AWS Certified Security - Specialty Cheat Sheet

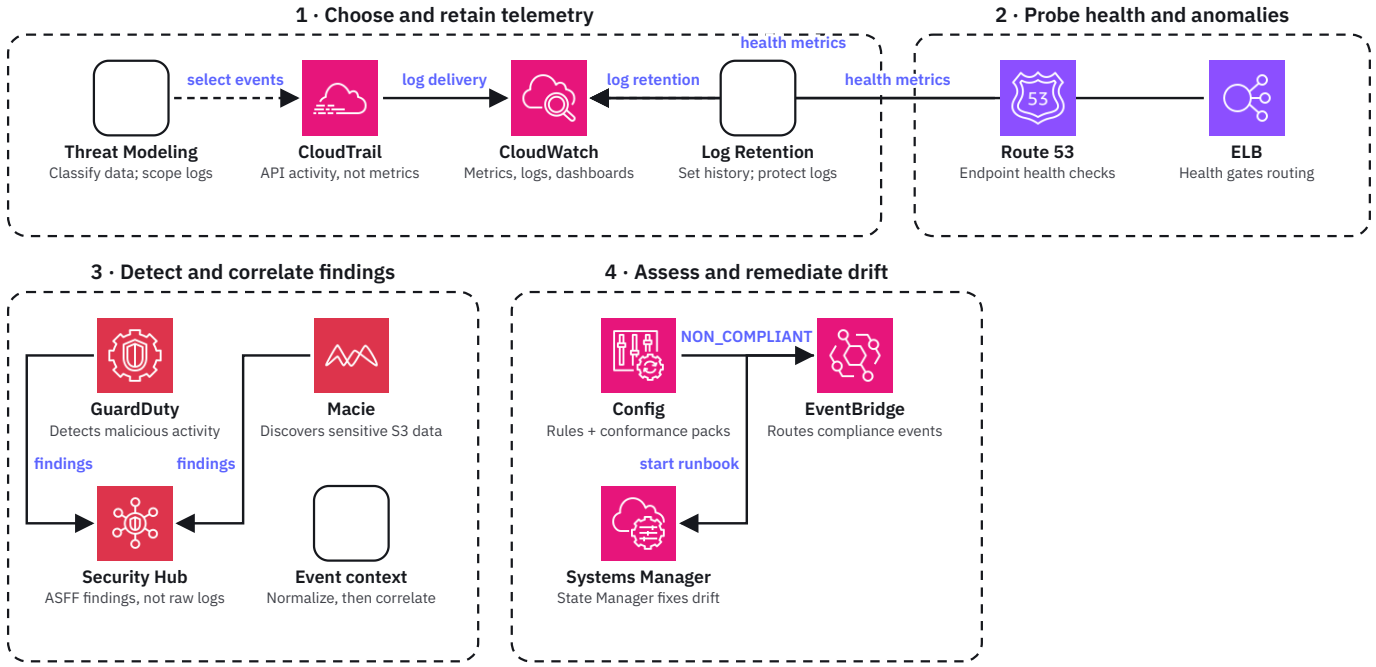
SCS-C03 · Domain 1 of 6

BlowStack

DOMAIN 1 · DETECTION · 16% OF THE EXAM · TASK STATEMENT 1.1

Design and implement monitoring and alerting solutions for an AWS account or organization

Scope, monitor, correlate, remediate



1 Choose and retain telemetry

Threat Modeling and Data Classification determine audit events, metrics, and response urgency. Set Log Retention explicitly; CloudWatch Logs retains indefinitely by default.

2 Probe health and anomalies

CloudWatch alarms evaluate metrics; Anomaly Detection uses a learned baseline. Route 53 checks endpoint availability; ELB health checks determine target eligibility for routing.

3 Detect and correlate findings

AWS Security Hub aggregates findings in ASFF, not raw logs. Log Normalization aligns event fields; Event Correlation links account, identity, resource, and time to reconstruct activity.

