, tests and real events. *[IR Exercises and Threat Information Sharing]*

Transchiffrement — Re-encrypting a partition under a new data encryption key (key rotation of the disk itself). *[ANSSI Encryption Tools: Zed! and Cryhod (2/2, Cryhod)]*

Transformation — Normalization applied before matching (t:lowercase, t:urlDecodeUni, t:htmlEntityDecode) so encodings do not evade rules. *[WAF and API Gateway Configuration]*

Transformers — Self-attention architecture (2017, "Attention is all you need"). Processes all tokens in parallel, captures long-range context; basis of GPT, Claude, Llama, BERT. *[AI Fundamentals for Cybersecurity]*

Transient execution — Speculative or out-of-order work a CPU later discards, whose micro-architectural traces can still leak data. *[CPU Side Channels and Memory Attacks]*

Transitive trust — After decryption the browser no longer sees the real server certificate: it trusts whatever the proxy's TLS client accepted (R15). *[HTTPS Flow Inspection: Proxy and Reverse Proxy]*

Transparency log — Append-only, publicly auditable Merkle-tree log (Sigstore Rekord) that records signing events so misuse of an identity is detectable. *[Software Supply Chain Security]*

Trap vs inform — Both are unsolicited notifications from the agent; an inform is acknowledged by the manager and resent if lost, a trap is not. *[Network Operations: Documentation, Monitoring, Resilience]*

Treatment plan — Set of actions, owners, budget, milestones and expected residual risk for a chosen response, tracked like a project. *[CRISC Domain 3: Risk Response and Reporting]*

Tree — One or more domains sharing a contiguous DNS namespace (corp.example.com and eu.corp.example.com). A forest can hold several trees with different namespaces. *[On-Prem Active Directory Architecture; Git Internals and Repository Security]*

Triage — First assessment of an alert: is it real, how bad, who owns it next, within minutes. *[SOC Operations and SOAR]*

TRIM — Command telling an SSD which blocks the file system no longer uses, so garbage collection can erase them early. *[Storage: Interfaces, SSD Internals, RAID, SMART]*

Triple extortion — Adds DDoS, calls to customers, patients or employees, or pressure on partners. *[Ransomware: Anatomy, Detection, Prevention]*

Trojan — Looks legitimate, does something else; a RAT (remote access trojan) gives persistent remote control. Does not self-replicate. *[Malware, Attacks and Indicators]*

True positive / false positive — Alert on real attack / alert on benign traffic (tuning burden). *[NIST Network Security Guides]*

Trunk — Carries many VLANs tagged plus one **native VLAN** untagged. Both ends must agree on native VLAN and allowed list. *[Switching: VLANs, Trunks, Spanning Tree, EtherChannel]*

Trunk / access port — An access port carries one VLAN untagged to an end device; a trunk carries several VLANs tagged with 802.1Q between switches. *[Access Switch Audit Grid: DAT-NT-025 R1-R71]*

Trust algorithm — The logic inside the PE. Criteria-based: pass a fixed set of checks (device compliant AND MFA AND allowed role). Score-based: sum weighted signals into a confidence score and compare to a threshold for the resource's sensitivity. Real deployments blend both and re-run them continuously (detailed in 'Zero Trust...'). *[Zero-Trust Architecture]*

Trust anchor — Root keys pre-installed in OS / browser stores. A rogue or breached CA breaks everything below it: DigiNotar (2011) issued a *.google.com cert, then went bankrupt. Certificate Transparency logs (RFC 6962) now expose mis-issuance. *[Network Security I - Crypto, PKI, IPsec, Firewalls, Wi-Fi]*

Trust boundaries — authenticate at every boundary (802.1X, mTLS, MFA), least privilege, separate admin accounts *[ANSSI Secure Architecture: sensitive and RD systems]*

Trust boundary — A line in the data-flow diagram where the level of trust changes: privilege, ownership, network zone or tenant. Every flow crossing it needs **authentication, authorisation, validation, encryption and logging**; elements on the same side may share assumptions. Zero trust pushes the boundary down to each request and... *[Secure Architecture Patterns; Threat Modeling Methods +1]*

Trust direction vs access — Access flows opposite to trust: if A trusts B, users in B can be granted access to A. A two-way trust allows both. *[On-Prem Active Directory Architecture]*

Trust level — Operational unit shares the level of trust in data and systems; strategic unit assesses criticality of compromised

data and decides bypass measures. *[Cyber Crisis Management & Communication]*

Trust score (score de confiance) — explicit, continuously computed trust level; a device's score can never exceed the implicit trust granted to its device type. *[ANSSI Zero Trust Model]*

Trust store (root program) — The set of root CAs an OS or browser trusts by default (Microsoft, Apple, Mozilla NSS, Chrome Root Store). A private/enterprise store adds internal roots. *[PKI and Certificate Architecture]*

Trust vs trustworthiness (F.1) — Trust is a belief that an entity meets certain expectations and can be relied upon; trustworthiness is demonstrated by evidence supporting a claim of being worthy of trust. Trust granted without the required trustworthiness is a significant contributor to risk (E.29 Substantiated Trustworthiness). *[Engineering Trustworthy Secure Systems]*

Trust zone (zone de confiance) — Resources of homogeneous sensitivity administered by administrators of the same trust level; criteria: business criticality, internal vs outsourced, exposure, regulation, geography. *[ANSSI Secure Administration of IS (PA-022)]*

Trusted Computing Base (TCB) — the hardware, firmware and software whose bugs would break the security of the whole system (term from the US DoD Orange Book, TCSEC, 1985). In a cloud VM it normally includes the host OS and hypervisor operated by the CSP. *[Confidential Computing]*

Trusted core (coeur de confiance) — Identity management, administration, security supervision and hypervisors; its compromise compromises the whole IS, so keep it minimal. Often centred on AD, but not necessarily. *[Managing Cyber Remediation]*

Trusted core (socle de confiance) — The part of the IS that, if compromised, makes the whole IS suspect: identity management, virtualisation management, administration, security supervision. Remediation actions are carried out from it; keep it **minimal** and manage every control it contains from inside it. *[Managing Cyber Remediation]*

Trusted list — Signed national list of qualified trust services and PID providers; the EU List of Trusted Lists (LOTL) points to every national list. *[eIDAS 2 and the EU Digital Identity Wallet]*

Trusted network — PA-043 term for the dedicated network carrying RADIUS traffic between authenticators and servers. *[BGP, 802.1X & VPN]*

Trusted node — QKD relay where keys exist in clear and must be physically protected; it breaks end-to-end security. *[ANSSI PQC Transition: Positions and Protocols]*

Trusted referee — CSP agent or third party who makes risk-based decisions for applicants who cannot meet the standard process (no documents, disability, minors). CSP SHALL publicize and document the service when offered (63A-4 Sec. 3.15.1). *[Digital Identity Guidelines SP 800-63-4]*

