Enterprise Cloud Incident Response and Forensic Readiness on AWS
Author: Adedayo
Specialization: Cloud Security & Incident Response
Platform: Amazon Web Services (AWS)

1. Introduction

This document describes the design, implementation, and validation of an enterprise cloud incident response and forensic readiness framework in AWS.

I implemented this framework to ensure that security incidents involving IAM credentials, malicious API activity, data exposure, and infrastructure misconfigurations can be detected, investigated, contained, and remediated efficiently.

The framework integrates AWS-native security services, documented response playbooks, forensic preservation procedures, and automated remediation workflows.

2. Objectives

The primary objectives were to:

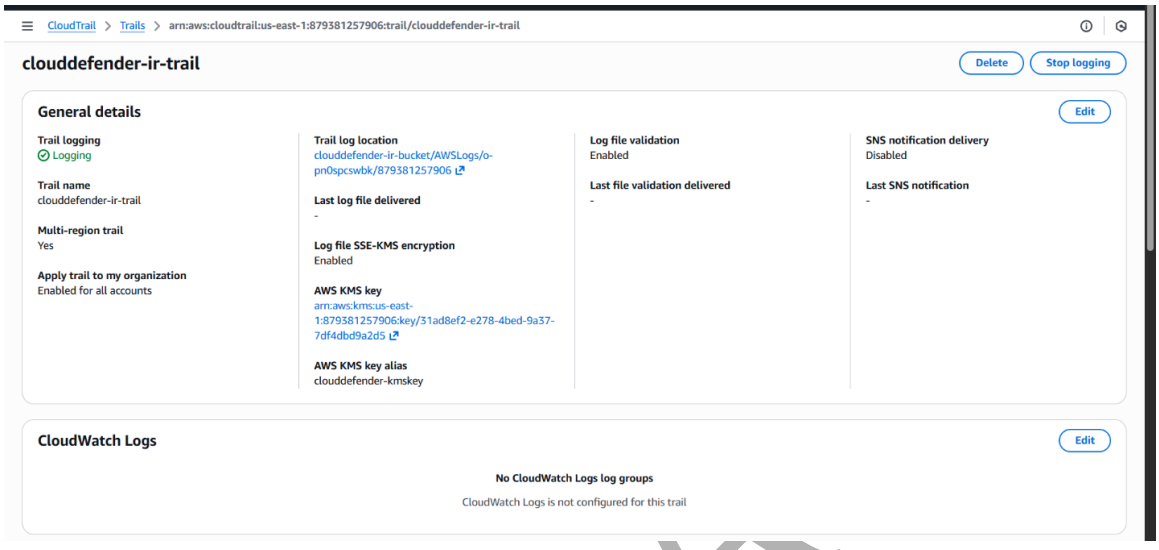
- Improve cloud incident detection and response capability
- Establish standardized response playbooks
- Preserve forensic evidence securely
- Reduce incident response time
- Enable automated containment
- Support audit and compliance requirements

3. Incident Response Evidence Repository

A dedicated S3 bucket was created to store forensic evidence.

The bucket was configured with:

- Encryption enabled
- Versioning enabled
- Restricted access policies
- Deletion protection




This repository stores CloudTrail logs, CloudWatch exports, snapshots, and investigation artifacts.

4. Centralized Logging for Incident Response

AWS CloudTrail was configured for centralized API logging.

CloudTrail serves as the primary forensic data source and supports investigation of:

- Credential compromise
- Privilege escalation
- Resource tampering
- Data access

Logs are automatically delivered to the evidence repository.

