AWS Cloud Security – Incident Response Report

Project: AWS Security Foundations & Monitoring Project
Incident Type: Simulated GuardDuty High-Severity Finding
Prepared By: Abhinav Yanambaka
Date: Simulated Exercise

1. Executive Summary

This document outlines a simulated incident response exercise conducted as part of the AWS Security Foundations and Monitoring Project. The objective of this exercise was to validate detection, investigation, containment, and recovery processes using native AWS security services.

2. Incident Detection

Amazon GuardDuty generated a high-severity sample finding indicating suspicious activity consistent with potential credential misuse or reconnaissance behavior. CloudWatch alarms configured on CloudTrail logs served as supporting indicators of abnormal API activity.

3. Investigation

The GuardDuty finding was reviewed to identify affected resources, timestamps, and recommended remediation actions. CloudTrail and CloudWatch Logs were analyzed to correlate API calls, identify the source of the activity, and confirm whether privilege escalation or unauthorized configuration changes occurred.

4. Containment Actions

- Disabled or rotated impacted IAM credentials.
- Validated Multi-Factor Authentication enforcement.
- Reviewed IAM policies for least-privilege compliance.

5. Recovery

Normal operations were restored after verifying credential security and ensuring no unauthorized changes persisted. Security Hub was reviewed to confirm that key security controls such as CloudTrail and GuardDuty remained enabled and healthy.

6. Lessons Learned

- Centralized logging and alerting significantly reduce detection time.
- Role-based access and MFA are critical for limiting blast radius.
- Documented response workflows improve repeatability and readiness.

7. Conclusion

This simulated incident response exercise demonstrates practical cloud security operations aligned with Cloud Security Engineer responsibilities. The project validates the effectiveness of identity hardening, centralized monitoring, managed threat detection, and structured response procedures.