



SCS-C03 Domain 1: Detection, Monitoring and Logging

AWS Certified Security - Specialty SCS-C03 exam guide, Domain 1 (16 %) | GuardDuty, Security Hub, Inspector, Macie, Config, CloudTrail, VPC Flow Logs, Security Lake, CloudWatch; analysis and troubleshooting

SCS-C03 Domain 1 Detection Logging

What Domain 1 tests

Task (SCS-C03)	What you must be able to do	Services the exam names
1.1 Monitoring and alerting for an account or organisation	analyse a workload's monitoring needs, health checks, aggregate events, metrics, alerts, dashboards, automated assessments	GuardDuty, Security Hub, Security Lake, Macie, Config conformance packs, SSM State Manager
1.2 Logging	pick log sources, configure an organisation trail and a dedicated logging account, the CloudWatch agent, a log data lake, analysis and correlation	CloudTrail, CloudWatch Logs, Logs Insights, Athena, OpenSearch, Managed Grafana, Flow Logs, Route 53 Resolver logs
1.3 Troubleshoot monitoring and logging	find why logs or alerts are missing: permissions, configuration, agents	Lambda and API Gateway logging, CloudFront logs, CloudWatch agent

INFO

SCS-C02 put detection and incident response together (Domain 1) and logging in Domain 2. SCS-C03 splits them into **Detection** (16 %) and **Incident Response** (14 %, next sheet). The ASFF (AWS Security Finding Format) left the task list, but Security Hub still uses it: know it exists.

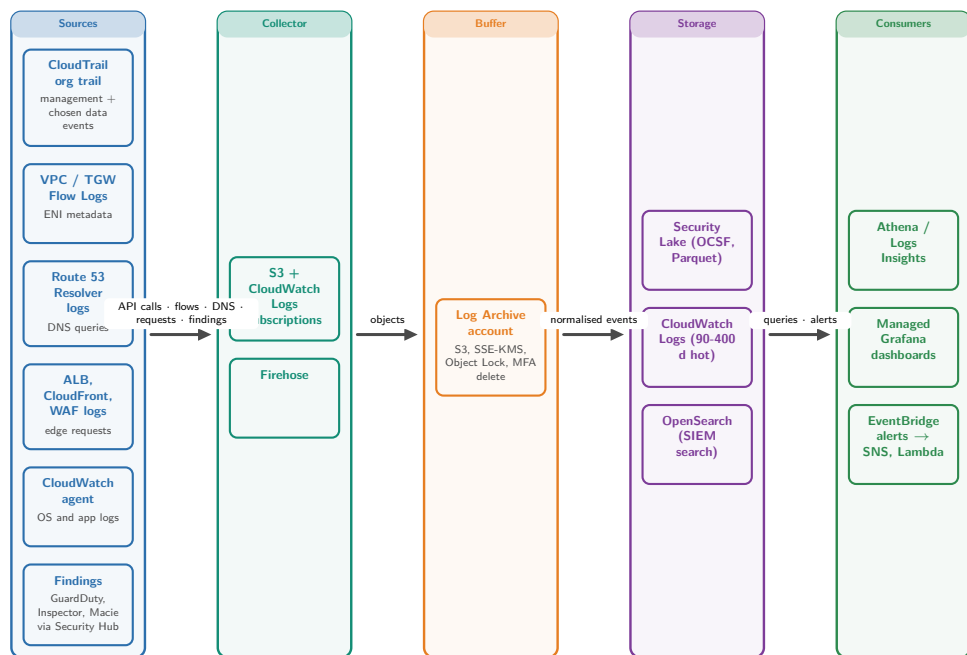
The detection services, one line each

Service	Detects or records	Scope and key facts
GuardDuty	threats: compromised credentials, crypto-mining, C2 traffic, recon, exfiltration	regional; reads CloudTrail management events, VPC Flow Logs and DNS logs on its own copy (no need to enable them); org-wide via delegated admin; 30-day free trial
Security Hub	aggregated findings + posture checks (CIS AWS Foundations, AWS Foundational Security Best Practices, PCI DSS, NIST SP 800-53)	needs AWS Config recording for its checks; cross-region aggregation to one home region; automation rules; 2025 relaunch adds exposure findings and correlation (posture checks are now Security Hub CSPM)
Inspector	software vulnerabilities (CVE) and unintended network reachability	EC2 (SSM agent or agentless snapshot scan), ECR images, Lambda functions and code; Inspector risk score
Macie	sensitive data (PII, credentials, financial) and S3 bucket posture	managed + custom data identifiers; automated sensitive data discovery samples every bucket