Trusted referee (3.15.1) — CSP, third-party or RP agent who makes risk-based decisions for applicants who cannot complete the normal process (no documents, disability, disaster victims, minors). Public notice, written procedures, training and certification, annual reassessment of visual inspection skills, full session record. *[Proofing Evidence and FAL Requirements]*

Trusted timestamp (TSA) — A time-stamp authority (TSA, defined in RFC 3161) signs a hash together with the time, proving the data existed then; used in code signing and legal e-signatures under eIDAS (EU regulation on electronic identification and trust services). *[Fundamental Security Concepts]*

Trusted toolkit — Statically linked binaries (busybox, UAC, AVML) run from read-only media or a share, because the suspect's ps, ls or libraries may be trojanised. *[Linux DFIR and Live Response]*

TSIG — Transaction Signature (RFC 8945): shared-secret HMAC that authenticates DNS messages such as zone transfers, NOTIFY and dynamic updates. *[DNS, Wi-Fi & DDoS Architectures; DNS Infrastructure Operations]*

TT&C (telemetry, tracking and command) — The control channel of a satellite: telemetry reports its health, commands change its state. Unauthenticated commands can take control of the spacecraft. *[Space and Satellite Security]*

TT&E — Test, training and exercise: the SP 800-84 program that keeps IT plans (incident response, contingency, continuity) valid and staff ready. *[IR Exercises and Threat Information Sharing]*

TTL — Time To Live: hop counter in every IP packet, decremented by each router; at 0 the packet is dropped and an ICMP 11 is returned (traceroute relies on it). *[IP Addressing, ICMP, DHCP and Network Triage]*

TTL (DNS) — seconds an answer may be cached; short TTLs speed up changes (and fast-flux), long TTLs prolong a poisoned or hijacked answer. *[DNS Security in Practice]*

TTP — Tactics, Techniques and Procedures: how an adversary operates; expensive for them to change, so the most durable

basis for detection. *[Threat Hunting Playbooks; Threat Actor Profiles +1]*

TTPs — Tactics, techniques and procedures: the behavior pattern of an adversary. *[CEH v13: Exam Blueprint and Module Map; CEH v13: Core Concepts, Phases and Legal Framework]*

Tuning — Adjusting thresholds, disabling irrelevant signatures and whitelisting known-good activity so alerts become actionable. *[Firewall Policy Management and IDS/IPS]*

Tunnel — Encapsulation of one packet inside another: the inner packet keeps private addresses, the outer header carries public addresses between the two tunnel endpoints. *[VPNs in Depth: IPsec/IKEv2, TLS VPN, WireGuard]*

Type 1 vs Type 2 — Bare metal (ESXi, Hyper-V, KVM) vs hosted on an OS (VirtualBox, Workstation). *[Hardware: Self-Assessment]*

U

U/L bit — Second-least significant bit of the first octet: 1 = locally administered. Randomized Wi-Fi MACs (iOS, Android, Windows 'random hardware addresses') set it, so the second hex digit is 2, 6, A or E. NAC (Network Access Control) and MAB (MAC Authentication Bypass: the switch authenticates a device by its MAC alone)... *[Ethernet, MAC Tables and ARP]*

UAT — User acceptance test: business users confirm the system meets requirements before go-live. *[CISA Domain 3: IS Acquisition, Development and Implementation]*

UDP scan (-sU) — Slow but the only way to find DNS/SNMP/TFTP and other UDP services a SYN scan cannot see. *[Reconnaissance and OSINT]*

UDS (ISO 14229) — Unified Diagnostic Services: request/response diagnostic protocol (read data, write data, flash firmware); service 0x27 SecurityAccess (seed/key) and 0x29 Authentication (certificate-based, 2020 edition) gate sensitive functions. *[Automotive and Embedded Security]*

UEBA — User and Entity Behavior Analytics: flags deviations from each user's or host's normal behaviour. *[SIEM and Detection Engineering; CEH v13: Core Concepts, Phases and Legal Framework +3]*

UEBA (user and entity behavior analytics) — Statistical or ML baselines of normal behaviour per user, host or service; deviations raise risk scores. *[Security Operations]*

UEBA (User and Entity Behaviour Analytics) — Analytics that learn a baseline per user, device or service account and per peer

group (same team, same role), then score deviations and chain them into a risk score that decays over time. *[Insider Threat Program]*

UEFI lock — Windows option storing a VBS setting in a UEFI variable so malware or admins cannot disable it from the OS. *[Windows Privacy GPOs and VBS Deployment; UEFI, Secure Boot and Bootkits]*

UEM / MDM — Unified Endpoint Management / Mobile Device Management: central configuration and compliance of laptops and phones. *[DoD Zero Trust and NSA Hardening Guidance]*

UGAP — Union des groupements d'achats publics: the national public central purchasing body. *[PPST Research Protection and Buying Qualified Security]*

UKI (Unified Kernel Image) — One EFI binary bundling kernel, initramfs and command line, signed as a whole so Secure Boot covers all three. *[ANSSI GNU/Linux Hardening Deep Dive (BP-028 R1-R49); Linux Boot, Processes and System Calls]*

ULA / GUA — Unique Local Address (fd00::/8, private) / Global Unicast Address (2000::/3, public). *[IPv6 in Depth: Addressing, NDP, SLAAC, Security]*

Unacceptable risk (prohibited) — Art. 5: social scoring, manipulative or exploitative techniques, untargeted facial-image scraping, emotion recognition at work or school, biometric categorisation of sensitive traits, predictive policing based on profiling alone; banned since 2 Feb 2025. *[AI Compliance Frameworks]*

Unawareness and unintervenability — people not informed or unable to act on their data *[Privacy Engineering and PETs; Threat Modeling Methods]*

Undefined vs unspecified behaviour — undefined: the standard imposes nothing (signed overflow); unspecified: several allowed outcomes, none imposed (order of # and ## evaluation). Full lists in annexes G/J of C90/C99. *[C and Rust Secure Coding Rule Catalogue]*

Underlay — Physical routed IP network that carries encapsulated packets between tunnel endpoints; knows VTEP loopbacks, never tenant addresses. *[Overlay, Data-Centre and Cloud Network Internals]*

Underlay vs overlay — The underlay is the physical IP-routed spine-leaf network; the overlay is the set of VXLAN tunnels carrying tenant segments on top of it. *[Data-Centre Architecture]*

Uni — one-way data transfer between two zones (stateful firewall, gateway or data diode depending on class), placed closest to the lower class. *[ANSSI ICS/SCADA Security]*

