AWS Incident Detection and Response

SEC404

Investigate and respond to attacks in AWS using the evidence the platform records: CloudTrail, GuardDuty, VPC Flow Logs, and AWS Config. From a leaked access key through privilege escalation, persistence, and data exfiltration to full containment.

Modules	20
Lessons	150
Phases	6
Free preview	Course Orientation (7 lessons)

The method

An AWS investigation is bounded by what the account was configured to log before anything happened. This course runs the same loop for every attack path it covers.

1. Establish what this account records. CloudTrail coverage, data events, VPC flow logs and GuardDuty are each a decision somebody made or did not make. That decision is your evidence ceiling.

2. Query at scale, not by hand. A busy account produces more CloudTrail than a console will show you. Learning to query the evidence is what makes the rest of the course possible.

3. Follow the identity, because everything is one. Users, roles, instance profiles and assumed sessions. Nearly every AWS attack path is an identity moving somewhere it should not.

4. Separate what was reached from what was taken. S3 access patterns and API calls tell you different things, and conflating them is how exfiltration figures get overstated.

5. Contain without destroying the evidence. Revoking a session, detaching a policy and terminating an instance have very different consequences for the investigation still running.

The course closes on a full-chain cloud incident worked end to end.

What this course assumes

No minimum experience and no prerequisite course. IAM, the log sources and the AWS service model are explained where they first matter, and the course does not assume you administer AWS.

What makes it go faster: an AWS account you can read CloudTrail in. Not required, because every query in the course runs against the AWS Query Lab, which holds a real corpus with known answers.

What this course does not cover: AWS administration, cloud architecture and Azure or GCP. This is detection and incident response inside AWS.

Full syllabus

Phase 1: Foundations

Course Orientation FREE PREVIEW

What AWS Incident Detection and Response teaches: take an unknown AWS account, pull the right logs, and reconstruct an intrusion from first access to impact, then contain it.

1. AWS0.1 Purpose and Scope
2. AWS0.2 Getting the Most from This Course
3. AWS0.3 The Control Plane Is the Crime Scene
4. AWS0.4 Ephemeral by Design
5. AWS0.5 Identity Is the Perimeter
6. AWS0.6 The Threats You'll Learn to Catch
7. AWS0.7 Course Toolkit and Environment

The AWS Detection and IR Landscape

Where AWS evidence lives, the shared responsibility line for incident response, the Northgate AWS Organization and the vantage point you investigate from, and your first queries against real CloudTrail.

1. AWS1.1 Shared Responsibility for Incident Response
2. AWS1.2 The AWS Organization and Your Vantage Point
3. AWS1.3 CloudTrail, the Spine
4. AWS1.4 GuardDuty and the Detectors
5. AWS1.5 The Supporting Sources
6. AWS1.6 The Analysis Surface
7. AWS1.7 Reading a CloudTrail Record
8. AWS1.8 Your First Queries
9. AWS1.9 The Guided Walkthrough
10. AWS1.10 Module Summary
11. Check My Knowledge

Phase 2: The AWS Analysis Surface

AWS Log Sources and What They Capture

What each AWS evidence source records, what it silently misses, how long it lasts, and which investigative question it answers.

1. AWS2.1 Coverage Before Questions
2. AWS2.2 CloudTrail Management Events
3. AWS2.3 CloudTrail Data Events
4. AWS2.4 VPC Flow Logs
5. AWS2.5 GuardDuty as a Source
6. AWS2.6 AWS Config
7. AWS2.7 S3 Server Access Logs
8. AWS2.8 Reconciling the Sources
9. AWS2.9 Coverage Map and Gaps
10. AWS2.10 Module Summary
11. Check My Knowledge

Querying AWS Evidence at Scale

The SQL-over-CloudTrail workflow the rest of the course runs on: filtering millions of events to the few that matter, reaching into nested records, summarizing behavior, sequencing a timeline, and pivoting from one finding to the next.