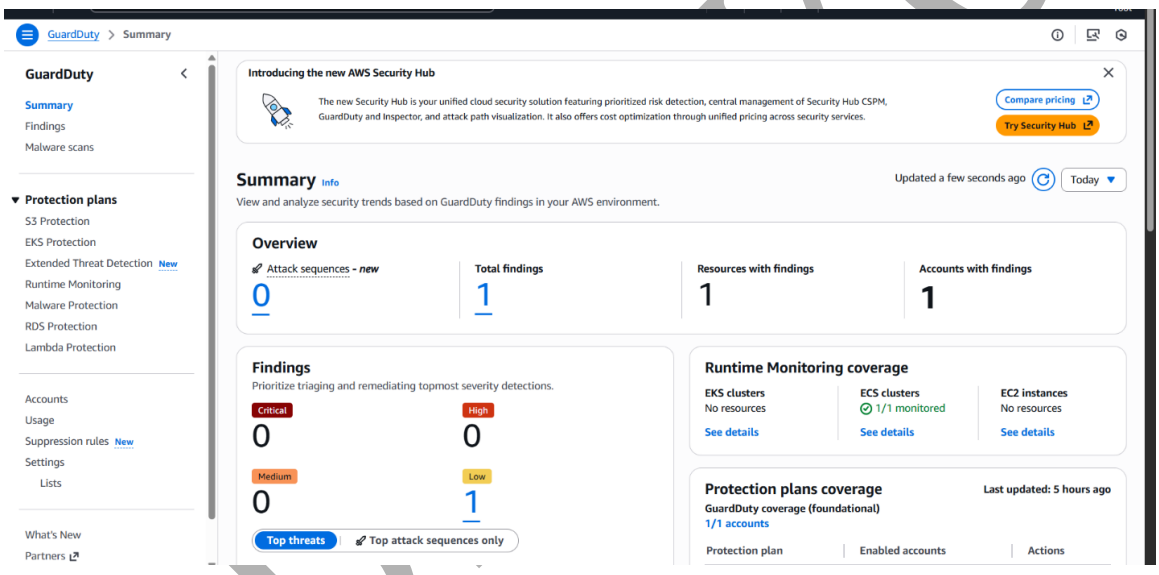
5. Threat Detection Services

5.1 Amazon GuardDuty

GuardDuty was enabled for continuous threat detection.

It supports detection of:

- IAM credential compromise
- Malicious API behavior
- Data exfiltration
- EC2 compromise
- Lambda abuse




GuardDuty findings trigger incident response workflows.

5.2 AWS Security Hub

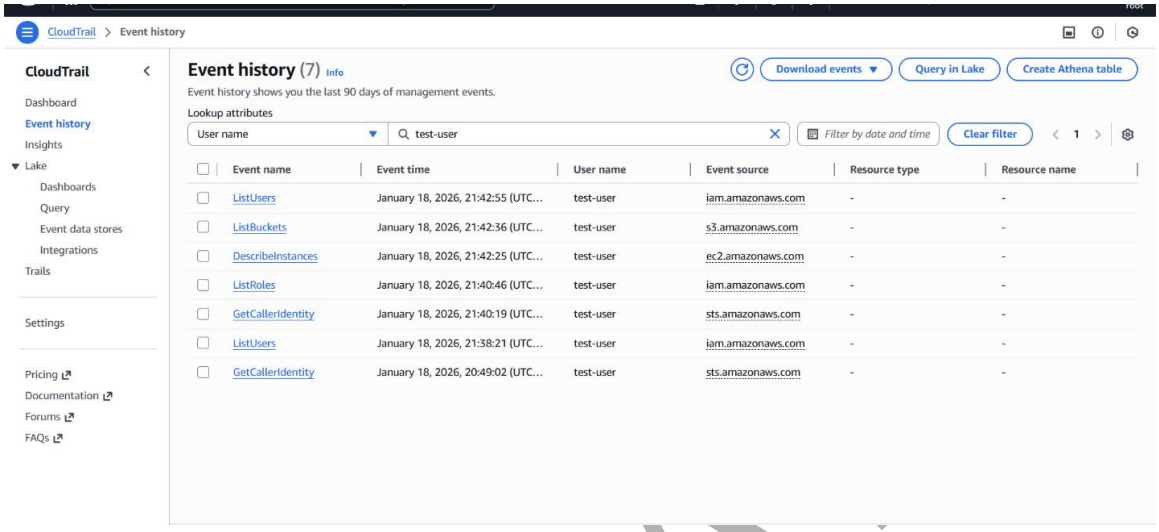
Security Hub was enabled for centralized findings management.