Config	resource configuration history and compliance with rules	configuration recorder per region; managed or custom (Lambda, Guard) rules; aggregator across accounts and regions
CloudTrail	who called which API, when, from where	90 days of management events free in Event history; trails for longer; data events and network activity events opt-in
Detective	investigation, not detection: entity behaviour graph	up to a year of data; pivots from a GuardDuty or Security Hub finding
IAM Access Analyzer	resources shared outside your zone of trust, unused access, policy validation	external access analyzer (account or organisation), unused access analyzer (paid), custom policy checks

- **GuardDuty protection plans** S3 Protection (S3 data events), EKS Protection (audit logs), Runtime Monitoring (agent for EKS, ECS on Fargate and EC2), Malware Protection for EC2 (EBS snapshot scan on finding) and for S3 (scan new objects), RDS Protection (Aurora login anomalies), Lambda Protection (network activity)
- **Extended Threat Detection** GuardDuty correlates signals over time into attack sequence findings (critical severity) covering several MITRE ATT&CK tactics
- **Finding severity** GuardDuty 1.0-8.9 (low < 4, medium 4-6.9, high 7-8.9) and critical 9-10 for attack sequences; suppression rules archive expected findings; trusted IP and threat lists

A central logging architecture



Control Tower's default: Log Archive account for logs, Audit (security tooling) account for delegated admins

Log source	Default	Destinations	Trap
CloudTrail management events	on (Event history, 90 d)	trail → S3, CloudWatch Logs; Lake	Event history is not exportable for long-term retention: create a trail
CloudTrail data events	off	trail or event data store	S3 object-level reads are only here (or in S3 server access logs)
VPC Flow Logs	off	CloudWatch Logs, S3, Firehose	no payload; skips Amazon DNS, DHCP, 169.254.169.254 metadata, time sync, license activation
Route 53 Resolver query logs	off	CloudWatch Logs, S3, Firehose	only queries through the VPC resolver; share configs with AWS RAM
ELB access logs	off	S3 only	bucket policy must allow the ELB log delivery principal
CloudFront standard logs	off	S3, CloudWatch Logs, Firehose (v2 logging)	real-time logs go to Kinesis Data Streams
AWS WAF logs	off	CloudWatch Logs, S3, Firehose	name must start with aws-waf-logs-
S3 server access logs	off	S3 (other bucket)	best effort, hours of delay; CloudTrail data events are the audit-grade option
API Gateway execution / access logs	off	CloudWatch Logs, Firehose	REST APIs need the account-level CloudWatch role ARN set first
Lambda logs	on	CloudWatch Logs	execution role needs logs:CreateLogStream and logs:PutLogEvents

Organisation trail and alerts as code

Command	Effect
<code>aws cloudtrail create-trail --name org-trail --s3-bucket-name log-archive-ct --is-organization-trail --is-multi-region-trail --enable-log-file-validation --kms-key-id alias/ct</code>	one trail for all accounts and regions, digest files on, SSE-KMS
<code>aws cloudtrail put-event-selectors --trail-name org-trail --advanced-event-selectors file://s3-data.json</code>	add S3 data events for selected buckets only (cost control)
<code>aws cloudtrail validate-logs --trail-arn ARN --start-time 2026-10-01T00:00:00Z</code>	prove no log file was changed or deleted
<code>aws guardduty enable-organization-admin-account --admin-account-id 111122223333</code>	delegate GuardDuty to the Audit account (run from the management account)
<code>aws securityhub create-finding-aggregator --region-linking-mode ALL_REGIONS</code>	aggregate findings of every region into the current one

EventBridge pattern: high and critical GuardDuty findings

```
{
  "source": ["aws.guardduty"],
  "detail-type": ["GuardDuty Finding"],
  "detail": { "severity": [{ "numeric": [">=", 7] }] }
}
```