4 Assess and remediate drift

Configuration Drift requires assessment and enforcement. Config conformance packs bundle rules and optional remediation; State Manager reapplies desired state. EventBridge can trigger Automation runbooks.

Exam traps

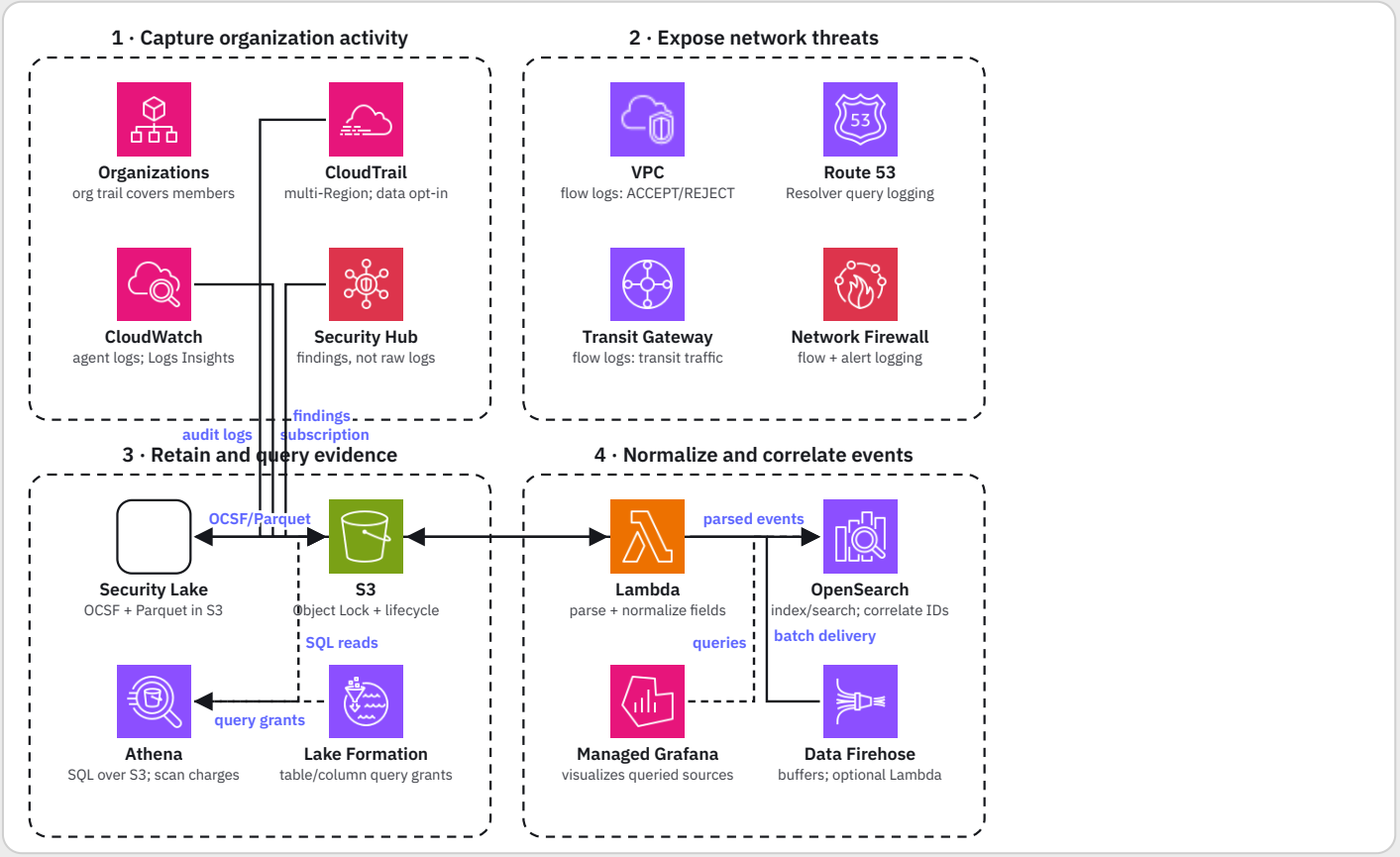
- **CloudTrail to CloudWatch Logs** requires configured delivery; it is not automatic. Metric filters turn matching log events into metrics; alarms evaluate those metrics.
- **Noncompliant is not remediated**: a Config evaluation or Security Hub finding reports a condition. Correction requires configured remediation or another explicit action.
- **Organization-wide is not automatic**: configure member coverage and supported Region aggregation. Enabling a detector in one account and Region does not cover the organization.