Uni (unidirectionality) — data can only be written or read from one of the two zones, so the flow is strictly one-way; placed nearest the lower class; implemented by a stateful firewall, a gateway or a diode depending on class. *[ANSSI ICS Detailed Measures v2 (2/2): technical measures]*

Unified audit log (UAL) — Tenant-wide record of user and admin actions across Exchange, SharePoint, OneDrive, Teams, Entra and Power Platform, searched in Purview or with Search-UnifiedAuditLog. *[Microsoft 365 Hardening]*

Unified log — Apple's single logging system since macOS 10.12 / iOS 10: binary .tracev3 files in /private/var/db/diagnostics plus format strings in /private/var/db/uidtext; read with log show. *[macOS and iOS Forensics for Defenders]*

Unique + long — banned-password lists, 14+ chars *[Network and Authentication Attacks]*

Unit test — Tests one program or module in isolation, usually by the developer. *[CISA Domain 3: IS Acquisition, Development and Implementation]*

Unit test data — A true-positive event sample and a known-benign sample committed beside the rule so a schema change that breaks it fails CI, not silently in production. *[Detection Rules: Sigma and YARA Catalogue]*

Universal default password — the same factory password on every unit (admin/admin): banned by ETSI EN 303 645, UK PSTI and EN 18031 *[IoT and Medical Device Security]*

Unskilled attacker — script kiddie, public tools, opportunistic *[Threat Actors and Threat Vectors]*

Updatable help — PowerShell ships only command syntax by default; the full help text (descriptions, examples) is downloaded on demand with Update-Help. *[Read the Manual: man, help, tldr and info]*

Upstream (tracking) — the remote branch a local branch is linked to, so bare git push/git pull know where to go; set with -u. *[Essential Git Commands: a Working Reference]*

Upward interconnection (montante) — Data goes low → high. Essential service: **unidirectionality** (R11). Risk: integrity and availability of the high IS via injected data. *[Multilevel Interconnections & Trusted Core]*

URG — Urgent pointer field is valid; almost never used *[TCP and UDP Deep Dive]*

uRPF (unicast Reverse Path Forwarding) — Anti-spoofing check: the router accepts a packet only if its routing table would send replies to that source out of the same interface (strict) or out of any interface (loose). *[IPv4 Addressing, Subnetting, VLSM and NAT]*

USB drops — Seeded USB devices in lots/lobbies. Use benign beacon payloads only. *[Vulnerability Discovery and Analysis]*

USCG — United States Coast Guard, author of the 2025 cybersecurity rule for US-flag vessels and port facilities (33 CFR part 101). *[Cyber Security On Board Ships]*

Use-after-free — Memory is used after being released, so an attacker can control what occupies it: BlueKeep. *[Secure Coding in C and Rust, CMS and JRE Hardening; Famous Vulnerabilities Explained]*

Use case — a documented detection objective: threat, data source, logic, expected response, owner and test. *[ANSSI Logging and Security Supervision]*

Use-case profile — The AI RMF functions, categories and sub-categories implemented for one setting, e.g. a hiring profile or a fair-housing profile. *[AI Risk Management Framework]*

User domain (domaine utilisateur) — A user's complete OS, data and software, implemented as a **VM** (sandboxes are not enough: shared kernel, larger attack surface). *[Multi-Environment Workstation and Refurbishing]*

User Interaction — N none, P passive, A active (3.1: N/R) *[Vulnerability Management and Security Testing]*

User-managed SA — name@project.iam.gserviceaccount.com; both a principal and a resource. Attach to VM/GKE/Cloud Run/Functions; the workload gets tokens from the metadata server without any key. *[GCP Security Essentials]*

User space — The unprivileged mode where every normal program, including those run by an administrator, executes. *[Operating System Concepts for Beginners]*

usersn-remap — Docker option mapping container UID 0 to an unprivileged host UID range through a user namespace. *[Docker Container Security]*

Using the work of an expert — The auditor may rely on a specialist (e.g. cryptography, legal) after assessing their competence, independence and the adequacy of their work (ITAF 1206). *[CISA Domain 1: Information System Auditing Process]*

UTL (unité de traitement local) — Local door controller: decides whether to open, holds the rights logic and keys; installed

inside the protected zone. *[Physical Access Control and CCTV (ANSSI PA-72)]*

UTM (unified threat management) — One appliance combining firewall, IPS, antivirus, web filtering and VPN. *[VPN and Firewall Security]*

V

V15.3 defensive coding (L2) — No automatic redirects on backend fetches (15.3.2); mass-assignment field limits (15.3.3); trusted client-IP header chain (15.3.4); strict type comparisons (15.3.5); prototype-pollution-safe JavaScript (15.3.6); HTTP parameter pollution defence (15.3.7). *[ASVS 5.0 - Chapter Highlights and 4.0.3 Delta]*

V17 WebRTC (all L2/L3) — TURN media relays refuse reserved or internal IP ranges, so they cannot be used as an SSRF proxy (17.1.1); DTLS (TLS for UDP) keys managed by the key policy (17.2.1); approved DTLS suites and SRTP (Secure Real-time Transport Protocol) profile (17.2.2); signaling survives floods through rate limiting (17.3.1). *[ASVS 5.0 - Chapter Highlights and 4.0.3 Delta]*

v8 → v8.1 changes — New **Govern** security function; new **Documentation** asset class; safeguard wording and asset types revised; glossary expanded; mappings updated to NIST CSF 2.0. Safeguard numbering stayed the same as v8, so v8 evidence carries over. *[CIS Controls v8.1: All 153 Safeguards]*

VAD — Virtual Address Descriptor: kernel tree node describing one memory region of a process (range, protection, file backing); the basis of injection detection. *[Memory Forensics with Volatility 3]*

Validating data integrity — Hash at acquisition (SHA-256, also MD5 for legacy tools), record in the custody form, re-hash at every transfer and before analysis. *[Incident Response and Management]*

Validation Authority (VA) — Serves revocation status to relying parties via OCSP responders and CRL distribution points. *[PKI and Certificate Architecture]*

Valley-free routing — Economic rule of Internet paths: routes learned from a provider or a peer are re-announced only to customers; violating it is a route leak. *[BGP and Internet Routing in Practice]*

Value chain and component integration — opaque third-party data, models and components integrated without traceability or quality checks. *[AI Risk Management Program Design]*

Value delivery — Security investment optimized so that it supports business objectives at acceptable cost. *[CISM Domain 1: Information Security Governance]*

Values — The configuration that fills the templates; defaults in values.yaml, overridden by `-f file` then `--set key=val`. *[Helm, operators and the CRD ecosystem (with security)]*

Variable sampling — Estimates a monetary or quantity value of the population; used in substantive testing. *[CISA Domain 1: Information System Auditing Process]*

vCISO (virtual CISO) — fractional CISO bought as a service, typical for small and mid-size firms; accountability for risk still sits with management *[Building a Security Program]*

vCPU — Virtual CPU: on KVM, a host thread that loops on entering guest mode and handling exits. *[Virtualization Internals and VM Isolation]*

