■ Security & Compliance Report
DevSecOps EKS Infrastructure Assessment

Project: DevSecOps Candidate Evaluation
Date: December 2024
Version: 1.0
Author: DevSecOps Team

Executive Summary

This report provides a comprehensive security assessment of the DevSecOps infrastructure including Docker containerization, Terraform Infrastructure as Code (IaC), and Kubernetes deployment. The overall security posture is strong, with critical improvements required in Terraform and EKS configuration before production deployment.

Component	Score	Status
Docker Image Hardening	90/100	Strong
Terraform / EKS Security	68/100	Needs Improvement
Kubernetes Hardening	88/100	Strong
Monitoring & Observability	80/100	Good

1. Docker Security Assessment

Docker images follow industry best practices including minimal base images, multi-stage builds, non-root execution, and vulnerability scanning using Trivy and Dockle. No critical or high vulnerabilities were detected.

2. Terraform & EKS Security Assessment

Terraform security scanning identified multiple critical and high-risk findings primarily related to network exposure and overly permissive IAM policies. These findings must be remediated before production use.

Critical Issues Identified:

- EKS public endpoint accessible from 0.0.0.0/0
- Unrestricted security group egress rules
- Node groups with public internet access
- IAM policies using wildcard resources

3. Kubernetes Security Assessment

Kubernetes workloads are well-hardened with Pod Security Contexts, network policies, resource limits, and security linting. All manifests passed validation and security linting checks.

4. Risk Summary

Critical risks must be resolved immediately to prevent unauthorized access, data exfiltration, and compliance violations. High and medium risks should be addressed before production deployment.

5. Compliance Status

The infrastructure partially complies with CIS benchmarks. Docker and Kubernetes show high compliance, while AWS EKS controls require remediation to meet baseline security standards.

6. Action Plan

A phased remediation approach is recommended, prioritizing critical network and IAM issues before enabling production workloads.

7. Conclusion

Docker and Kubernetes configurations are production-ready. However, Terraform and EKS configurations are not production-ready due to multiple critical and high-risk security findings. Production deployment should be blocked until remediation is complete.

Classification: Internal Use Only
Next Review: Post Remediation