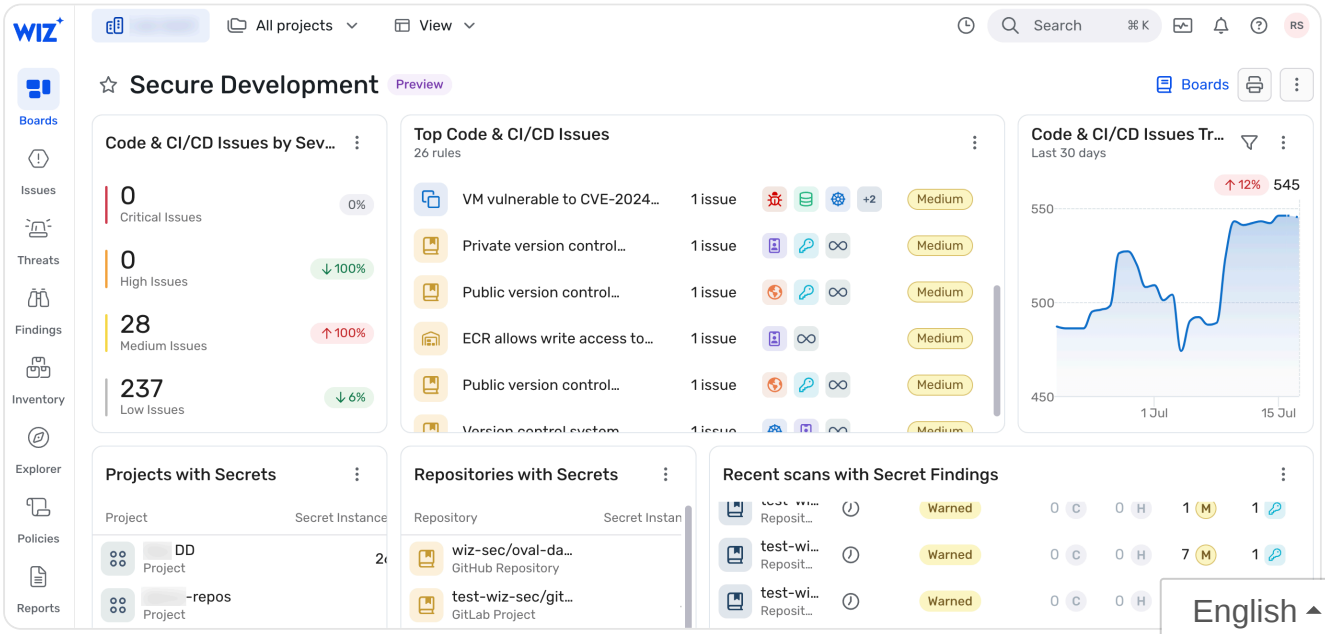
SDLC Security Posture

Wiz helps you secure the infrastructure of your SDLC (Software Development Lifecycle) by detecting misconfigurations and other security risks (e.g. identity and network exposure) in your version control systems (VCS) themselves. This reinforces the shifting left approach and enhances the security posture of your CI/CD pipeline. Learn how code scanning works in VCS and with Wiz CLI.

Support for SDLC Security Posture

To perform SDLC Security Posture, Wiz supports essential external compliance frameworks such as CIS GitHub 1.0.0, OWASP CI/CD Top 10 Risks, and OpenSSF Source Code Management Platform Best Practices and maps them to dedicated Controls and Cloud Configuration Rules. These frameworks help you manage source code, ensure secure coding practices, and safeguard against potential misconfigurations. See the guide on the OpenSSF Source Code Management Platform Best Practices framework.

To complement this compliance infrastructure, Wiz provides the built-in Wiz for Code & Supply Chain Security framework, aimed to assist in detecting risks in your code and VCSs. In addition, the built-in Secure Development board allows for exploring and monitoring easily the security posture of your CI/CD pipeline through widgets for metrics such as your OpenSSF compliance score, code & CI/CD Issues by severity, and repositories with secrets.



English

Detect misconfigurations in your SDLC

VCS Connectors use Cloud Configuration Rules to detect misconfigurations in your VCS. Each Cloud Configuration Rule for SDLC is a check that applies to a specific SDLC infrastructure tool type. For example:

- GitHub repository set to public (T-IAC-Rule-e2e02095-c6bb-2067-8081-63f5fe91c9aa)
- Repository should not allow workflows to approve pull requests (Repository-001)

Each Rule is defined by:

- Target platform (e.g. GitHub)
- Severity
- Scope—By default, all Cloud Configuration Rules apply to all applicable Cloud Organizations, but you can edit the Rule and scope it only to specific resources in specific Organizations
- Status (disabled or enabled)

> All Cloud Configuration Rules for SDLC include remediation steps detailing how to fix the misconfiguration in your VCS.

All Cloud Configuration Rules for SDLC are listed on the Policies > Cloud Configuration Rules page. You can filter them by clicking at the top Cloud Platform and choosing the relevant VCS. The most recent results of the cloud configuration assessment appear on the Findings > Cloud Configuration Finding page; this report is updated after every scan.

