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

Unfortunately, there aren't any scan findings provided in the question. However, I can provide general recommendations that often arise from common security scans.

1. Regular Security Training: Team members should be regularly trained on good security practices, updated on new security threats, and educated on how to properly handle data to avoid common vulnerabilities.

2. Implement Secure Coding Practices: Encourage developers to adopt secure coding practices, such as validating input, encoding data, implementing secure user authentication, and managing sessions securely.

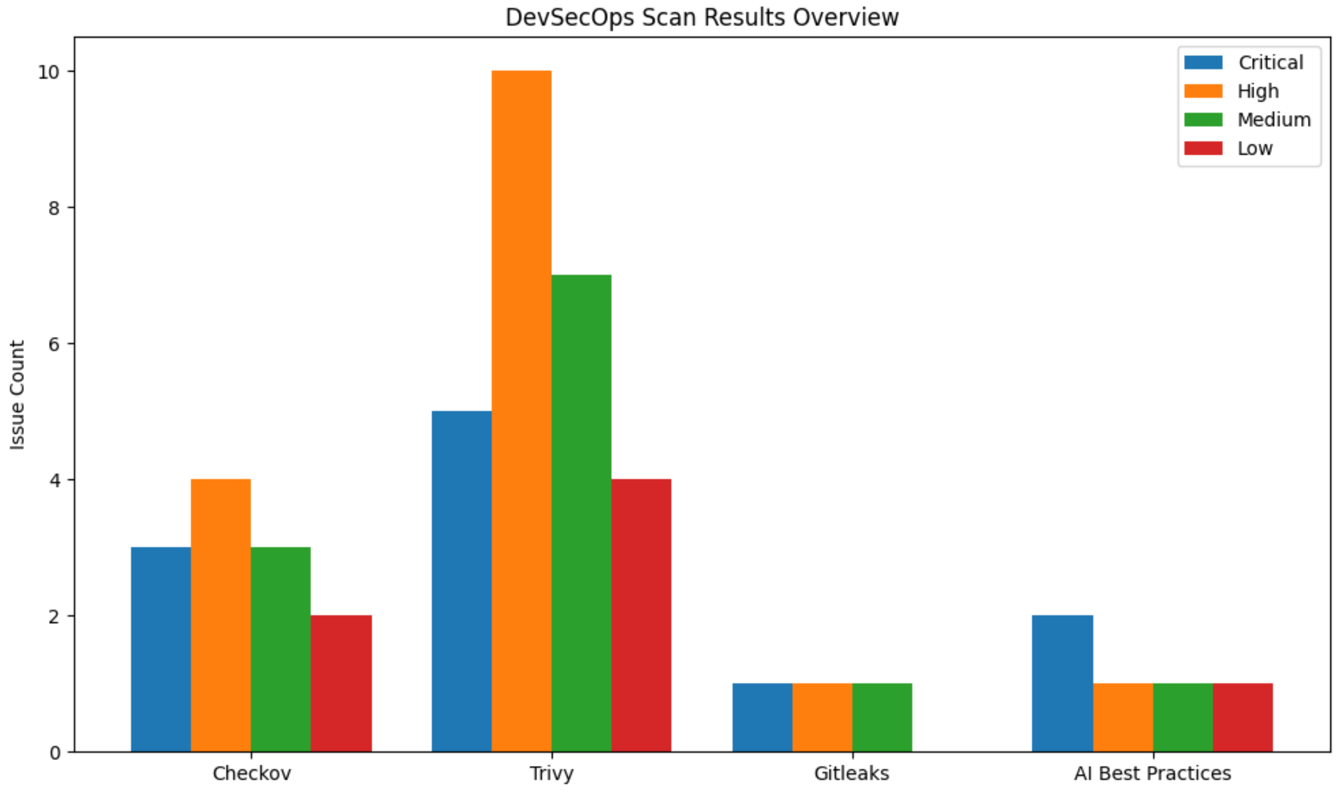
3. Regular Security Scans: Conduct static code analysis, dynamic analysis, and penetration testing regularly to identify and correct vulnerabilities. This will help to catch and fix errors early, saving time and effort.

4. Update and Patch Regularly: Keep all systems, applications, and libraries updated with the latest patches. Cyber-attackers often exploit known vulnerabilities in outdated software.

5. Implementation of Security Policies: Create and implement organization-wide security policies. This can include practices like rotating sensitive keys, limiting access privileges only to necessary individuals, using

multi-factor authentication, etc.

Please provide the specific scan findings for a more detailed and targeted set of recommendations.


DevSecOps Scan Results Overview
Issue Count
Critical
High
Medium
Low
Checkov
Trivy
Gitleaks
AI Best Practices