VDP — vulnerability disclosure policy: public way for researchers to report flaws, with a promise to acknowledge and fix *[IoT and Medical Device Security]*

VDP (BOD 20-01) — vulnerability disclosure policy every agency must publish so researchers can report flaws safely. *[CISA Zero Trust Maturity Model v2.0]*

vDPA — virtio data path acceleration: a NIC that implements virtio rings in hardware, so the guest keeps a generic virtio driver and can still migrate. *[Virtualization Internals and VM Isolation]*

VDR / BNWAS — Voyage Data Recorder (the ship's black box) / Bridge Navigational Watch Alarm System (checks the officer on watch is awake). *[Cyber Security On Board Ships]*

Vector storage — Nearest-neighbour index (pgvector, Pinecone, Milvus, Chroma). Needs tenant isolation and per-chunk ACLs (LLM08:2025 Vector and Embedding Weaknesses). *[AI Fundamentals for Cybersecurity]*

Vendor monitoring — Ongoing oversight after signing: annual reassessment, SLA reports, security rating services (BitSight, SecurityScorecard), breach news, certificate renewals, subprocessor changes. *[Governance, Risk and Third-Party Management]*

Verb — The action on a resource (get, create, update, patch, delete, watch); RBAC rules are (apiGroup, resource, verb) triples, so kubectl verbs map straight to permissions. *[kubectl and Cluster Operations Mastery]*

Verifiable mix-net (annex C) — Ballots are re-encrypted and shuffled with a proof of correct shuffle, breaking the link between arrival order and voter (1-07) while keeping the tally au-

ditable (1-11, 3-02). *[Internet Voting for Non-Political Elections]*

Verification hash — acquisition hash recomputed on the image; must match the source hash to prove the copy is faithful. *[DFIR Artifacts and Tools]*

Verification level — L1, L2 or L3: cumulative subsets of requirements; each requirement is tagged with the lowest level that needs it. *[OWASP ASVS 5.0 - Application Security Verification Standard]*

Verified vs measured boot — **Verified** (Secure Boot) refuses unsigned code, locally. **Measured** only records hashes; a remote verifier or a sealed key decides later. Use both: verified stops known-bad, measured detects what signatures allowed. *[Hardware Roots of Trust and the TPM 2.0]*

Verifier — Kernel static analyser that walks every path of a program and rejects unsafe memory access, unbounded loops or disallowed helpers before it can run. *[Confidential Computing and Remote Attestation; eBPF in Depth]*

Verify full functionality — and implement preventive measures *[Hardware: Self-Assessment]*

verify-required — Key option demanding user verification (PIN or biometric) in addition to touch at every use; enforce server-side with PubkeyAuthOptions verify-required. *[SSH in Depth]*

Versioned and immutable — desired state lives in a store that keeps full history (git, OCI registry); every change is a signed, reviewable commit *[GitOps and Continuous Delivery Security]*

Versions — OASIS PKCS#11 v2.40 (2015), v3.0 (2020, adds EdDSA, ChaCha20-Poly1305, profiles), v3.1 (2023). *[HSMs, Supply Chain, Physical Security, Decommissioning]*

VERW buffer clearing — Microcode makes the VERW instruction clear CPU buffers; kernels issue it on every return to user space or VM entry (MDS, TAA, RFDS, TSA). *[CPU Side Channels and Memory Attacks]*

veth pair — Virtual Ethernet cable: two linked interfaces, a frame sent into one comes out of the other; used to join namespaces to a bridge. *[Linux Networking Toolbox]*

VEX — Vulnerability Exploitability eXchange: a supplier statement that a product is or is not affected by a given vulnerability, and why. *[Container Image and Registry Security; Software Supply Chain Security +2]*

VFIO — Linux virtual function I/O framework that gives a user-space process such as QEMU safe access to a device behind an IOMMU. *[Virtualization Internals and VM Isolation]*

VGA LED — GPU seating and PCIe power, try iGPU *[Hardware Troubleshooting Playbook]*

VIB — vSphere Installation Bundle: the signed software package format of ESXi (drivers, agents). *[VMware vSphere and ESXi Security]*

virtio — OASIS standard for paravirtual devices: guest and host share virtqueues (descriptor, available and used rings) in guest memory. *[Virtualization Internals and VM Isolation]*

Virtual access — Any access to an IRR or SIRR, wherever the user sits, counts as access to the ZRR and needs a ministerial opinion, as for physical entry. *[PPST Research Protection and Buying Qualified Security]*

Virtual drive mounting — Mount a cloud share or ISO/VHD as a local drive (Obj 5.3) to stage and move data through a trusted mount, blending with normal file I/O. *[Post-Exploitation and Lateral Movement]*

Virtual environment (venv) — A per-project folder with its own installed packages, activated so that python and pip point to it. *[Python for Security from Zero]*

Virtual infrastructure (4.3) — Limit virtual disks to the guests that use them; shared install images read-only. Virtual switches may not meet monitoring policy: use VLANs, virtual firewalls or central inspection appliances. Virtual storage networks raise the same issue. *[Cloud Outsourcing and Virtualization Lifecycle]*

Virtual patch — WAF rule that blocks exploitation of one known vulnerability at the HTTP layer until the application itself is fixed. *[SecurityX Discriminator Pairs and Gap Closers; WAF and API Gateway Configuration]*

Virtual switch (vSwitch) — A software switch inside the host connecting VMs to the physical NIC and the ToR; distributed vSwitches span many hosts with one policy. *[Data-Centre Architecture]*

Virtual table — osquery table generated on demand by C++ code when a query touches it; nothing is stored until a scheduled query logs results. *[osquery and Velociraptor for Fleet Visibility]*

Virus — Attaches to a host file or program and needs the user to run it; boot-sector, macro, polymorphic (changes its code each copy) and fileless (lives only in memory and scripts) variants. *[Malware, Attacks and Indicators]*

Visa de securite — ANSSI security visa: CSPN certification, Common Criteria certification or qualification of a product or service. *[Remote Work (Digital Nomadism)]*

Visa de sécurité / Security visa — ANSSI label (certification or qualification) identifying products and services evaluated by approved labs with a rigorous method. *[ANSSI CyberDico FR/EN Glossary]*

Vishing / smishing — Voice-call phishing / SMS phishing. *[Social Engineering and Phishing Simulation]*

VLAN ranges (Cisco) — 1 default (cannot be deleted), 2-1001 normal (stored in `vlan.dat`), 1002-1005 reserved for legacy FDDI/Token Ring, 1006-4094 extended (needs VTP v3 or transparent mode on older IOS). *[Switching: VLANs, Trunks, Spanning Tree, EtherChannel]*

