



CompTIA CySA+ CS0-003

CompTIA Cybersecurity Analyst (CySA+) exam CS0-003 | Domain weights, objectives 1.1-4.2 explained, question formats, study plan, acronym drill

#CySAPlus

#SecurityAnalyst

#ExamOverview

#StudyPlan

Exam facts

CySA+ (Cybersecurity Analyst) is CompTIA's intermediate, vendor-neutral certification for the **defensive analyst**: the person in a SOC (Security Operations Center, the team that monitors and triages alerts 24/7) who reads logs, hunts threats, manages vulnerabilities, handles incidents and reports to management. It sits after Security+ and next to PenTest+ (the offensive counterpart).

85

questions maximum

multiple choice + PBQ
(performance-based question)

165 min

exam duration

about 1.9 min per question

750

passing score

on a scaled range of 100-900

3 years

validity

renew with 60 CEUs (continuing
education units)

Launched June 2023; the previous version CS0-002 retired December 2023. Its successor CS0-004 launched on 23 June 2026 (Security Operations 34 %, Vulnerability Management 26 %, Incident Response and Management 24 %, Reporting and Communication 16 %); CS0-003 retires on 22 December 2026 (confirm on comptia.org before booking)

Recommended Network+ and Security+ (or equivalent) plus 4 years hands-on as SOC or incident response analyst (a recommendation, not a prerequisite)

Languages English, Japanese, Portuguese, Spanish, Thai (check current list before booking)

Renewal 60 CEUs over 3 years (1 CEU is roughly 1 hour of training, a conference or a work task mapped to the objectives), the CertMaster CE (continuing education) course, or passing a higher CompTIA cert: CASP+ (CompTIA Advanced Security Practitioner, renamed SecurityX in 2024) or PenTest+

1. Security+
(foundation)

2. CySA+ (defend)

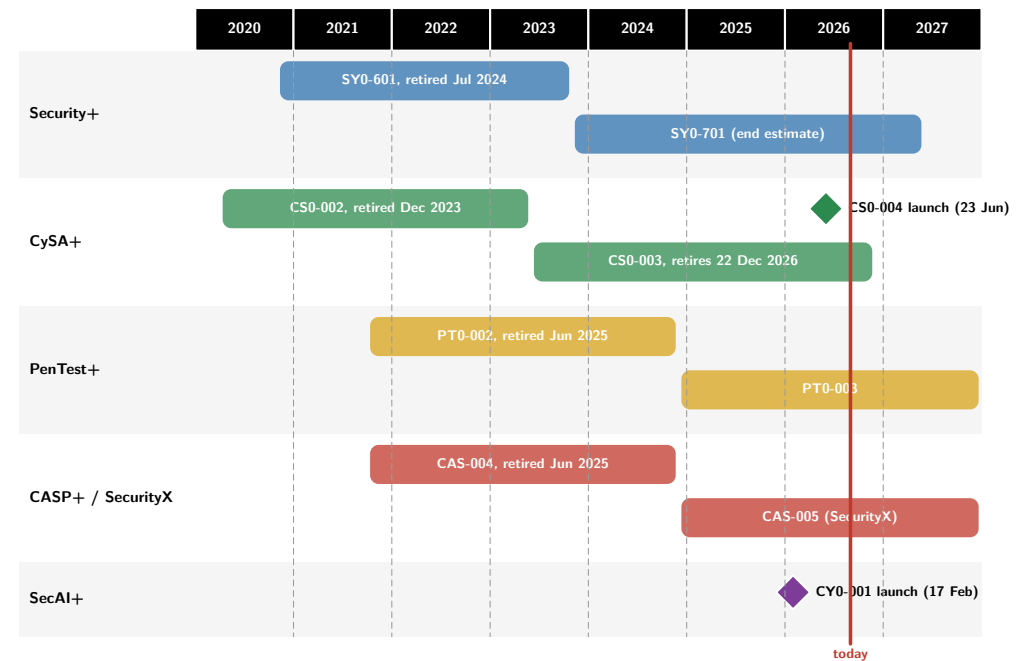
3. PenTest+ (attack)