1. AWS3.1 Asking the First Question
2. AWS3.2 Narrowing the Field
3. AWS3.3 Reading What CloudTrail Buries
4. AWS3.4 From a List to a Pattern
5. AWS3.5 Putting Events on a Clock
6. AWS3.6 Giving an Event Its Context
7. AWS3.7 Building the Query You Don't Have Yet
8. AWS3.8 Following the Thread
9. AWS3.9 Module Summary
10. Check My Knowledge

Phase 3: Identity and Access

IAM and the Identity Attack Surface

Why identity is the perimeter in AWS, and how to read it.

1. AWS4.1 Identity Is the Perimeter
2. AWS4.2 The Five Faces of a Principal
3. AWS4.3 Users and Access Keys
4. AWS4.4 Roles and the Assume-Role Model
5. AWS4.5 Reading the Session
6. AWS4.6 Federation and the Identity with No Name
7. AWS4.7 Permission Is the Payload
8. AWS4.8 Mapping the Identity Attack Surface
9. AWS4.9 Module Summary
10. Check My Knowledge

Detecting Credential Compromise

Turning identity reading into detection. The signals that betray a stolen credential being used by the wrong hands, source and geography, console logins and MFA gaps, reconnaissance bursts, anomalous role assumption, and how to corroborate them into a defensible finding and scope the initial access.

1. AWS5.1 The Initial-Access Problem
2. AWS5.2 Where It Is Used: Source and Geography
3. AWS5.3 Console Logins and MFA Gaps
4. AWS5.4 Reconnaissance as a Signal
5. AWS5.5 Anomalous Role Assumption
6. AWS5.6 Scoping the Compromise
7. AWS5.7 From Signals to a Determination
8. AWS5.8 Module Summary
9. Check My Knowledge

Phase 4: Persistence and Data

Privilege Escalation and Persistence

Detecting what an attacker does with a foothold: widening limited access into broad control through the IAM permission system, and wiring in the backdoors that survive the loss of the original credential.

1. AWS6.1 The Escalation Problem
2. AWS6.2 Rewriting Permissions: Policy Version Abuse
3. AWS6.3 The PassRole Path
4. AWS6.4 Manufacturing a New Identity
5. AWS6.5 The Persistence Problem
6. AWS6.6 Event-Driven Backdoors: Lambda and EventBridge
7. AWS6.7 Persistence Beyond the Foothold
8. AWS6.8 Scoping and Eradicating the Foothold
9. AWS6.9 Module Summary
10. Check My Knowledge

S3 and Data Exfiltration

Detecting the objective of most cloud intrusions: the theft, exposure, and destruction of data in S3.

1. AWS7.1 The Data Exfiltration Problem
2. AWS7.2 The S3 Logging Layers
3. AWS7.3 Discovery: Finding the Data
4. AWS7.4 The Exfiltration
5. AWS7.5 Scoping the Theft
6. AWS7.6 Public Exposure: When the Bucket Is the Door
7. AWS7.7 Destruction and Ransom
8. AWS7.8 Scoping the Data Incident
9. AWS7.9 Module Summary
10. Check My Knowledge

Phase 5: Compute and Evasion

Compute Compromise

The third way into a cloud account: a compromised machine whose role credentials the attacker steals through the instance metadata service.

1. AWS8.1 The Compute Compromise Problem
2. AWS8.2 The Instance Metadata Service
3. AWS8.3 Detecting Stolen Instance Credentials
4. AWS8.4 Using Instance Credentials
5. AWS8.5 Cryptojacking
6. AWS8.6 The Network Lens: VPC Flow Logs
7. AWS8.7 Scoping and Eradicating the Compute Compromise
8. AWS8.8 Module Summary
9. Check My Knowledge

Defense Evasion

When the attacker's goal shifts from using the account to hiding in it.

