AI-Powered DevSecOps Summary Report

Scan Date: 2025-06-11

Pipeline Trigger: GitHub Pull Request

Environment: IaC Security Pipeline for T2S

Generated By: Emmanuel Naweji

Findings Summary

Checkov: Total Issues: 12 (Critical: 3, High: 4, Medium: 3, Low: 2)

Trivy: Total Issues: 26 (Critical: 5, High: 10, Medium: 7, Low: 4)

Gitleaks: Total Issues: 3 (Critical: 1, High: 1, Medium: 1, Low: 0)

AI Best Practices: Total Issues: 5 (Critical: 2, High: 1, Medium: 1, Low: 1)

AI Recommendations

As you didn't provide any specific scan findings, I'll provide you with some general security improvement recommendations:

1. Regular Updates and Patch Management: Outdated software often has known vulnerabilities that can easily be exploited by attackers. Therefore, it is crucial to regularly update and patch all software, systems, and applications to their latest versions.

2. Enable Firewall and Intrusion Detection Systems: It is crucial to use firewalls and intrusion detection systems to monitor network traffic, block suspicious activities, and alert your team to potential security threats.

3. Implement Secure Coding Practices: DevSecOps teams should follow secure coding practices to minimize the number of vulnerabilities in the final codebase. This includes input validation, correct error handling, secure session management, and secure coding conventions.

4. Incorporate Automated Security Scans in CI/CD Pipeline: As part of the continuous integration and deployment process, regularly schedule automated security scans to identify and fix security vulnerabilities as

soon as possible.

5. Enhance Authentication and Access Controls: Ensure that all systems, applications, and data are protected with strong authentication methods (including multi-factor authentication) and stringent access controls based on the principle of least privilege (only grant access to what is necessary for a task).

These are general recommendations. If you provide me with specific scan findings, I can give you more targeted improvement ideas.