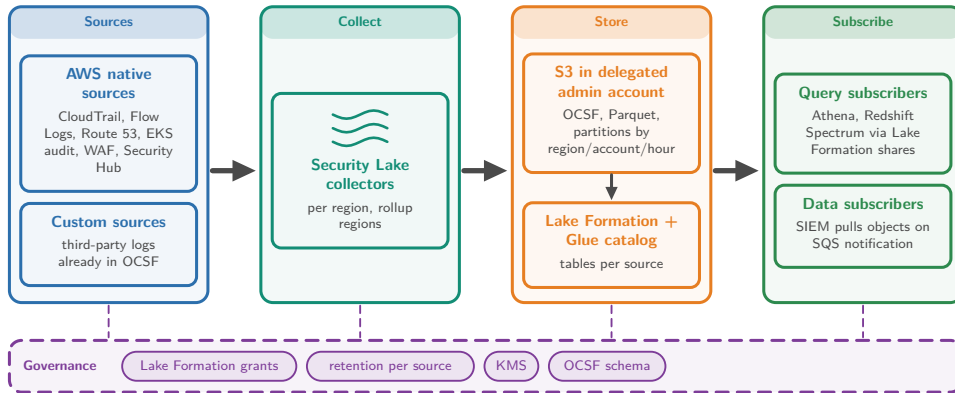
Logs Insights: console sign-ins without MFA

```
fields @timestamp, userIdentity.arn, sourceIPAddress
| filter eventName = "ConsoleLogin"
| filter additionalEventData.MFAUsed = "No"
| stats count(*) by userIdentity.arn, sourceIPAddress
| sort count(*) desc
```

CIS alarms in three steps

CloudTrail → CloudWatch Logs group; `aws logs put-metric-filter` with a pattern such as `{ $.userIdentity.type = "Root" && $.eventType != "AwsServiceEvent" }`; `aws cloudwatch put-metric-alarm` on that metric (threshold ≥ 1 , period 300 s) → SNS. Security Hub CSPM control CloudWatch.1 checks that this exists.

Security Lake and detection content



Root user activity

HIGH

T1078.004 CLOUD ACCOUNTS

SOURCE CloudTrail management events (org trail)

LOGIC `userIdentity.type = Root AND eventType != AwsServiceEvent`

FIRES ON any console sign-in or API call by a root user

FALSE +

- documented break-glass test
- root-only tasks such as closing an account

RESPOND

- confirm with the account owner
- rotate root password, check MFA device
- review the session's API calls in Detective

TUNING with centralised root access, members should have no root credentials at all

Instance credentials used outside AWS

HIGH

T1552.005 CLOUD INSTANCE METADATA

SOURCE GuardDuty finding UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

LOGIC EC2 role session credentials seen from an IP not owned by AWS

FIRES ON stolen IMDS credentials (SSRF, compromised host)

FALSE +

- rare: credentials copied to a developer laptop

RESPOND

- revoke sessions: deny policy with `aws:TokenIssueTime`
- enforce IMDSv2
- isolate and snapshot the instance

Troubleshooting missing logs and alerts

Organisation trail writes no files to the Log Archive bucket

HIGH

LIKELY CAUSES

- Bucket policy lacks `cloudtrail.amazonaws.com PutObject` with `aws:SourceArn` of the trail
- KMS key policy does not let CloudTrail use the key (GenerateDataKey*)
- SCP or bucket Object Ownership blocks the write

HOW TO CONFIRM

Trail status shows LatestDeliveryError

```
aws cloudtrail get-trail-status --name org-trail
```

FIX

- ✓ Add the CloudTrail statements to bucket and key policies
- ✓ Re-check delivery after 15 minutes

EC2 application logs never reach CloudWatch Logs

MEDIUM

LIKELY CAUSES

- Instance profile lacks `CloudWatchAgentServerPolicy`
- Agent config wrong path or not loaded
- No route to logs endpoint (private subnet without NAT or interface endpoint)

HOW TO CONFIRM

Read the agent's own log and status

```
amazon-cloudwatch-agent-ctl -a status; tail /opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
```

FIX

- ✓ Attach the managed policy
- ✓ Store config in SSM Parameter Store and fetch-config
- ✓ Add a logs interface endpoint

REST API in API Gateway produces no execution logs

LOW

LIKELY CAUSES

- Account setting CloudWatch log role ARN not set
- Stage logging level OFF

HOW TO CONFIRM

Stage settings and account settings

```
aws apigateway get-account
```

FIX

- ✓ Set `cloudwatchRoleArn` with `AmazonAPIGatewayPushToCloudWatchLogs`
- ✓ Enable INFO or ERROR logging on the stage

📊 Sizing the log archive

PROBLEM A 40-account organisation produces 120 GB of CloudTrail, Flow Logs and DNS logs per day. Policy: 30 days hot for investigations, 400 days total retention, Athena queries usually cover one day. How much is stored and how much does a query scan?