4. SecurityX
(architect)

Where CySA+ sits in the CompTIA security path

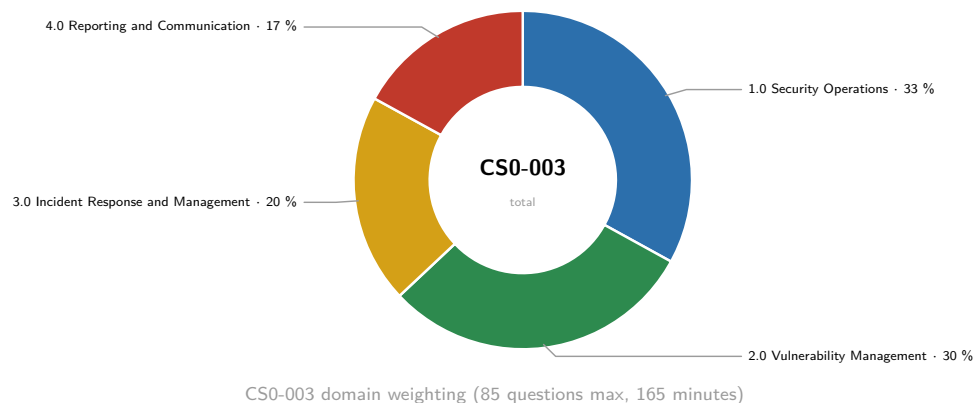
EXAM TIP

- Scores are scaled, not a percentage. No penalty for wrong answers: never leave a question blank. Unsourced trial questions are mixed in without any marking.
- When two answers seem right, prefer the one that adds context (asset value, exposure) or automation - the CS0-003 bias.



CompTIA cybersecurity exam versions: each bar starts at launch; the old version stays bookable until the retirement date shown (end dates marked estimate: confirm on comptia.org)

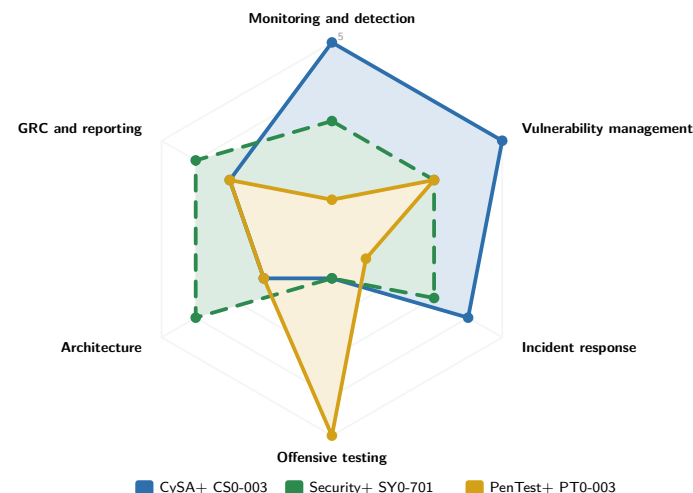
Domain weights



Mnemonic: **SVIR**

- S Security operations** 33 % - logs, indicators, tools, threat intel, efficiency
- V Vulnerability management** 30 % - scanning, CVSS, prioritization, mitigations, response
- I Incident response** 20 % - frameworks, detection, containment, preparation, post-incident
- R Reporting** 17 % - vulnerability and incident reports, metrics, stakeholders

CS0-002 (2020)	CS0-003 (2023)
5 domains	4 domains
Threat and Vulnerability Mgmt 22 %, Software and Systems Security 18 %	Security Operations 33 % absorbs monitoring, tools and threat intel
Security Ops and Monitoring 25 %, Incident Response 22 %	Vulnerability Management 30 % absorbs software security
Compliance and Assessment 13 %	Reporting and Communication 17 % (new focus on metrics, stakeholders)