Get practice exams and lessons for AWS Certified Security - Specialty

DOMAIN 1 · DETECTION · TASK STATEMENT 1.2

Design and implement logging solutions

Capture, retain, query, correlate



1 Capture organization activity

Use an **organization trail** for member-account API auditing; enable data events explicitly. CloudWatch agents collect guest/app logs; cross-account observability shares views, not stored copies.

2 Expose network threats

Select telemetry by **threat model**: Resolver queries expose DNS tunneling; east-west flow logs support lateral-movement analysis. Enable firewall alert logs for inspected threats; AWS WAF logs capture web requests.

3 Retain and query evidence

Retention: lifecycle tiers/expires objects; Object Lock compliance prevents early deletion. Security Lake normalizes supported AWS sources and authorizes subscribers. Residency includes rollup and subscriber Regions.

4 Normalize and correlate events

Normalize identities, fields, and UTC timestamps before correlation. Use **event time**, not arrival time; account for clock skew and delivery delays. Firehose supports Lambda transformation and third-party destinations.

Exam traps

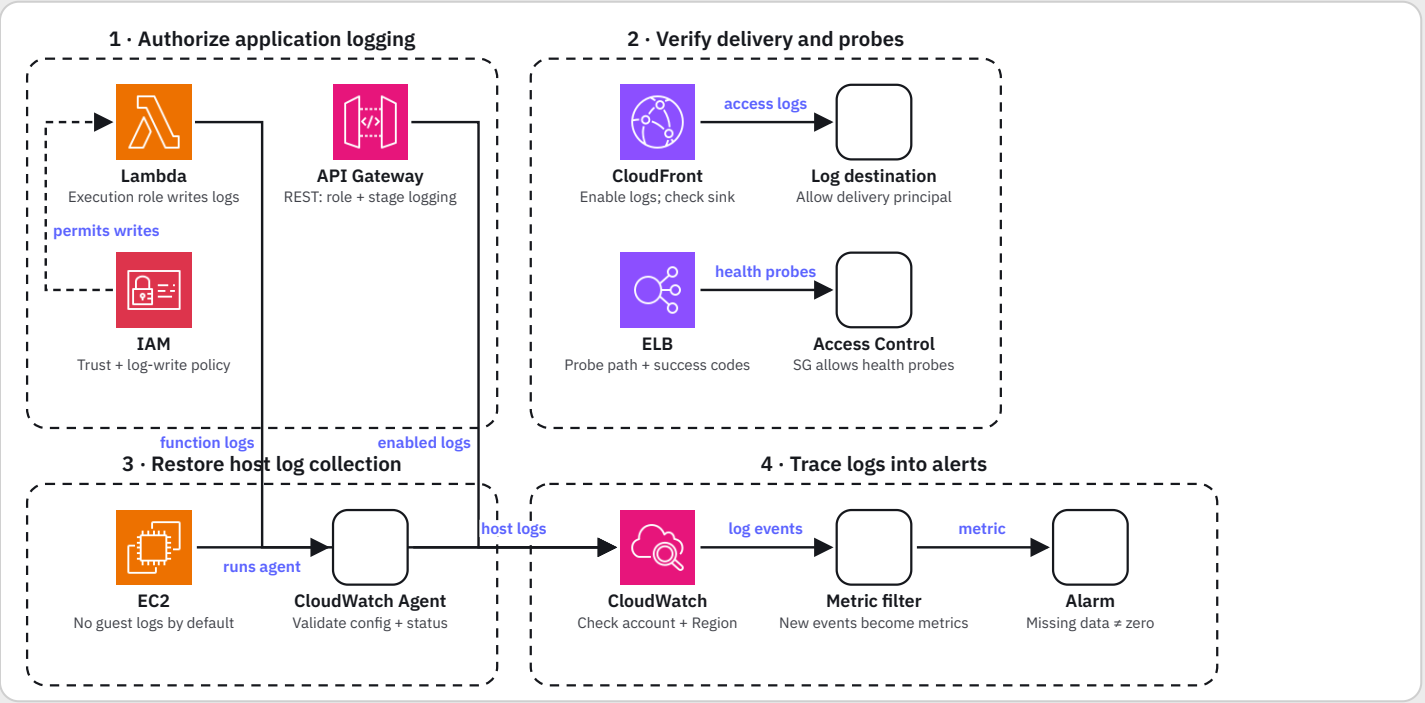
- **Event history ≠ trail**: CloudTrail event history gives 90 days of regional management events, not data events or durable organization-wide retention.
- **Integrity ≠ immutability**: CloudTrail digest validation detects changes; it does not prevent deletion. S3 versioning alone is not WORM; use Object Lock with protected retention.
- **Flow logs ≠ packet capture**: VPC/transit gateway logs show metadata, not payloads or DNS names. Resolver logs expose DNS behavior; correlate identity and network logs for lateral movement.