GIVEN

- ingest $D = 120$ GB/day
- hot window $H = 30$ days
- retention $R = 400$ days
- query window $Q = 1$ day

1 Total stored at steady state

$$D \times R = 120 \times 400 = 48,000 \text{ GB} = 48 \text{ TB}$$

Why: each day's logs are kept R days

2 Hot share (S3 Standard)

$$D \times H = 120 \times 30 = 3,600 \text{ GB} = 3.6 \text{ TB}$$

Why: lifecycle moves objects older than 30 days

3 Cold share (Glacier Instant Retrieval)

$$48,000 - 3,600 = 44,400 \text{ GB}$$

Why: still millisecond reads for audits

4 Scan per query with partitions (date)

$$D \times Q = 120 \text{ GB}$$

Why: partition projection on the date prefix

5 Scan per query without partitions

$$48,000 \text{ GB, 400 times more}$$

Why: Athena bills per TB scanned

ANSWER 48 TB retained (3.6 TB hot, 44.4 TB cold); a partitioned one-day query scans 120 GB instead of 48 TB

CHECK ✓ $3.6 + 44.4 = 48$ TB; Parquet (Security Lake) shrinks the scan further

🚩 Myths, recap, self-test

MYTH

✗ GuardDuty needs VPC Flow Logs and DNS logging enabled first

FACT

✓ GuardDuty reads its own independent stream of these sources
Enable Flow Logs for your own investigations and retention, not for GuardDuty.

✗ CloudTrail Event history is my audit archive

✓ Event history keeps 90 days of management events only
Use an organisation trail to S3 or CloudTrail Lake for longer retention and data events.

✗ Security Hub detects threats by itself

✓ Security Hub aggregates findings and runs posture checks
Threat detection comes from GuardDuty, Inspector, Macie and partners feeding it.

✗ Flow Logs show which URL was requested

✓ Flow Logs carry metadata only, no payload or host name
Use ALB, CloudFront or WAF logs for URLs, Route 53 Resolver logs for names, Traffic Mirroring for packets.

Key takeaways

01

Delegate, then aggregate

GuardDuty, Security Hub, Inspector, Macie, Detective admin in the Audit account; findings to one region

02

One organisation trail

multi-region, log file validation, SSE-KMS, Log Archive bucket with Object Lock

03

Know what each log cannot see

Flow Logs no payload, S3 reads only in data events, ELB logs to S3 only

04

Alert through EventBridge

finding pattern → SNS, Lambda, Step Functions

05

Missing logs = permissions first

bucket policy, KMS key policy, role, then config

Q1 Which CloudTrail feature proves a log file was not tampered with?

A Log file integrity validation: hourly SHA-256 digest files signed with RSA; check with `aws cloudtrail validate-logs`.

Q2 Where do you see who downloaded an object from an S3 bucket?

A CloudTrail data events for S3 (GetObject), or S3 server access logs; management events do not include it.

Q3 GuardDuty must cover all current and future accounts. How?

A Delegated administrator from the management account, then auto-enable for the organisation (ALL members) in every region.

Q4 Which service normalises logs to OCSF in your own S3 buckets?

A Amazon Security Lake.

Q5 Security Hub shows no CIS check results. First thing to check?

A AWS Config recording is enabled in that account and region (Security Hub CSPM checks rely on Config).

Q6 WAF logging to Firehose fails with an invalid name. Why?

A The delivery stream (or log group or bucket) name must start with `aws-waf-logs-`.

Q7 Find unusual spikes of IAM write API calls without writing rules?

A CloudTrail Insights on the trail (API call rate and error rate insights).

Q8 Run the same Config rules and remediations in every account at once?

A An organisation conformance pack deployed from the management or delegated admin account.

Q9 Which DNS queries do Route 53 Resolver query logs miss?

A Queries that do not go through the VPC resolver, for example an instance using its own external DNS server.