Objective map

1.0 Security Operations 33 %

- 1.1 System and network architecture concepts
 - Log ingestion: time synchronization (NTP), logging levels
 - OS: Windows registry, hardening, file structure, config file locations, processes
 - Infrastructure: serverless, virtualization, containers; on-prem, cloud, hybrid
 - Network: segmentation, zero trust, SASE, SDN (software-defined networking)
 - IAM: MFA, SSO, federation, PAM, passwordless, CASB
 - Encryption: PKI, TLS inspection; data protection: DLP, PII, CHD
- 1.2 Analyze indicators of potentially malicious activity
 - Network: beaconing, bandwidth spikes, scans/sweeps, rogue devices, odd ports
 - Host: CPU/memory/disk anomalies, unauthorized software or changes, persistence
 - Application: anomalous activity, new accounts, unexpected output, service interruption
 - Other: social engineering, obfuscated links
- 1.3 Use tools and techniques to determine malicious activity
 - Tools: Wireshark/tcpdump (packet capture), SIEM, SOAR, EDR, DNS/IP reputation, sandbox
 - Techniques: pattern recognition, email header analysis, file hashing, user behavior analysis
 - Scripting and query languages: Python, PowerShell, shell, regex, JSON/XML
- 1.4 Threat intelligence and threat hunting
 - Actor types, TTP, confidence levels (timeliness, relevancy, accuracy)
 - Sources: open source, closed/proprietary, ISACs; information sharing
 - Hunting: IoC collection, focus areas (config, isolated networks, business-critical assets)
- 1.5 Efficiency and process improvement
 - Standardize processes, automate, orchestrate (SOAR), integrate tools, single pane of glass

2.0 Vulnerability Management 30 %

- 2.1 Vulnerability scanning methods and concepts
 - Asset discovery (map scans, fingerprinting); internal vs external scans
 - Agent vs agentless, credentialed vs non-credentialed, passive vs active
 - Static vs dynamic analysis (fuzzing, reverse engineering); OT/ICS/SCADA care

- Baselines and frameworks: PCI DSS, CIS Benchmarks, OWASP, ISO 27000
- 2.2 Analyze output from vulnerability assessment tools
 - Nmap, Angry IP Scanner, Maltego; Nessus, OpenVAS; Burp Suite, ZAP, Nikto
 - Debuggers (GDB, Immunity); Metasploit, Recon-ng; cloud: Scout Suite, Prowler, Pacu
- 2.3 Analyze data to prioritize vulnerabilities
 - CVSS base metrics; true/false positive and negative validation
 - Context (internal, external, isolated), exploitability, asset value, zero-day
- 2.4 Recommend controls to mitigate attacks and software vulnerabilities
 - XSS, overflows, injection, CSRF, SSRF, directory traversal, LFI/RFI, RCE
 - Broken access control, crypto failures, misconfiguration, outdated components
- 2.5 Vulnerability response, handling and management
 - Control types, compensating controls, patching, maintenance windows, exceptions
 - Risk treatment (accept, transfer, avoid, mitigate), SLOs, attack surface management
 - Secure coding, SDLC (software development life cycle), threat modeling

■ 3.0 Incident Response and Management 20 %

- 3.1 Attack methodology frameworks
 - Cyber Kill Chain, Diamond Model, MITRE ATT&CK, OSSTMM, OWASP Testing Guide
- 3.2 Perform incident response activities
 - Detection and analysis: IoC, evidence acquisition, chain of custody, legal hold
 - Containment, eradication, recovery: scope, impact, isolation, re-imaging
- 3.3 Preparation and post-incident activity phases
 - Preparation: IR plan, tools, playbooks, tabletop exercises, training, BC/DR
 - Post-incident: forensic analysis, root cause analysis, lessons learned

■ 4.0 Reporting and Communication 17 %

- 4.1 Vulnerability management reporting and communication
 - Reports (affected hosts, risk score, recurrence), compliance reports, action plans
 - Inhibitors to remediation: MOU, SLA, governance, legacy and proprietary systems
 - Metrics and KPIs: trends, top 10, critical vulnerabilities, zero-days, SLOs
- 4.2 Incident response reporting and communication
 - Stakeholders, incident declaration and escalation, report content and timeline
 - Communications: legal, public relations, regulators, law enforcement
 - Root cause, lessons learned, metrics: MTTD, MTTR, alert volume

SASE — Secure Access Service Edge: networking (SD-WAN) and security delivered together as a cloud service close to the user.

SSE — Security Service Edge: the security half of SASE (SWG + CASB + ZTNA), without the WAN part.

SWG — Secure Web Gateway: cloud or on-prem proxy that filters users' web traffic (URL categories, malware).