VLSM — Different mask lengths inside one block; allocate largest subnets first to avoid overlap. *[Networking Fundamentals I - Models, IP, TCP, Ports]*

VLSM (Variable-Length Subnet Masking) — Cutting one block into subnets of different sizes (a /25 for 100 users, a /30 for a router link) instead of equal-size subnets. *[IPv4 Addressing, Subnetting, VLSM and NAT]*

VM escape — Guest-controlled input triggers a bug in the hypervisor or device model and the attacker gains code execution on the host. *[ToIP and Virtualization Security; Virtualization Internals and VM Isolation]*

VM exit — Hardware switch from guest to hypervisor, saving guest state in the VMCS and recording a reason code. *[Virtualization Internals and VM Isolation]*

VMCS (virtual machine control structure) — Per-vCPU memory block holding guest state, host state, execution controls (which events cause exits) and exit information; AMD calls it VMCB. *[Virtualization Internals and VM Isolation]*

VMkernel adapter — IP interface of ESXi for infrastructure traffic (management, vMotion, storage, backup); one per flow type on its own VLAN (R5). *[VMware vSphere and ESXi Security]*

VMM / vTPM — Virtual Machine Monitor, the per-VM emulator process (e.g. QEMU); virtual TPM giving each user domain its own measured boot and sealed keys. *[Multi-Environment Workstation and Refurbishing]*

vMotion — live migration of a running VM between ESXi hosts; the VM's memory crosses the network. *[VMware vSphere and ESXi Security]*

VMS — Video Management System: records and displays camera streams and camera alarms. *[Physical Access Control and CCTV (ANSSI PA-72)]*

VNI — VXLAN Network Identifier: 24-bit segment id (about 16.7 million segments versus 4,094 usable 802.1Q VLAN ids). *[Overlay, Data-Centre and Cloud Network Internals]*

VoIP (SIP, RTP) — Use SIP over TLS and SRTP; separate voice VLAN; risks are toll fraud, eavesdropping, vishing. *[CISSP Domain 4: Communication and Network Security]*

Volatile evidence — Data lost when a system stops: memory, running processes, network connections, instance-store disks. *[Cloud Incident Response and Forensics]*

Voluntary notification (Art. 30) — any entity may report incidents, cyber threats and near misses; does not create extra obligations *[NIS2 Directive: EU-wide Obligations]*

VPC — Virtual private cloud: isolated cloud network where private model endpoints are exposed only internally. *[SecAI+ Discriminators and Practice Scenarios]*

VPC (virtual private cloud) — Isolated virtual network of one customer inside a public cloud, filtered by security groups. *[Cloud Computing Security]*

VPN concentrator — Gateway appliance that terminates the VPN tunnels of all nomadic devices; ANSSI calls it *concentrateur VPN*. *[Remote Work (Digital Nomadism)]*

VPN (Virtual Private Network) — An encrypted and authenticated tunnel over a shared network (usually the Internet) that makes remote hosts or sites behave as if they were on the private network. *[VPNs in Depth: IPsec/IKEv2, TLS VPN, WireGuard]*

VRF — Virtual Routing and Forwarding: separate routing tables on one router, so zones do not reach each other unless a firewall routes between them. *[Segmentation and IS Mapping]*

VRM — Voltage regulator module: board circuitry converting 12 V to CPU core voltage; weak VRMs throttle high-end CPUs. *[CPUs, Memory, Motherboards and Buses]*

VSAT — Very small aperture terminal: customer satellite dish and modem, managed remotely by the network operator (the target in the Viasat attack). *[Space and Satellite Security]*

VSAT / CPE — Very small aperture terminal (satellite Internet link) / customer premises equipment, the on-board satellite router. *[Cyber Security On Board Ships]*

VSM (Virtual Secure Mode) — Memory region isolated by the Hyper-V hypervisor (VTL1) where the Secure Kernel and

trustlets run, unreadable from the normal Windows kernel (VTL0). *[Windows Privacy GPOs and VBS Deployment]*

VTEP — VXLAN Tunnel End Point: device that encapsulates and decapsulates overlay frames; a leaf switch (hardware VTEP) or a hypervisor virtual switch (software VTEP). *[Overlay, Data-Centre and Cloud Network Internals]*

VTEP (VXLAN Tunnel Endpoint) — The point (a leaf switch or a hypervisor) that wraps and unwraps VXLAN, mapping a VM's frames to a VNI (VXLAN network identifier). *[Data-Centre Architecture]*

VTP / MVRP / GVRP — Automatic VLAN propagation; disabled (R25) because a rogue server with a higher revision number erases the VLAN database. *[Network Equipment Hardening]*

vTPM — virtual Trusted Platform Module: software TPM given to a VM to record boot measurements and seal keys. *[Confidential Computing]*

Vulnerability — A weakness in an asset or control that a threat can exploit. *[CEH v13: Core Concepts, Phases and Legal Framework; CISM Domain 2: Information Security Risk Management +2]*

Vulnerability classification — Group by type (misconfiguration, missing patch, weak crypto, injection, default credentials) and by asset class to route to the right team. *[Vulnerability Management and Monitoring]*

Vulnerability management — Continuous cycle of discovering, prioritizing, remediating and verifying weaknesses. *[CEH v13: Core Concepts, Phases and Legal Framework; CompTIA CySA+ CS0-003]*

Vulnerability (V.x) — a weakness that makes a risk possible, e.g. V4 management interface reachable remotely. *[ENISA Cloud Computing Risk Register (2009)]*

VXLAN — Virtual eXtensible LAN (RFC 7348): carries an Ethernet frame inside UDP with a 24-bit VNI (VXLAN Network Identifier); IANA port 4789, Linux and Flannel default 8472. *[Kubernetes and Container Networking Explained]*

VXLAN (RFC 7348) — Virtual eXtensible LAN: L2 frames in UDP **4789** between VTEPs (VXLAN tunnel endpoints, usually the leaf switches) over a routed underlay (OSPF, IS-IS or eBGP per RFC 7938). Underlay MTU at least 1550, usually 9216. *[Wireless, Data-Center Fabrics and Cloud Networking]*

W

W xor X / ASLR — a memory page is writable or executable, never both / Address Space Layout Randomization: code and data at unpredictable addresses. *[System Partitioning: ANSSI PG-040]*

WAF — Web Application Firewall: reverse proxy that filters HTTP requests with attack signatures. *[Attack Mitigation and Vulnerability Response; WSTG v4.2 - Complete Test Catalogue +1]*

WAF (web application firewall) — Layer-7 filter that parses HTTP requests and responses and blocks those matching attack signatures, anomaly scores or policy rules. *[VPN and Firewall Security; WAF and API Gateway Configuration]*

