WIZ + HashiCorp Terraform

WIZ INTEGRATION (WIN) PROGRAM

DevOps teams use infrastructure as code (IaC) tools like HashiCorp's Terraform to automate infrastructure provisioning, release new features, and keep up with customer demand. Building 'secure by design' is critical to reduce the risk of an attack in the cloud when relying on IaC tools.

Wiz provides proactive and real-time security visibility into the cloud, allowing customers to secure their production cloud environments. The Wiz integration with Terraform's Run Task helps teams shift security left earlier in the development process by scanning for secrets and misconfigurations in IaC templates before pushing deployments to production.

Benefits of the integration

- **Reduce risk early:** Wiz enables you to take runtime security learnings and apply them as security scans and policies into Terraform pipelines before it provisions infrastructure in production.
- **Improve developer efficiency:** Fixing security risks earlier helps reduce the time development teams focus on investigating and fixing production issues and can focus on what they enjoy and what the business values the most: improving and building new applications.
- **Protect production environments:** The risk introduced into your production environment isnot just isolated to what you're deploying but becomes a holistic risk to all the existingapplication crown jewels you have in your cloud.

Market challenge

The cloud introduces a new environment that developers and security teams must understand and protect. Organizations must secure all of their cloud environments-dev, testing, and production environments, alongside the CI/CD pipelines that deploy to each of these environments. Securing these environments requires security and development teams to gain comprehensive visibility into their cloud, understand the new, unique risks in this environment, and learn how to work together to solve critical security issues

The better together story

Wiz starts by providing teams with immediate visibility into the workloads across an organization's cloud environment. Wiz then scans for and combines risks like vulnerabilities, misconfigurations, and secrets exposures to find attack paths that the security team should fix immediately. Terraform streamlines cloud infrastructure deployment for DevOps teams, leveraging automation to minimize errors during cloud deployments.

Integrating Wiz with Terraform Cloud and Terraform Enterprise provides mutual customers with a critical security check either after the planning stage or before applying changes. This check scans Infrastructure as Code (IaC) Terraform configurations for secrets or misconfigurations before these risks reach production environments. By automating the enforcement of security best practices, this integration ensures the deployment of secure infrastructure, effectively lowering the organization's risk profile

Use Case

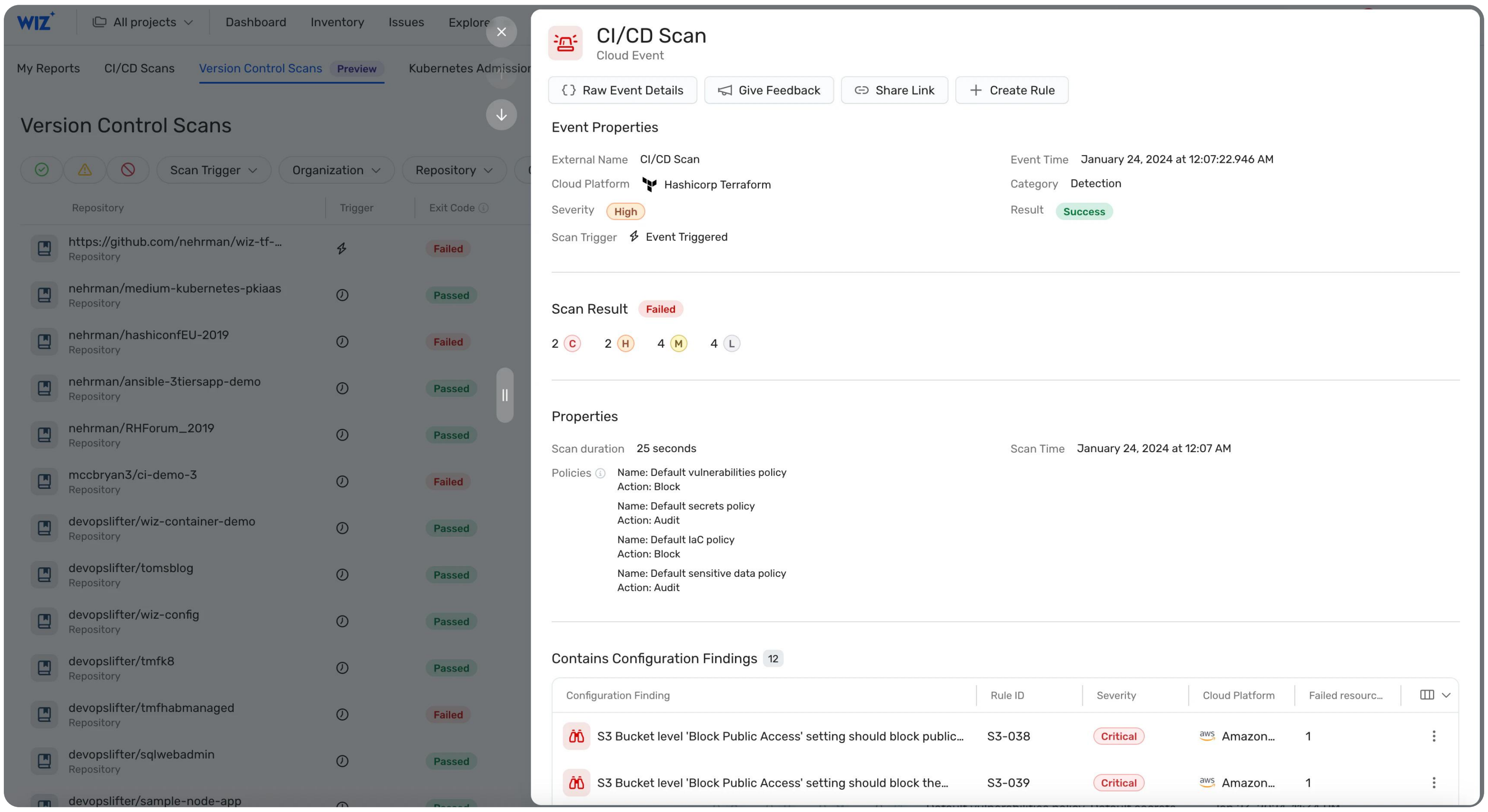
There have been more security incidents in your cloud environment recently due to risks that expose your critical infrastructure and data to attacks. You want to catch and fix issues before they ever reach production to ensure that deployments don't introduce new risks.