ZTNA — Zero Trust Network Access: per-application access granted after identity and device checks, replacing flat VPN access.

CASB — Cloud Access Security Broker: visibility and policy control over SaaS use (shadow IT, data sharing, DLP).

IAM / MFA / SSO — Identity and Access Management; Multifactor Authentication; Single Sign-On (one login, many applications).

PAM — Privileged Access Management: vaulting, just-in-time elevation and session recording for admin accounts.

PKI — Public Key Infrastructure: certificate authorities that issue and revoke the certificates behind TLS and signing.

DLP — Data Loss Prevention: detects and blocks sensitive data leaving by email, web, USB or cloud.

PII / PHI — Personally Identifiable Information (name + ID number, email...); Protected Health Information (medical data, HIPAA).

CHD / SAD — Cardholder Data (card number, name, expiry); Sensitive Authentication Data (CVV, PIN, track data), never stored after authorization under PCI DSS.

SIEM / SOAR / EDR — Security Information and Event Management (collect, correlate, alert); Security Orchestration, Automation and Response (playbooks); Endpoint Detection and Response.

ISAC — Information Sharing and Analysis Center: sector community that shares threat intelligence (FS-ISAC for finance, H-ISAC for health).

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.

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.

XSS / CSRF / SSRF — Cross-Site Scripting; Cross-Site Request Forgery; Server-Side Request Forgery (fixes in the sheet "Attack Mitigation and Vulnerability Response").

LFI / RFI / RCE — Local File Inclusion; Remote File Inclusion; Remote Code Execution.

OSSTMM — Open Source Security Testing Methodology Manual (ISECOM): a measured, repeatable security testing method.

BC/DR — Business Continuity / Disaster Recovery: keep critical functions running, then restore IT after a major outage.

MOU / SLA — Memorandum of Understanding (non-binding agreement); Service Level Agreement (contractual target, e.g. 99.9 % uptime).

MTTD / MTTR — Mean Time To Detect; Mean Time To Respond (or Remediate, Recover: read the stem). Lower is better.

PCI DSS — Payment Card Industry Data Security Standard (v4.0.1 current): mandatory controls for anyone storing, processing or transmitting card data.

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.

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.

📖 Question formats

✓ Single-answer multiple choice

Most questions. Stem asks for BEST, MOST likely, FIRST or NEXT. Eliminate answers that skip a phase.

☰ Multiple response

"Select TWO" - both must be right for credit. Usually pairs a control with its detection or a tool with its output.

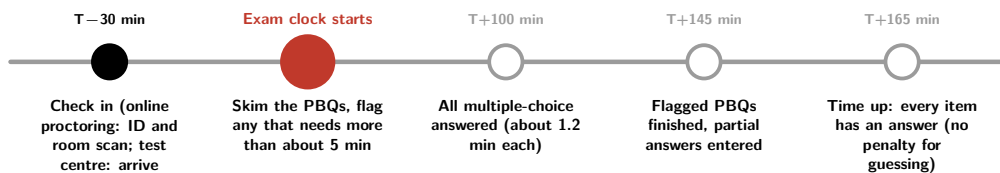
Performance-based (PBQ)
Simulations and drag-and-drop, typically at the start.
Log analysis, scan interpretation, ordering IR steps, matching attack to mitigation.

Exhibit questions
A log line, Nmap or Nessus output, email header or CVSS vector is shown; you identify the indicator or the priority.

Typical PBQ	What you must do
Firewall or proxy log	Spot beaconing (regular small call-backs to a command-and-control server), a port scan or exfiltration (large outbound transfer); pick the source IP to block
Windows Security log	Match event IDs to the story: 4624 successful logon (with its logon type: 2 interactive, 3 network, 10 RDP), 4625 failed logon (many = brute force), 4688 new process created, 4720 user account created (possible persistence)
Nmap / Nessus output	Identify open service, version and its CVSS score; rank remediation order
Email header	Read the Received chain bottom-up (oldest hop at the bottom); interpret SPF (is the sending IP allowed for the domain?), DKIM (is the signature valid?), DMARC (does the visible From domain align, and what policy applies?)
Vulnerability list with context	Prioritize by exploitability, internet exposure and asset value, not raw CVSS
IR phase ordering	Drag activities into the NIST SP 800-61 (Computer Security Incident Handling Guide) phases: Preparation → Detection and Analysis → Containment, Eradication and Recovery → Post-incident activity