Wallet unit attestation — statement by the wallet provider that the wallet instance and its WSCD are genuine and not revoked, checked by issuers before issuance *[eIDAS 2 and the EU Digital Identity Wallet]*

War — State cyber operations against critical infrastructure and military targets alongside kinetic conflict. *[Threat Actors and Threat Vectors]*

Warninglist — MISP list of known-benign values (top domains, public DNS resolvers, cloud ranges) that flags likely false positives before they reach a blacklist. *[Cyber Threat Intelligence Lifecycle]*

Watering hole — Compromise a site the target group visits instead of contacting them directly. *[Social Engineering and Phishing Simulation]*

Watering hole (T1189 Drive-by Compromise) — Compromise a site the target group visits; drive-by exploit or fake update. *[Indicators of Malicious Activity]*

WDAC — Windows Defender Application Control (App Control for Business): kernel-enforced allow-list of drivers and executables. *[ANSSI Endpoint Security: Overview and Windows]*

Web application firewall — Layer 7 proxy for HTTP: OWASP Core Rule Set (CRS) signatures, virtual patching, bot and rate limits. Complements, does not replace, the NGFW. *[NIST Network Security Guides]*

WebRTC — Web Real-Time Communication: browser audio, video and data; TURN servers relay media when direct paths fail. *[OWASP ASVS 5.0 - Application Security Verification Standard]*

WebView — Embedded browser inside an app; a JavaScript bridge exposes native functions to page scripts. *[OWASP Mobile - Top 10 2024, MASVS v2.1, MASTG]*

WEF — Windows Event Forwarding: built-in push of selected event logs from endpoints to a collector server. *[ANSSI Endpoint Security: Overview and Windows]*

WEF / WEC — Windows Event Forwarding: built-in agentless forwarding of Windows events over WinRM to a Windows Event Collector server. *[ANSSI Logging and Security Supervision; Windows Audit Policy and Event ID Reference]*

Welfare network — Separate crew Internet network for personal devices, isolated from ship business IT and OT. *[Cyber Security On Board Ships]*

whatis database — a pre-built index of every man page's NAME line, rebuilt by `mandb` (Linux) or `makewhatis` (BSD/macOS); `apropos` and `whatis` search it, so a stale index makes them find nothing. *[Read the Manual: man, help, tldr and info]*

White cell (control team) — Small client-side group that knows about the exercise, owns the rules of engagement, deconflicts incidents and can stop the test; renamed control team in TIBER-EU 2025 and DORA TLPT. *[Red Team Programme and Rules of Engagement]*

White hat — Authorized security tester working with permission and a defined scope. *[CEH v13: Exam Blueprint and Module Map]*

White team — The few client staff who know a covert test is running; they authorize, deconflict and can stop it. *[CompTIA PenTest+ PT0-003]*

WIDS — Wireless intrusion detection: flags rogue access points and deauthentication floods. *[CEH v13: Countermeasures by Module Family]*

Wildcard mask — Inverted mask used by ACLs and OSPF network statements: 0 bits must match, 1 bits are ignored (0.0.0.255 = any value in the last octet). *[IPv4 Addressing, Subnetting, VLSM and NAT; Cisco IOS Configuration Lab]*

Win32_DeviceGuard (annex E) — Namespace `root\Microsoft\Windows\DeviceGuard`. `AvailableSecurityProperties` / `RequiredSecurityProperties`: 1 base virtualization, 2 Secure Boot, 3 DMA protection, 4 Secure MOR, 5 NX protection, 6 SMM mitigations. `SecurityServicesConfigured` / `Running`: 1 Credential Guard, 2 HVCI. `VirtualizationBasedSecurityStatus`: 0... *[Windows Privacy GPOs and VBS Deployment]*

Window scaling stripped — A middlebox removing option 3 caps every flow at 64 KiB per RTT: long-distance transfers crawl while LAN tests look fine. *[TCP and UDP Deep Dive]*

Windows LAPS — Built-in (April 2023 update onwards) service that gives every machine a unique, rotated local admin password stored encrypted in Active Directory or in Microsoft Entra ID; replaces legacy Microsoft LAPS (MSI, cleartext `ms-Mcs-AdmPwd` attribute). *[Windows Hardening Baseline]*

WinRM — Windows Remote Management: SOAP-over-HTTP(S) remote administration used by PowerShell Remoting. *[Networking Ports and Protocols]*

Wiper — Malware that destroys data or boot records; sometimes dressed up as ransomware with no working decryption. *[Landmark Incidents and Lessons]*

Withdrawn — Ids are never reused: AC-2(10) is withdrawn, incorporated into AC-2k. The control number remains in the tables. *[SP 800-53 Rev. 5 Security and Privacy Controls]*

Withdrawn / superseded — Kept for history only. Policies and contracts that cite a withdrawn revision (SP 800-61r2, SP 800-88r1) are out of date. *[NIST Cyber Publications 2024-2026 Roundup]*

WLAN (wireless LAN) — IEEE 802.11 (Wi-Fi) network of access points (AP) and clients (stations). *[Wireless Security and IDS/IPS]*

Word splitting — Cutting an unquoted expansion into several arguments at spaces, tabs and newlines (the characters in IFS). *[Bash Scripting from Zero]*

Wordlist — A file of candidate passwords (leaked-password corpora, dictionaries) a cracker tries first; the famous `rockyou.txt` came from a 2009 breach. *[Password and Hash Auditing for Defenders]*

Work factor — Time and effort needed to break a cryptosystem; should exceed the value and lifetime of the data. *[CISSP Domain 3: Security Architecture and Engineering; Security Operations: Logs, Malware, Servers, Media +1]*

Work profile — Android container separating professional apps and data from personal ones on the same phone. *[Mobile Device Security and MDM]*

Work Role — A grouping of Tasks (with their K and S) that describes a job function, not a job title: "Incident Response", "Secure Software Development". *[NICE Workforce Framework for Cybersecurity]*

Workgroup — Peer-to-peer Windows computers, each with its own local accounts; no central control, fine for fewer than

about 10 PCs. *[Windows Administration and Active Directory Basics]*

Workload identity — Identity used by software (role, managed identity, service principal, service account) rather than by a person. *[Cloud Entitlement Management and Least Privilege]*

Workload identity federation — Letting a workload trade a token from its own platform for cloud credentials, with no stored secret. *[GCP Security Essentials; Multi-Cloud Identity Federation]*

WORM — Write Once Read Many storage (S3 Object Lock, immutable blob): logs cannot be modified or deleted before retention expires. *[Linux and Cloud Logging; Malware, Attacks and Indicators]*

WORM storage — Write Once Read Many: archive media or object-lock that prevents rewriting or deleting logs before their retention ends. *[ANSSI Logging and Security Supervision; Security Operations: Logs, Malware, Servers, Media]*