Challenges:

- Gaining visibility into exposure risks across the cloud
- Having the necessary context to understand if this is a risk worth spending valuable security time
- Bringing risk context and learnings from production to earlier in the development lifecycle

Solution:

Combining Wiz with Terraform brings posture management earlier in the development process.To start, Terraform takes the laC configuration and constructs a plan for the code. At the same time, Wiz's Run Task intervenes to scan, find a misconfiguration or exposed secret, and halt the deployment before it reaches the apply stage. Together, Terraform and Wiz ensure that publicly exposed secrets or misconfigurations that could open exposure points or lateral movements for attackers do not deploy to production.



Version Control Scans

Repository	Trigger	Exit Code
https://github.com/nehrman/wiz-tf-... Repository	⚡	Failed
nehrman/medium-kubernetes-pkiaas Repository	◷	Passed
nehrman/hashiconfEU-2019 Repository	◷	Failed
nehrman/ansible-3tiersapp-demo Repository	◷	Passed
nehrman/RHForum_2019 Repository	◷	Passed
mccbryan3/ci-demo-3 Repository	◷	Failed
devopslifter/wiz-container-demo Repository	◷	Passed
devopslifter/tomsblog Repository	◷	Passed
devopslifter/wiz-config Repository	◷	Passed
devopslifter/tmfk8 Repository	◷	Passed
devopslifter/tmfhabmanaged Repository	◷	Failed
devopslifter/sqlwebadmin Repository	◷	Passed
devopslifter/sample-node-app		

CI/CD Scan
Cloud Event

Event Properties

External Name: CI/CD Scan
Cloud Platform: Hashicorp Terraform
Severity: High
Scan Trigger: ⚡ Event Triggered
Event Time: January 24, 2024 at 12:07:22.946 AM
Category: Detection
Result: Success

Scan Result: Failed

2 C 2 H 4 M 4 L

Properties

Scan duration: 25 seconds
Scan Time: January 24, 2024 at 12:07 AM
Policies:
Name: Default vulnerabilities policy
Action: Block
Name: Default secrets policy
Action: Audit
Name: Default IaC policy
Action: Block
Name: Default sensitive data policy
Action: Audit

Contains Configuration Findings 12

Configuration Finding	Rule ID	Severity	Cloud Platform	Failed resourc...
S3 Bucket level 'Block Public Access' setting should block public...	S3-038	Critical	aws Amazon...	1
S3 Bucket level 'Block Public Access' setting should block the...	S3-039	Critical	aws Amazon...	1

Get started today

Sign up for a demo to learn more or check out the Wiz listing in AWS Marketplace to get started.

Get a Demo