Findings from GuardDuty and AWS security standards are aggregated and prioritized for response.

6. Incident Simulation and Testing

6.1 Incident 1: IAM Credential Misuse

Detection Source: CloudTrail




Unusual API enumeration activity was detected from an IAM user.

Triage Actions:

- Reviewed CloudTrail events
- Identified access key and source IP
- Confirmed suspicious behavior.

Severity: SEV 2 (High)

Forensic Preservation:

- CloudTrail logs archived
- IAM metadata documented

Containment:

- Access key deactivated

Outcome:

- No data loss
- Early containment

Lessons Learned:

- Manual log review remains critical
- Early isolation reduces impact

6.2 Incident 2: EC2 Public SSH Exposure

Detection Source: Security Hub

An EC2 instance was found with SSH open to 0.0.0.0/0.

Triage Actions:

- Reviewed security group rules
- Verified public IP exposure

Severity: SEV 2 (High)

Forensic Preservation:

- EBS snapshot created
- Metadata recorded

Containment:

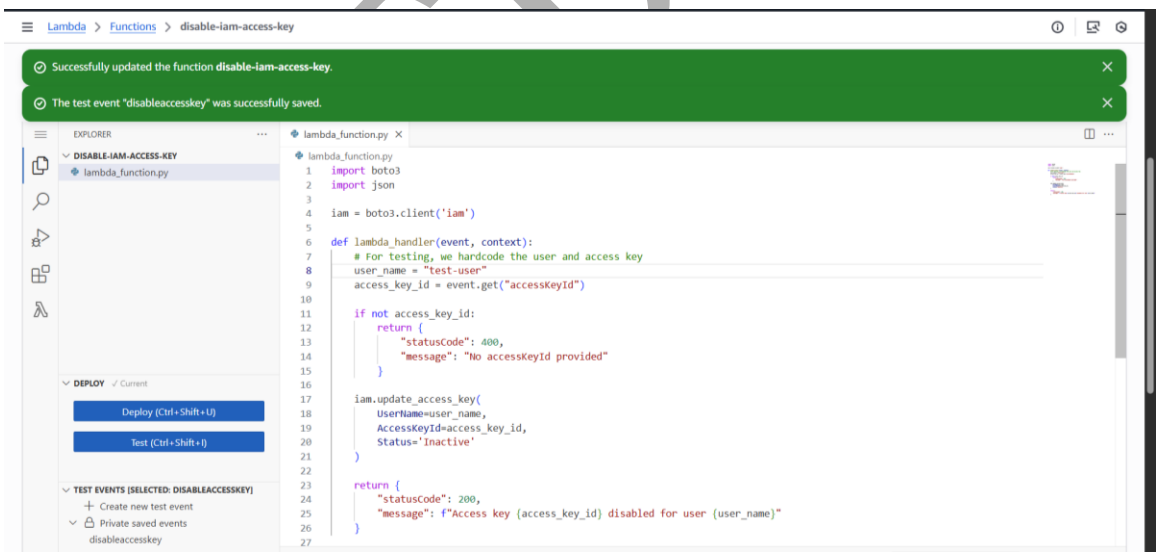
- SSH access restricted

Outcome:

- No unauthorized access
- Risk eliminated

7. Automated Remediation Framework

An automated remediation workflow was implemented using AWS Lambda.