1. AWS9.1 The Defense Evasion Problem
2. AWS9.2 Disabling CloudTrail
3. AWS9.3 Dismantling the Rest of the Telemetry
4. AWS9.4 Reading the Absence
5. AWS9.5 Hiding the Source: Tor
6. AWS9.6 Designing Against Evasion
7. AWS9.7 Scoping and Responding to Evasion
8. AWS9.8 Module Summary
9. Check My Knowledge

Phase 6: Response and Capstone

Cloud Incident Response and Containment

The AWS incident response process, from triage to a closed incident.

1. AWS10.1 The Cloud IR Problem
2. AWS10.2 Triaging the Incident
3. AWS10.3 Containing Compromised Identities
4. AWS10.4 Isolating Compromised Resources
5. AWS10.5 Preserving Evidence Before Eradication
6. AWS10.6 Org-Level Response and Recovery
7. AWS10.7 The Containment Runbook
8. AWS10.8 Module Summary
9. Check My Knowledge

Capstone: Full-Chain Cloud Incident

One chained AWS incident, investigated end to end.

1. AWS11.1 The Brief
2. AWS11.2 Initial Access: From Baseline to Breach
3. AWS11.3 Reconnaissance
4. AWS11.4 Privilege Escalation and Persistence
5. AWS11.5 The Pivot and Exfiltration
6. AWS11.6 The Final Report
7. AWS11.7 Capstone Summary
8. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

Athena queries by investigation area, each with the console path, the fields that carry the decision, and what the answer does not establish.

1. Query Patterns
2. Log Sources and Coverage
3. Identity and Principals
4. Credential Compromise
5. Privilege Escalation and Persistence
6. S3 and Data Exfiltration
7. Compute Compromise
8. Defense Evasion
9. Response and Containment
10. Events, Findings and Fields

Cookbooks

Seven procedures an AWS responder repeats: triaging a finding, scoping a leaked credential, following an identity chain, establishing what data left, and preserving evidence before eradication.

1. Triaging a GuardDuty Finding
2. Scoping a Leaked Credential
3. Establishing What Data Left
4. Confirming or Refuting Log Tampering
5. Preserving Cloud Evidence
6. Investigating Across an Account Boundary
7. Reconstructing the Incident Timeline

Lab Setup
Building an AWS account that produces the evidence this course investigates, with the cost guardrails in place before anything is switched on.

1. The Account, and the Guardrails That Go First
2. Turning On the Evidence
3. Making It Queryable
4. Adding the Detection Layer
5. Generating Evidence Worth Investigating
6. Verify It Works, Then Turn It Off

Walkthroughs
Six worked AWS investigations against the course corpus, each ending in a written finding with its confidence stated and its gaps named.

1. The Role That Was the Build Pipeline
2. The Key That Was Three Months Old
3. The Role That Called From Somewhere Else
4. The Bucket That Was Open for Thirty-Three Hours
5. The Trail That Was Deleted and Changed Nothing
6. The Query That Moved the Start Date

Playbooks
Seven response playbooks keyed to what actually fires in AWS, each with a pre-flight, a sequence, escalation tiers and the false positives that live in that domain.

1. Instance Credentials Used Outside AWS
2. Logging Stopped or a Trail Deleted
3. Administrative Permissions Granted
4. Anomalous Object Read Volume
5. Objects Deleted at Volume
6. An Instance Talking to Somewhere It Should Not
7. API Calls From an Anonymizing Network

Playground
Where to practice AWS investigation and use it at work: query drills against the course corpus, your own account, the detection library, and the reference pages worth keeping open.

References & Further Reading
AWS service documentation, security guidance, frameworks, and threat-intelligence sources used throughout the AWS Incident Detection and Response course.

Course Completion

Course Exam
AWS Incident Detection and Response end-of-course exam: a simulation-based assessment testing your ability to triage, investigate, and respond to an AWS intrusion you have not seen before, using the evidence and the method built across all 12 modules.

1. Course Completion. AWS Incident Detection and Response

Generated 2026-09-01 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/aws-detection-and-response/