Apiiro + HashiCorp

Contextual Infrastructure-as-Code Security
Better Together: Apiiro + HashiCorp

With Apiiro, DevSecOps engineers can completely shift-left security and remediate risks early in the SDLC. In addition, security champions and security architects can gain complete risk visibility to remediate risks faster and with context - by connecting all application code components.

In order to get started, all a security practitioner needs to do is connect source control managers to Apiiro.

Scenario #1: Remediate Exposed Secrets

An Application Security Architect needs to:

1. Identify all instances of exposed secrets in their source code
2. Remediate exposed secrets according to risk
3. Safely store all secrets in a vault.

Apiiro connects to source control managers in 5 minutes via read-only API. Apiiro analyzes all repositories and builds an application inventory and software bill-of-materials (SBOM) that is updated automatically and continuously.

Get visibility to existing secrets

With Apiiro, you can filter all of your applications and repositories to see only those that contain exposed secrets.
Get complete context for every secret

For each secret Apiiro discovers, the Security Engineer can see the exact file the secret is in, the type of secret, when it was added, and by which developer.

Remediate addition of unencrypted exposed secrets in the pull-request

Apiiro provides automated workflows that can comment on the pull request in which a secret is added. This immediately alerts the developer, shifting security left, and minimizing rework.
Update access keys #4

**idanelor** commented 23 minutes ago

No description provided.

---

**apiiro** bot commented 20 minutes ago

2 material changes identified by Apiiro:
WORKFLOW-1 · Exposed Secrets Added to Source Code:
Oh no! You are about to add an exposed secret to our safe application.

Please safely store it in vault as described in this guide:

Here's a code example on how to interact with encrypted secrets:

- User password added to source code (2)
  - complete/config.yaml - lines: #3
  - complete/config.yaml - lines: #5

View in Apiiro
Scenario #2: Build a complete Infrastructure-as-Code inventory and remediate cloud misconfigurations before production

With Apiiro you can continuously analyze terraform assets and get complete visibility into cloud misconfigurations in the pull-request - before they get to production.
About Apiiro

The Apiiro Code Risk Platform™ helps you build a risk-based & measurable AppSec program that extends from cloud to code. With Apiiro, you can detect and prioritize cloud misconfigurations by combining a deep understanding of both application and Infrastructure as Code. Using context from across the SDLC, security professionals can finally truly understand their IaC risks instead of having to manage a laundry list of alerts that don't provide useful, actionable information.

Apiiro is re-inventing the Secure Software Development Lifecycle for agile and cloud-native development.

Discover
All application assets to build an inventory, from cloud to code

Remediate
Critical risks in cloud-native applications, before releasing

Measure
DevSecOps maturity and remediation KPIs across the entire SDLC