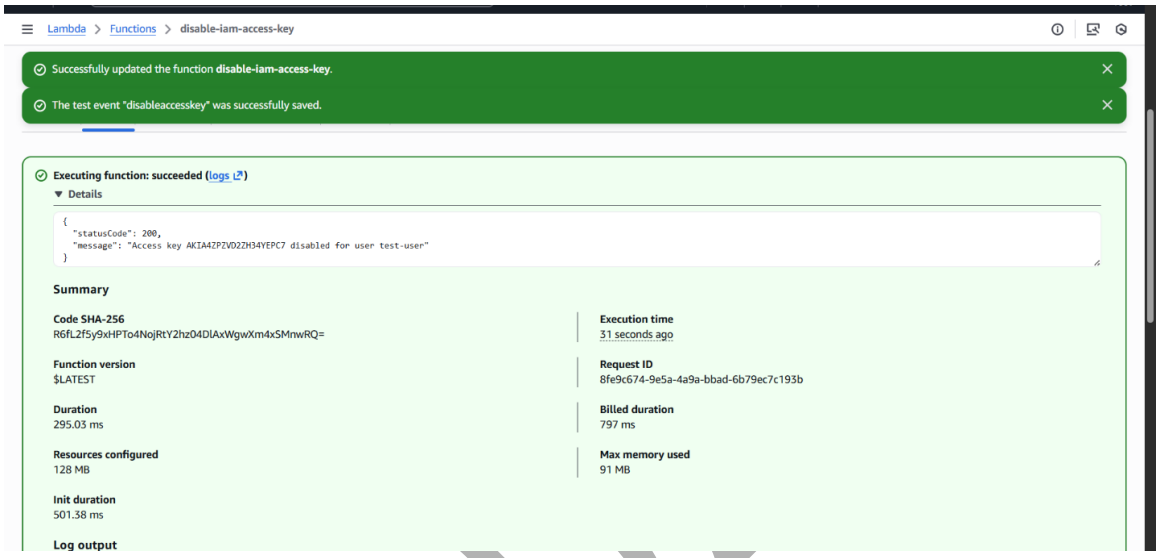

The workflow:

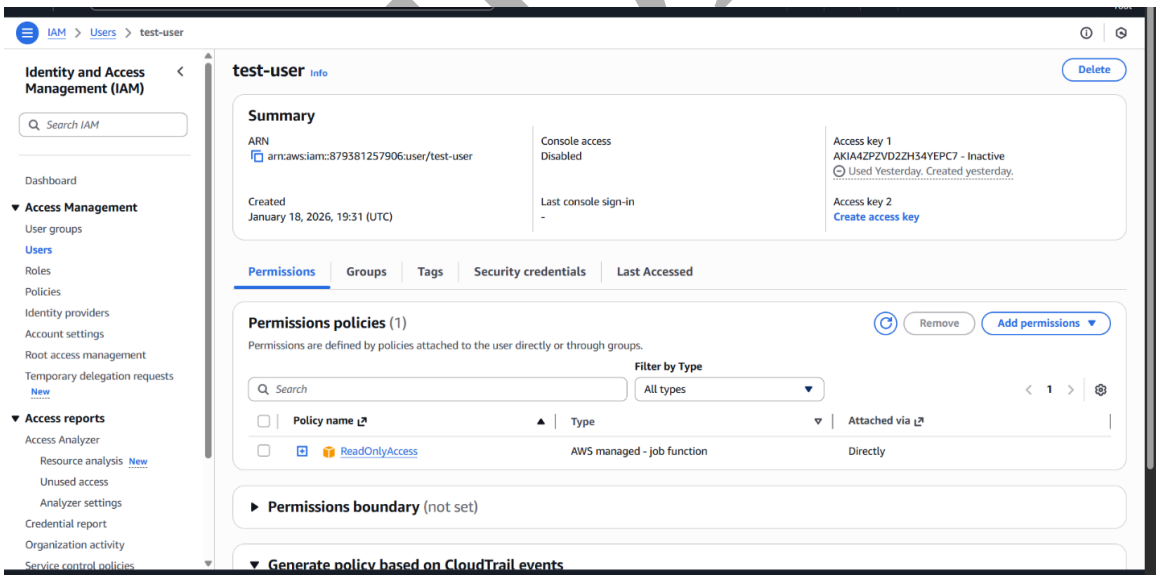
- Receives compromised access key IDs
- Disables keys

