SafeOps-LogMiner — DevSecOps Security Report

Pipeline: github-actions
Generated: 2025-12-24T19:15:59.098Z

Security Score: 14/100

Findings: 18 | TotalRisk: 108 | Anomalies: 3

Vulnerabilities (VulnDetector)

Report #5 — status=failed — Wed Dec 24 2025 17:02:50 GMT+0000 (Coordinated Universal Time)
- [CRITICAL] Exposed secret in logs
  desc: A token or secret was detected in pipeline output.
  fix: Remove secrets from logs, enable secret masking, and use a vault (GitHub Secrets, Vault, etc.).
- [CRITICAL] Secret exposed via semantic event
  desc: A secret was detected as a semantic event.
  fix: Rotate exposed secrets immediately and prevent secrets from being echoed in logs.
- [MEDIUM] Pipeline contains error keywords
  desc: Error-like keywords detected (failed, exception, error).
  fix: Investigate failing steps and ensure security checks are not skipped.
- [MEDIUM] Error detected as semantic event
  desc: An error was detected as a semantic event.
  fix: Review pipeline logs and fix the failing step.
- [HIGH] Potential bypass attempt
  desc: The logs include bypass or skip wording.
  fix: Block bypass flags, enforce required checks and branch protection rules.
- [HIGH] Security bypass semantic event
  desc: A bypass attempt was detected in semantic events.
  fix: Disallow security bypass options and enforce mandatory CI policies.
- [LOW] External URL usage in pipeline
  desc: External URLs were found in pipeline logs.
  fix: Verify external URLs and pin dependencies to trusted sources.
- [MEDIUM] Suspicious job or step detected
  desc: A pipeline job or step may indicate risky behavior.
  fix: Review job isolation and permissions for this pipeline step.

Report #4 — status=failed — Wed Dec 24 2025 17:01:34 GMT+0000 (Coordinated Universal Time)
- [CRITICAL] Exposed secret in logs
  desc: A token or secret was detected in pipeline output.
  fix: Remove secrets from logs, enable secret masking, and use a vault (GitHub Secrets, Vault, etc.).
- [CRITICAL] Secret exposed via semantic event
  desc: A secret was detected as a semantic event.
  fix: Rotate exposed secrets immediately and prevent secrets from being echoed in logs.
- [MEDIUM] Pipeline contains error keywords
  desc: Error-like keywords detected (failed, exception, error).
  fix: Investigate failing steps and ensure security checks are not skipped.
- [MEDIUM] Error detected as semantic event
  desc: An error was detected as a semantic event.
  fix: Review pipeline logs and fix the failing step.
- [HIGH] Potential bypass attempt
  desc: The logs include bypass or skip wording.
  fix: Block bypass flags, enforce required checks and branch protection rules.
- [HIGH] Security bypass semantic event
  desc: A bypass attempt was detected in semantic events.

    fix: Disallow security bypass options and enforce mandatory CI policies.
  - [LOW] External URL usage in pipeline
    desc: External URLs were found in pipeline logs.
    fix: Verify external URLs and pin dependencies to trusted sources.
  - [MEDIUM] Suspicious job or step detected
    desc: A pipeline job or step may indicate risky behavior.
    fix: Review job isolation and permissions for this pipeline step.

Report #1 — status=done — Sun Dec 21 2025 15:27:49 GMT+0000 (Coordinated Universal Time)
  - [CRITICAL] Hardcoded AWS Key
    fix: Use GitHub Secrets
  - [MEDIUM] Docker runs as root
    fix: Use USER in Dockerfile

Fix Suggestions (FixSuggester)

Showing latest 2 fixes.

- R001 — Exposed secret in logs — Wed Dec 24 2025 17:03:56 GMT+0000 (Coordinated Universal Time)
- R001 — Fix: move secrets to GitHub Secrets — Wed Dec 24 2025 15:47:16 GMT+0000 (Coordinated Universal Time)

Behavioral Anomalies (AnomalyDetector)

Anomalies detected for pipeline "github-actions": 3