Wormable — Exploitable remotely, without credentials or user action, so malware can spread machine to machine on its own: EternalBlue, BlueKeep. *[Famous Vulnerabilities Explained]*

WPS PIN (annex C.5) — 8 digits, the last a checksum, verified in two halves: brute force needs at most 10,000 + 1,000 attempts, no client traffic required, hence R15. *[Wi-Fi and 802.1X: Full Recommendation Sets]*

Write amplification — Ratio of bytes written to NAND over bytes written by the host; lower is better for speed and endurance. *[Storage: Interfaces, SSD Internals, RAID, SMART]*

Write blocker — device or driver allowing read but blocking write to the source, preserving hashes and admissibility. *[DFIR Artifacts and Tools; Digital Evidence and Chain of Custody +1]*

WRT — Work recovery time: verifying data and returning to production after RTO; $RTO + WRT \leq MTD$. *[CISSP Domain 1: Security and Risk Management]*

WRT (Work Recovery Time) — time after systems are back to verify data, re-enter the backlog and resume normal work *[Governance and Risk Management; Business Continuity and ISO 22301]*

WSCD / WSCA — wallet secure cryptographic device and application: secure element (tamper-resistant chip), eSIM/eUICC (programmable SIM), embedded SE or remote HSM (hardware security module) holding the device-bound private keys; key extraction must be infeasible *[eIDAS 2 and the EU Digital Identity Wallet]*

WYSIWYG — What-you-see-is-what-you-get rich-text editor whose HTML output must be sanitised before display. *[ASVS 5.0 - Chapter Highlights and 4.0.3 Delta]*

X

x.1 in every requirement — x.1.1 policies and procedures documented, up to date, in use, known; x.1.2 roles and responsibilities documented, assigned and understood (new in v4). *[PCI DSS v4.0.1 Requirement by Requirement]*

X.509 certificate — standard structure binding a subject name and public key to a validity period and extensions, signed by an issuer (a CA, Certificate Authority, or itself when self-signed). *[OpenSSL and Certificate Tooling]*

XCCDF — Extensible Configuration Checklist Description Format: the XML format STIGs and scan results are written in; part of SCAP. *[DISA STIG Viewer 3 and STIG Checklists]*

XCCDF / OVAL — SCAP (Security Content Automation Protocol) languages: XCCDF describes a benchmark of rules and profiles, OVAL the machine checks behind each rule. *[Vulnerability and Configuration Scanners for Your Own Estate]*

XOF (extendable-output function) — Hash-like function producing output of any requested length (SHAKE128, SHAKE256). *[ANSSI Cryptographic Mechanisms and PQC]*

XoT — Zone transfer over TLS (RFC 9103): adds confidentiality to the transfer. *[DNS, Wi-Fi & DDoS Architectures]*

XPath filter — Query syntax used by Event Viewer, Get-WinEvent and WEF subscriptions to select events by channel, ID and field values. *[Windows Audit Policy and Event ID Reference]*

XProtect — built-in YARA-signature anti-malware checked at launch and on file change; XProtect Remediator (macOS 12.3+) scans periodically and removes known families. Updated silently outside OS updates. *[macOS Security for Defenders]*

XS-leak — Cross-site leak: inferring data about another origin from side effects (timing, window count, errors). *[Browser-Side Web Security Standards]*

XSS — Cross-site scripting: attacker-controlled script runs in another user's browser in the site's origin. *[Web Application Assessment]*

XSS (cross-site scripting) — Attacker-controlled script runs in your page's origin and can read its data and act as the user. *[Browser-Side Web Security Standards]*

XSS / CSRF / SSRF — Cross-Site Scripting; Cross-Site Request Forgery; Server-Side Request Forgery (fixes in the sheet "Attack Mitigation and Vulnerability Response"). *[CompTIA CySA+ CS0-003]*

XSSI — Cross-Site Script Inclusion: a foreign page loads your authenticated JSON/JS response via a script tag and reads it. *[OWASP Web Security Testing Guide v4.2]*

XTS — block-cipher mode for disk sectors (BitLocker, LUKS): no ciphertext expansion, but no integrity. *[Cryptography Primer]*

XXE — XML External Entity: an XML parser resolves an entity pointing to a file or URL, leaking data or reaching internal hosts. *[OWASP Top 10 - Web (2021 and 2025)]*

Z

Zachman framework — Matrix classifying architecture artefacts by stakeholder view and by what, how, where, who, when, why. *[CISM Domain 3: Information Security Program]*

Zeek — Network security monitor that turns traffic into logs (conn.log, dns.log). A conn_state of S0 (SYN, no reply) across many ports flags a scan. *[Network Scanning and Enumeration Reference (Authorized Labs)]*

Zero-day — A vulnerability exploited before the vendor has released a fix. *[CEH v13: Core Concepts, Phases and Legal Framework]*

Zero-knowledge proofs (annex B) — Proofs that a ballot encrypts 0 or 1, or an integer in a range, and that decryption was correct, without revealing the vote. *[Internet Voting for Non-Political Elections]*

Zero restore errors — restores tested and verified regularly *[Database Security]*

Zero Trust — Security model in which no user, device or network location is trusted by default: every request is authenticated, authorized and encrypted per session, using identity, device health and context. Reference: NIST (US National Institute of Standards and Technology) SP 800-207 'Zero Trust Architecture' (2020). *[Security Operations Architecture; Fundamental Security Concepts]*

Zero window — Receiver buffer full: it advertises window 0, the sender stops and sends zero-window probes. Cause is a slow receiving application or disk, not the network. *[TCP and UDP Deep Dive]*

Zeroization — Immediate erasure of keys by an HSM when tampering is detected or on command. *[Hardware Security: Self-Assessment]*

Zigbee — Low-power IEEE 802.15.4 mesh for IoT; AES-128 but weak key distribution in many deployments. *[CISSP Domain 4: Communication and Network Security]*

ZLE — Zsh Line Editor: zsh's own editor with emacs and vi keymaps; configured with bindkey in ~/.zshrc. *[Shell and Terminal Productivity on Every OS]*

Zone — Group of physical or logical assets that share the same security requirements and target security level (IEC 62443-3-2). *[OT/ICS Network Security]*

Zone / conduit — A zone groups assets with common security requirements; a conduit groups the communication channels between zones. 800-82r3 levels, tiers or zones map onto them. *[OT Architecture and the SP 800-82r3 OT Overlay]*

Zone (IEC 62443-3-2) — Grouping of assets sharing the same security requirements (same target SL). A device connected to devices of a zone inherits the highest SL of the zone. *[ANSSI ICS/SCADA Security]*