The process is as follows:

1. Every scan cycle, the VCS Connector fetches your VCS architecture and configuration.
2. Once data has been retrieved, all applicable Cloud Configuration Rules for SDLC are assessed against these Graph objects: Cloud Organization[1], User Account, Repository, and Repository Branch.
3. If one of the above fails a Configuration Rule assessment:
   i. It will be marked as `Unresolved` in the Findings > Cloud Configuration Findings page.
   ii. A Cloud Configuration Finding will be created and associated with it on the Security Graph. Use this query to see all Cloud Configuration Findings on the Security Graph.
4. If a resource passes a Configuration Rule evaluation:
   i. It is marked as `Passed` in the Findings > Cloud Configuration Findings page.
   ii. Previous Cloud Configuration Findings associated with it are removed from the Security Graph.

[1] Except for personal accounts which are modeled on the Security Graph as Organizations.

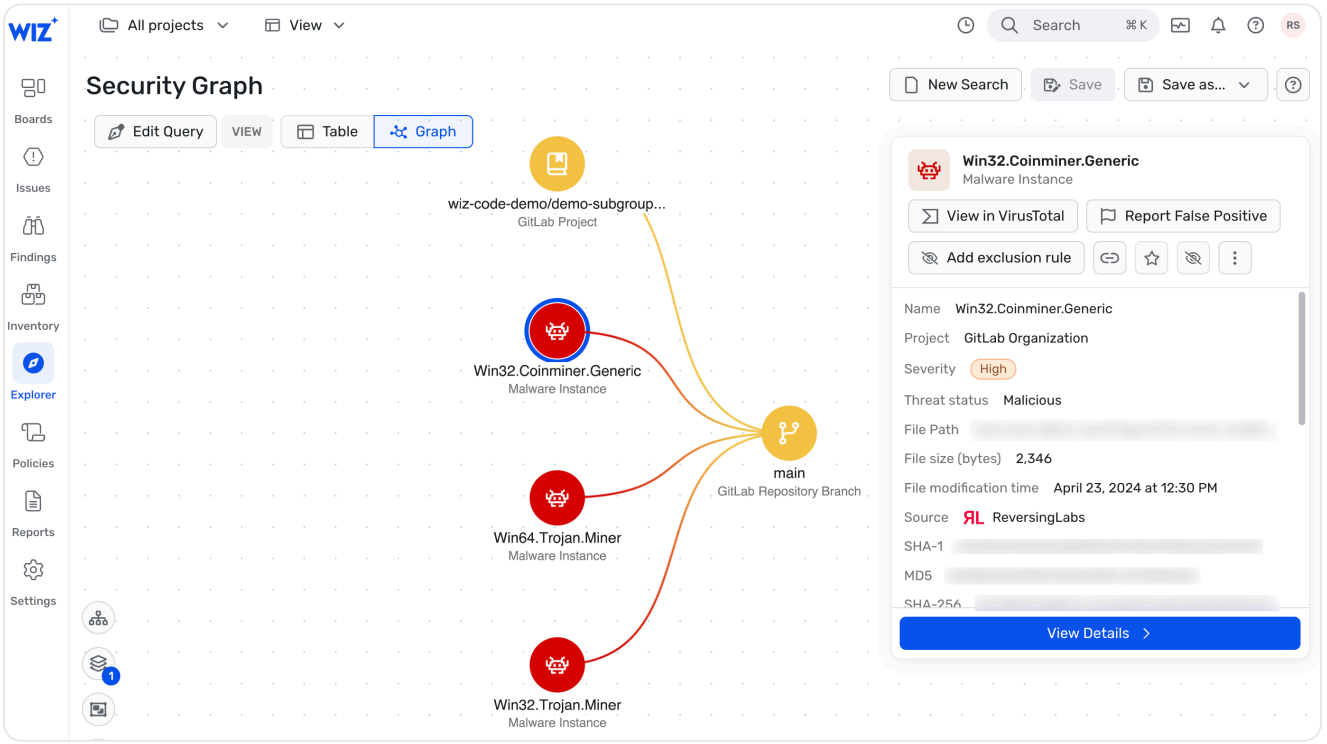
Learn about secure cloud configuration.

Detect other security risks in your SDLC

In addition to Cloud Configuration Rules to detect misconfigurations in your VCS, Wiz performs a context-based risk assessment; dedicated Controls correlate VCS misconfigurations with other risk factors and business impact risks to highlight your most critical Issues and help your organization prioritize remediation.

For example, consider the following Controls:

- Public version control system repository with pipeline that uses self-hosted CI runners (wc-id-1943)—External collaborators can potentially make commits and affect pipeline execution, e.g. access pipeline secrets.
- Public version control system repository hosting high/critical severity malware in the code (wc-id-2167)—A public repository with malware can act as a hub for spreading the malware externally while using the domain name of the hosting organization. Such malware can also end up in your production environment as part of the CI/CD pipeline.



- Organization with more than three owners (wc-id-2265)—Organization owners are highly privileged and could create great damage if compromised, so it is recommended to limit their number.

Updated 1 day ago

← Version Control Scanning

Analyze →