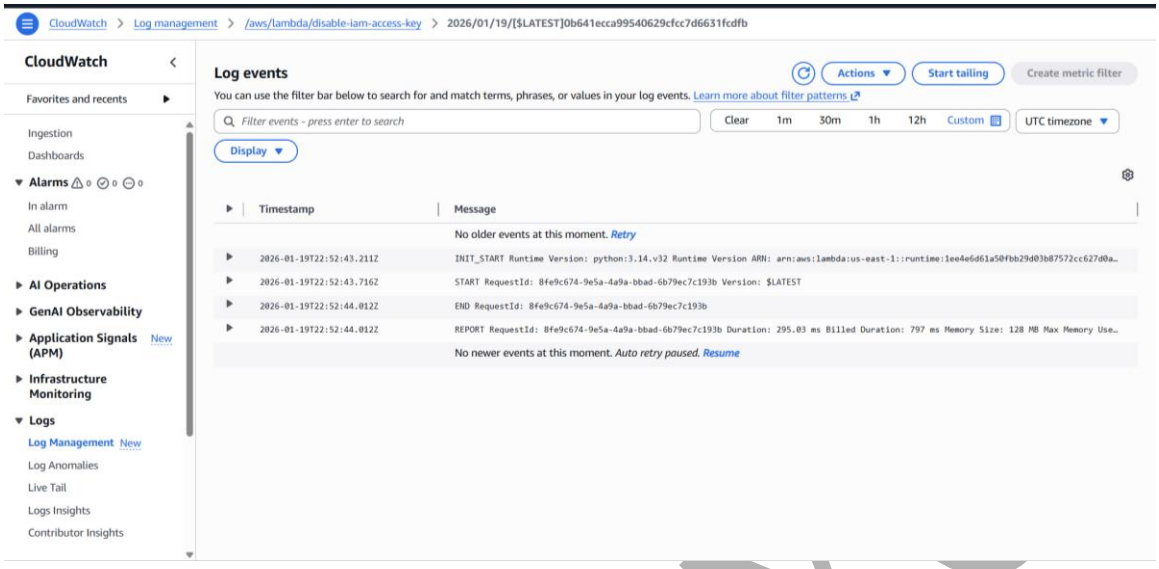
- Logs actions to CloudWatch

Keys are deactivated, not deleted, to preserve evidence.

Testing confirmed successful automated containment.






8. Alerting for Logging Tampering

CloudWatch alarms were created to detect:

- StopLogging
- DeleteTrail

These alerts provide early warning of audit log tampering.

9. Incident Response Playbooks

Cloud-specific response playbooks were developed for:

- Credential compromise
- API abuse
- Data exfiltration
- Resource misconfiguration

Each playbook defines detection, triage, preservation, containment, and escalation steps.

10. Forensic Preservation Procedures

Tested procedures include:

- CloudTrail archival
- CloudWatch export to S3
- EBS snapshots
- IAM key deactivation

All evidence is encrypted and access-controlled.

11. Governance and Documentation

All response workflows, evidence handling procedures, and automation processes were documented.

Documentation supports audits, investigations, and team readiness.

12. Outcomes and Impact

This implementation delivered:

- Faster incident response
- Strong forensic readiness
- Automated containment
- Improved detection coverage
- Reduced operational risk
- Audit-ready processes

13. Conclusion

I designed and implemented a comprehensive cloud incident response and forensic readiness framework on AWS.

Through integrated detection, evidence preservation, automation, and governance, this solution enables effective and resilient security operations.