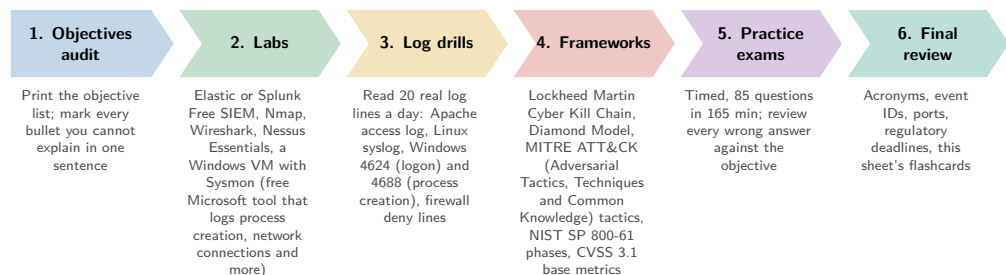
⚠ WARNING

PBQs are not weighted more than other questions but consume time. If one will take more than about 5 minutes, flag it, finish the multiple choice, then return with the remaining minutes; never leave it blank (partial credit is widely reported, not officially documented).



Illustrative pacing plan for 85 questions in 165 minutes: bank time on multiple choice, spend it on flagged PBQs, never submit a blank

🕒 Study plan



Six-week plan for candidates with Security+ background

📄 INFO

The exam was written against **CVSS 3.1** and the four-phase **NIST SP 800-61 r2 (2012)**. In April 2025 NIST published SP 800-61 r3, which maps incident response onto the six NIST CSF 2.0 functions (Govern, Identify, Protect, Detect, Respond, Recover), and FIRST released CVSS 4.0 in November 2023. Answer with the older models on the exam; know the new ones for work.

Ready-for-exam checklist

✓ non-negotiable before booking, □ strongly recommended

- ✓ Explain every objective bullet without notes
- ✓ Score 85 %+ on two different practice exams
- ✓ Read a Windows 4624 (successful logon) event and name the logon type (2 console, 3 network share, 10 RDP)
- **SHOULD** Compute a CVSS 3.1 base score from a vector such as AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (= 9.8)
- **MUST** Order the NIST 800-61 phases and the 7 Kill Chain steps (Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Actions on Objectives) from memory
- **SHOULD** Write a beaconing, brute-force and top-talker (hosts sending the most bytes) query in one SIEM
- **COULD** Name the notification deadlines: GDPR (EU data protection) 72 h to the authority; HIPAA (US health data) 60 days to individuals; NIS2 (EU directive for essential entities) 24 h early warning, 72 h notification

📖 Acronym drill

Q1 SIEM vs SOAR

A Security Information and Event Management aggregates, correlates and alerts; Security Orchestration, Automation and Response runs the response playbook across tools

Q2 EDR vs XDR

A Endpoint Detection and Response = endpoint telemetry and host containment; Extended Detection and Response correlates endpoint, network, identity, cloud and email

Q3 TTP

A Tactics (why: the goal, e.g. persistence), Techniques (how: e.g. registry Run key), Procedures (exact implementation by one group) - ATT&CK vocabulary

Q4 IoC vs IoA

A Indicator of Compromise = artefact after the fact (hash, IP); Indicator of Attack = behaviour in progress

Q5 CVSS, EPSS, KEV

A Common Vulnerability Scoring System = severity 0-10 (FIRST); Exploit Prediction Scoring System = probability 0-1 of exploitation in the next 30 days (FIRST); Known Exploited Vulnerabilities = CISA catalog of flaws exploited in the wild

Q6 MTTD, MTTR

A Mean time to detect; mean time to respond (or restore/remediate - read the question)

Q7 SLO vs SLA

A Service level objective = internal target (patch criticals in 15 days); SLA = contractual commitment

Q8 STIX / TAXII

A Structured Threat Information Expression = JSON format for threat intel objects; Trusted Automated Exchange of Intelligence Information = HTTPS protocol that transports it (both OASIS standards)

