NAME: AMUDA RANTI

ROLE: CLOUD SECURITY ENGINEER

TASK: CLOUD SECURITY COMPLIANCE ASSESSMENT WITH AWS SECURITY HUB

I conducted a comprehensive security compliance assessment using AWS Security Hub to evaluate the security posture of cloud resources. This experience focused on identifying security gaps, measuring compliance against CIS benchmarks, and implementing remediation strategies to align with industry best practices.

Key Responsibilities & Implementation

1. Evaluating Cloud Security Posture

Enabled AWS Security Hub across multiple AWS accounts to centralize security findings.

Integrated AWS Config, GuardDuty, and IAM Access Analyzer to provide a unified security view.

Conducted CIS AWS Foundations Benchmark assessment to measure compliance.

2. Analyzing Security Findings & Compliance Gaps

Reviewed Security Hub’s findings for misconfigurations, policy violations, and vulnerabilities.

Prioritized high-risk issues such as publicly exposed S3 buckets, weak IAM policies, and unencrypted databases.

Cross-referenced results with AWS Well-Architected Framework Security Pillar best practices.

3. Implementing Security Remediations

Applied IAM least privilege policies to restrict over-permissive access.

Enforced encryption at rest and in transit for critical data services.

Configured AWS Config Rules to monitor and enforce security best practices.

Enabled AWS Organizations Service Control Policies (SCPs) to restrict non-compliant actions.

4. Automating Continuous Compliance Monitoring

Used AWS Security Hub automation rules to send real-time alerts for non-compliance.

Integrated Amazon EventBridge to trigger remediation workflows for security violations.

Deployed an AWS Lambda function to auto-remediate misconfigured resources based on CIS recommendations.

Results & Business Impact

- Improved Security Posture – Identified and mitigated cloud security risks proactively.
- Achieved Higher Compliance Scores – Aligned AWS environments with CIS benchmarks and AWS best practices.
- Reduced Attack Surface – Hardened IAM, networking, and storage security configurations.
- Automated Security Operations – Implemented continuous compliance monitoring and auto-remediation.
- Demonstrated Expertise in Cloud Compliance – Hands-on experience with AWS security governance and risk management.

- AWS Security Hub compliance reports showing risk analysis and CIS benchmark scores.
- Remediation strategies & IAM policy updates to enforce least privilege access.
- AWS Config Rules & automation scripts for continuous security monitoring.

This experience showcases my ability to assess, enhance, and maintain cloud security compliance using AWS Security Hub. It demonstrates expertise in risk identification, compliance enforcement, and automated security remediation, proving my capability in securing enterprise cloud environments.