ZRR (zone a regime restrictif) — Premises (offices, labs, experimental platforms) whose access is legally restricted; unauthorised capture or intrusion is prosecuted. *[PPST Research Protection and Buying Qualified Security]*

ZTNA — Zero trust network access: per-application access brokered after identity and device checks. *[CISSP Domain 4: Communication and Network Security; CompTIA CySA+ CS0-003 +1]*

ZTNA (zero trust network access) — Brokered, per-application access granted after identity and device checks, instead of network-level VPN access. *[Classic Enterprise Network Architecture; Designing a Secure SME Network and Cloud Landing Zone +2]*

#

0 Emergency — system unusable *[Network Operations: Documentation, Monitoring, Resilience]*

0-RTT (early data) — TLS 1.3 data sent with the first message of a resumed session, before the handshake completes; replayable. *[ANSSI TLS and IPsec Guides: Full R Index]*

1 Alert — immediate action needed *[Network Operations: Documentation, Monitoring, Resilience]*

1 The decision-making unit turns operational — Technical debates at the wrong granularity. Moderators ask for a business-focused situation update (e.g. temporary lay-offs?), exfiltrate the person fuelling the debate via a call, or occupy them with injects. *[Organising a Cyber Crisis Management Exercise]*

2 Critical — critical condition *[Network Operations: Documentation, Monitoring, Resilience]*

2 Decision vs implementation gap — Guidelines ignore technical or time constraints. Add injects from the simulated technical teams raising difficulties as questions and requests for clarification. *[Organising a Cyber Crisis Management Exercise]*

2 Understand one's digital activity — from missions down to business values (processes and information) and supporting assets (IT that carries them), terms of ANSSI's EBIOS RM risk method; map the ecosystem of suppliers and partners (extended enterprise); list the legal frame by mission, sector, status (vital operator OIV, essential-service operator. . .) *[Digital Risk Governance - ANSSI-AMRAE 15 Steps]*

3-2-1 rule — Keep 3 copies of the data on 2 different media, 1 of them offline or off site, so ransomware cannot reach every copy. *[Business Travel and SME Cybersecurity]*

3 Decisions contradicting the exercise goals — E.g. closing the whole organisation when the goal is balancing remediation and continuity. The moderating unit refuses via an intervention (simulated or not) or the exercise agreement (rules of the game announced to players, e.g. which options are off-limits). *[Organising a Cyber Crisis Management Exercise]*

3 Error — error condition *[Network Operations: Documentation, Monitoring, Resilience]*

3 Know your risk acceptance threshold — risk appetite: the risk level management accepts to support activity and growth; set with banks, insurers, partners, customers; reassessed with indicators and watch *[Digital Risk Governance - ANSSI-AMRAE 15 Steps]*

32 vs 64-bit — 32-bit OS addresses 4 GB (about 3.2-3.5 GB usable). Windows 11 exists only as x64 and ARM64. *[CPUs, Memory, Motherboards and Buses]*

4.0 Environmental — Security requirements CR/IR/AR plus modified base metrics; MSI and MSA accept the extra value Safety (S) for human-injury impact. *[PCI DSS v4.0.1, CVSS and FIRST]*

4.0 scoring — About 15 million CVSS-BTE vectors grouped into 270 equivalence sets (MacroVectors) ranked by experts;

six equivalence dimensions EQ1 AV/PR/UI, EQ2 AC/AT, EQ3 VC/VI/VA, EQ4 SC/SI/SA, EQ5 E, EQ6 VC/VI/VA with CR/CI/CA; score interpolated inside each MacroVector. Qualitative bands unchanged from 3.1. *[PCI DSS v4.0.1, CVSS and FIRST]*

4.0 Supplemental (no score effect) — Safety S (Present per IEC 61508 marginal/critical/catastrophic, or Negligible), Automatable AU (all four first kill-chain steps automatable = wormable), Provider Urgency U (Clear, Green, Amber, Red), Recovery R (Automatic, User, Irrecoverable), Value Density V (Diffuse, Concentrated), Response Effort RE (Low, . . .) *[PCI DSS v4.0.1, CVSS and FIRST]*

4.0 Threat metric E — Attacked (A: attacks reported or exploit toolkits exist), Proof-of-Concept (P), Unreported (U); Not Defined (X) is scored as Attacked, so an unenriched score assumes the worst case. *[PCI DSS v4.0.1, CVSS and FIRST]*

4 Build one's worst risk scenarios — compliance with a baseline handles the most likely, untargeted attacks; the committee builds the critical targeted cyberattack scenarios (EBIOS RM workshops 2 risk origins and 3 strategic scenarios) and **quantifies them financially** *[Digital Risk Governance - ANSSI-AMRAE 15 Steps]*

4 Warning — warning condition *[Network Operations: Documentation, Monitoring, Resilience]*

4104 vs 4103 — 4104 = script block text as executed, deobfuscated at each layer, in Microsoft-Windows-PowerShell/Operational; 4103 = pipeline/module execution with bound parameters. PowerShell 7 logs to PowerShellCore/Operational. *[Windows Endpoint Telemetry and Sysmon]*

5 Cyber issues not explained — No shared vocabulary between technical and decision teams. Moderators create ad hoc situation updates with the CISO and the crisis director. *[Organising a Cyber Crisis Management Exercise]*

5 Notice — normal but significant (Cisco link up/down, config change) *[Network Operations: Documentation, Monitoring, Resilience]*

5 Security and promotion strategy — choose treatment (measures, process change, transfer by contract or insurance); four lines: baseline converging to the ISSP, response to critical scenarios in a SCIP with accreditation of the critical services, promotion, insurance transfer *[Digital Risk Governance - ANSSI-AMRAE 15 Steps]*

5G — Cellular with network slicing, SUPI concealment (SUCI) and a service-based core; enterprise private 5G needs its own

segmentation. *[CISSP Domain 4: Communication and Network Security]*

6 Informational — informational messages *[Network Operations: Documentation, Monitoring, Resilience]*

6 Suitable insurance policies — inventory existing cover (damage, liability), then specific cyber cover; test it against your

scenarios before signing *[Digital Risk Governance - ANSSI-AMRAE 15 Steps]*

7 Debug — debug; never leave on in production (CPU) *[Network Operations: Documentation, Monitoring, Resilience]*

80 PLUS — Certification of PSU efficiency (DC output / AC input) at 20, 50 and 100 % load. *[Power, Displays, Peripherals and Printers]*

802.1X — IEEE port-based access control: the switch (authenticator) relays the device's EAP exchange to a RADIUS server before opening the port. *[Network Equipment Hardening]*

802.1X / EAP — Port-based access control: the access point relays EAP (Extensible Authentication Protocol) exchanges to a RADIUS server that authenticates each user or device. *[DNS, Wi-Fi & DDoS Architectures]*