Get practice exams and lessons for AWS Certified Security - Specialty

DOMAIN 1 · DETECTION · TASK STATEMENT 1.3

Troubleshoot security monitoring, logging, and alerting solutions

Authorize, deliver, inspect, alert



1 Authorize application logging

Missing application logs: verify the **logging role**. Lambda needs execution-role log permissions; REST API execution logging needs an account-level regional role and stage logging settings.

2 Verify delivery and probes

Missing CloudFront logs: check logging and destination permissions. For **unhealthy targets**, check security groups, probe port/path, and success codes; access logging does not enable health checks.

3 Restore host log collection

For **missing host logs**, check agent installation/status, active configuration, file paths/read access, destination Region, instance-profile permissions, and outbound HTTPS access to logging endpoints.

4 Trace logs into alerts

When logs exist but alerts do not, inspect filter patterns, metric dimensions, alarm state, and enabled actions. **Missing-data treatment** is configurable; absent datapoints do not automatically mean zero.

Exam traps

- **EC2 detailed monitoring** increases instance-metric frequency; it does not collect guest logs. Guest-log collection requires a configured, running agent with publishing permissions.
- **API Gateway execution logging** applies to REST APIs; HTTP APIs support access logging, not execution logging. Enabling access logging does not enable execution logging.
- **Metric filters do not backfill** historical logs. A newly created filter processes newly ingested events; old matching events alone cannot produce its alarm metric.

Get practice exams and lessons for AWS Certified Security - Specialty

DOMAIN 1 · DETECTION · WHAT TO REMEMBER

Concepts and services of Detection

Concepts to know

Audit Logging

Audit records establish who acted, when, on which resource, and with what outcome. **Choose complementary log sources**: API activity, network flows, DNS queries, and application events provide different evidence.

Event Correlation

Correlation links records into an incident sequence using identities, resources, addresses, and timestamps. **Distinguish findings aggregation from raw-log analysis**; centralized findings do not replace the underlying evidence.

Log Retention

Retention determines how long evidence remains available. **Match retention and retrieval to investigation and compliance needs**; archival storage reduces cost, while immutability separately protects records from deletion or replacement.

Core services



Amazon CloudWatch

Choose **metrics, alarms, and Logs Insights** for operational detection and log queries. Missing host logs require checking agent configuration, permissions, connectivity, and destination Region.



AWS CloudTrail

Choose an **organization trail** for ongoing multi-account API auditing. Event history covers 90 days of management events per Region; data events require explicit selection.



AWS Security Hub

Choose **centralized findings and security posture checks** across accounts and Regions. It aggregates findings rather than raw logs; Amazon Security Lake normalizes supported security telemetry.

Get practice exams and lessons for AWS Certified Security - Specialty