Q9 TLP

A Traffic Light Protocol v2.0 (sharing labels): RED named recipients only, AMBER+STRICT own organization only, AMBER organization and its clients, GREEN community, CLEAR public

Q10 FIRST, CISA, OASIS

A Forum of Incident Response and Security Teams; US Cybersecurity and Infrastructure Security Agency; standards consortium (Organization for the Advancement of Structured Information Standards)

Discriminator pairs the exam loves

Pair	Tell them apart by	Where
Beaconing vs bandwidth spike	Regular small check-ins (C2) vs large irregular volume (exfiltration, DDoS)	1.2
Scan vs sweep	Many ports on one host vs one port or ping across many hosts	1.2
IoC vs IoA	Artefact left behind (hash, IP) vs behaviour in progress (technique)	1.4

Strategic vs operational vs tactical intel	Trends for executives vs campaigns and TTPs for SOC leads vs indicators for tools	1.4
Automation vs orchestration	One task scripted vs several tools chained into a playbook	1.5
Credentialed vs agent-based scan	Remote login at scan time vs software on the host reporting continuously	2.1
Passive vs active scanning	Observe traffic (safe for OT, fragile industrial systems) vs send probes (accurate, riskier)	2.1
False positive vs false negative	Reported but absent vs present but missed (the dangerous one)	2.3
Reflected vs persistent XSS (cross-site scripting)	Payload in the request, one victim per click vs stored on the server, hits every visitor	2.4
LFI vs RFI (local / remote file inclusion)	App includes a file already on the server (.././etc/passwd) vs fetches code from an attacker URL; fix both with an allow-list of files	2.4
Compensating vs corrective control	Stands in for a fix you cannot apply vs repairs after the event	2.5
Kill Chain vs ATT&CK vs Diamond	Seven linear phases vs technique knowledge base vs four-vertex analysis model	3.1
Containment vs eradication	Stop the spread vs remove the cause	3.2
MTTD vs MTTR	Time to notice vs time to respond (contain)	4.2

TIP

When two answers look right, the discriminator in the stem decides: the **interval** (regular = beacon), the **audience** (executive = strategic), the **phase** (spreading = contain first) or the **exposure** (internet-facing first). The sheet “CySA+ Practice Scenarios” drills these pairs as scenario cards.

Reading the question stem

✓ Do

- + Underline FIRST, NEXT, BEST, MOST likely: they ask for order or ranking
- + Locate the IR phase you are in before choosing an action
- + Prefer the answer that uses context (asset value, exposure, business impact)
- + Prefer containment that preserves evidence (isolate) over destroying it (wipe)

✗ Avoid

- Picking a technically true answer that skips a phase
- Ranking vulnerabilities by raw CVSS alone
- Answering from your own company’s tooling instead of the vendor-neutral concept
- Changing answers without a concrete reason

Three CS0-003-style items

1 A proxy log shows host 10.0.4.23 sending 350-byte HTTPS requests to one domain every 60 s (plus or minus 2 s) for 9 hours. MOST likely activity?

- ☐ A Data exfiltration
- ☒ B Command-and-control beaconing
- ☐ C Port scan
- ☐ D DDoS participation

→ Small, regular check-ins = beaconing; exfiltration is large and irregular volume.

2 CVSS 9.1 on an isolated lab server vs CVSS 7.5 on an internet-facing VPN appliance listed in CISA KEV (Known Exploited Vulnerabilities). Which is fixed FIRST?

- ☐ A The lab server (higher score)
- ☒ B The KEV-listed VPN appliance
- ☐ C Both in the next monthly window
- ☐ D Neither: accept the risk

→ Exploited in the wild + internet exposure beat raw CVSS (objective 2.3 context).

3 Ransomware is encrypting file shares from one workstation. What should the analyst do FIRST?

- ☐ A Re-image the workstation
- ☒ B Isolate the workstation with the EDR
- ☐ C Restore the shares from backup
- ☐ D Draft the lessons-learned report

→ Containment precedes eradication and recovery; EDR isolation also keeps memory evidence.

Worked exam items: the discriminator in each stem (interval, exposure, phase) selects the answer