NAME: AMUDA RANTI

ROLE: CLOUD SECURITY ENGINEER

TASK:CLOUD INCIDENT RESPONSE SIMULATION & FORENSIC ANALYSIS

I executed a hands-on cloud incident response simulation to assess and improve security resilience. This experience involved simulating an unauthorized access attempt to an Amazon S3 bucket, leveraging AWS security services to detect threats, conducting forensic analysis, and implementing remediation measures. The goal was to enhance security posture, mitigate risks, and establish a proactive incident response framework.

Key Responsibilities & Execution
1. Simulating a Security Breach
Configured an Amazon S3 bucket with misconfigured access policies to replicate real-world threats.
Used AWS IAM role escalation and credential exposure to simulate unauthorized access.
Introduced potential attack vectors such as:
Compromised credentials accessing restricted data.
Overly permissive S3 bucket policies leading to data exposure.

2. Threat Detection & Forensic Analysis
Activated AWS CloudTrail to log API activity and analyzed access anomalies.
Enabled Amazon GuardDuty to detect malicious actions like suspicious API calls and unauthorized region access.
Conducted forensic analysis using:
Amazon Athena to query CloudTrail logs and pinpoint unauthorized access attempts.
AWS Security Hub for centralized threat intelligence correlation.
AWS CloudWatch Logs & Metrics to monitor real-time activity spikes.

3. Incident Response & Mitigation
Developed a structured incident response plan aligned with AWS best practices:
Detection & Alerting – Configured AWS SNS to send security alerts on suspicious activity.
Containment – Revoked compromised IAM credentials and locked down misconfigured S3 policies.
Eradication & Recovery – Applied AWS Config rules to enforce security baselines and prevent policy misconfigurations.
Post-Incident Review – Documented findings and refined security policies to strengthen defenses.

4. Security Hardening & Prevention
Enforced IAM least privilege access and removed unnecessary permissions.
Enabled Multi-Factor Authentication (MFA) for all privileged users.
Implemented AWS Macie to identify and protect sensitive data in S3.
Applied AWS WAF (Web Application Firewall) to prevent unauthorized traffic and

mitigate threats.
Results & Business Impact

- Enhanced Security Posture – Strengthened AWS environment against unauthorized access and policy misconfigurations.
- Improved Threat Visibility – Established real-time monitoring and alerting for security anomalies.
- Mitigated Compliance Risks – Aligned cloud security with CIS, NIST, and AWS Well-Architected Framework standards.
- Demonstrated Proactive Security Response – Reduced incident response time by leveraging AWS automation.
- Showcased Hands-On Expertise – Applied practical cloud forensic analysis techniques in a simulated attack scenario.

- CloudTrail logs & forensic analysis reports detailing unauthorized access attempts.
- GuardDuty threat alerts & AWS Security Hub findings identifying suspicious activity.
- Incident response plan document with remediation steps and security recommendations.
- IAM & S3 policy updates to enforce hardened access controls.

This experience validates my expertise in cloud incident response, forensic investigation, and proactive security measures. It demonstrates my ability to detect, analyze, and remediate security incidents in an AWS environment, showcasing my readiness to secure cloud infrastructures at an enterprise level.