NAME: AMUDA RANTI

ROLE: CLOUD SECURITY ENGINEER

TASK:SECURING CONTAINERIZED WORKLOADS IN AWS EKS

I implemented end-to-end security for containerized workloads running on AWS Elastic Kubernetes Service (EKS). The focus was on deploying a secure Kubernetes environment, enforcing security policies, and proactively detecting vulnerabilities to ensure a robust cloud-native infrastructure.

Key Implementation & Security Measures
1. Secure Deployment of a Containerized Application
Provisioned an Amazon EKS cluster following AWS best practices.
Deployed a containerized web application using Kubernetes manifests (Deployments, Services, and Ingress).
Configured an Application Load Balancer (ALB) to securely manage traffic.

2. Kubernetes Security Policy Enforcement
Implemented Role-Based Access Control (RBAC) to enforce least privilege access for users and workloads.
Applied Pod Security Standards (PSS) to prevent privilege escalation and enforce security compliance.
Configured Kubernetes Network Policies to restrict inter-pod communication and prevent lateral movement attacks.

3. Container Vulnerability Scanning & Image Hardening
Scanned container images using Amazon ECR Image Scanning and Trivy to detect security vulnerabilities.
Used AWS Signer to enforce signed and trusted images, ensuring integrity and authenticity.
Ran Kube-bench to validate compliance with the CIS Kubernetes Security Benchmark.

4. Threat Detection & Security Monitoring
Enabled Amazon GuardDuty for EKS to detect anomalous behavior and security threats.
Integrated AWS CloudTrail and CloudWatch Logs to audit Kubernetes API activity and track unauthorized access.
Deployed Falco for real-time intrusion detection, logging suspicious runtime behaviors inside the cluster.
Configured Prometheus & Grafana dashboards to monitor security-related metrics.
Results & Business Impact

- Hardened Kubernetes Environment – Implemented security controls to mitigate risks.
- Reduced Attack Surface – Enforced security scanning and access control policies.
- Improved Compliance Posture – Aligned security with CIS, NIST, and AWS Well-Architected Framework best practices.
- Proactive Threat Detection – Established real-time security monitoring and automated alerts for suspicious activities.

- Demonstrated Expertise in Kubernetes Security – Hands-on application of industry security standards in a cloud-native environment.

- Kubernetes manifests & IAM configurations showcasing security enforcement.
- Container vulnerability scan reports from Amazon ECR and Trivy.
- RBAC & Network Policy configurations ensuring controlled access.
- Falco security logs & GuardDuty alerts detecting security threats.
- Documentation & Video Walkthrough (Optional) explaining security implementations.

This experience highlights my ability to design, deploy, and secure containerized workloads in AWS. It showcases my skills in Kubernetes security, vulnerability management, and threat detection—demonstrating my readiness to secure cloud-native applications in an enterprise environment.