NAME: AMUDA RANTI

ROLE: CLOUD SECURITY ENGINEER

TASK:CLOUD SECURITY MONITORING & THREAT DETECTION IN AWS.

As a Cloud Security Professional, I designed and implemented a robust cloud logging and monitoring framework in AWS. This project demonstrates my expertise in security operations by tracking user activities, detecting threats, and automating responses to potential security incidents. By leveraging AWS-native security tools, I enhanced visibility, ensured compliance, and improved incident response capabilities within the cloud environment.

Project Scope & Key Responsibilities

1. Implementing Centralized Logging with AWS CloudTrail

Enabled AWS CloudTrail to log API calls and track user activity across all AWS services.

Configured multi-region logging to maintain a complete security audit trail.

Secured logs by storing them in Amazon S3 with encryption and strict access controls.

Enabled log integrity validation to detect unauthorized modifications.

2. Threat Detection & Intelligence Using AWS GuardDuty

Deployed AWS GuardDuty to continuously analyze CloudTrail, VPC flow logs, and DNS logs.

Configured GuardDuty to detect suspicious activity such as unauthorized access, brute-force attempts, and reconnaissance attacks.

Integrated GuardDuty findings with AWS Security Hub for centralized security visibility.

3. Real-Time Alerts & Automated Incident Response

Configured Amazon CloudWatch Alarms to trigger alerts based on high-risk security events.

Implemented AWS SNS (Simple Notification Service) to deliver real-time security notifications via email and SMS.

Designed automated remediation workflows using AWS Lambda, enabling immediate

responses to security threats (e.g., automatically revoking compromised credentials).

4. Log Analysis & Security Incident Investigation

Utilized AWS Athena to query and analyze CloudTrail logs for forensic investigations.

Integrated logs with Amazon OpenSearch Service for real-time threat visualization and anomaly detection.

Conducted post-incident reviews and documented security improvements based on log insights.

Business Impact & Key Outcomes

- Increased visibility into AWS account activities, ensuring proactive security monitoring.
- Strengthened threat detection with real-time intelligence from AWS GuardDuty.
- Reduced response time to security incidents through automated remediation.
- Improved compliance with industry regulations and best security practices.
- Demonstrated hands-on expertise in AWS security monitoring, log analysis, and incident response.

Supporting Evidence & Deliverables

- Documented step-by-step configurations with architecture diagrams.
- AWS CloudTrail logs and GuardDuty threat detection reports.
- CloudWatch Alarms setup and automated security response workflows.
- Case studies showcasing security incidents and mitigation strategies.
- Optional: Video walkthrough demonstrating logging and monitoring setup.

This project highlights my ability to secure AWS environments through proactive monitoring, automated threat detection, and rapid incident response, making it a valuable addition to my professional portfolio.