Agentless File Integrity Monitoring (FIM)

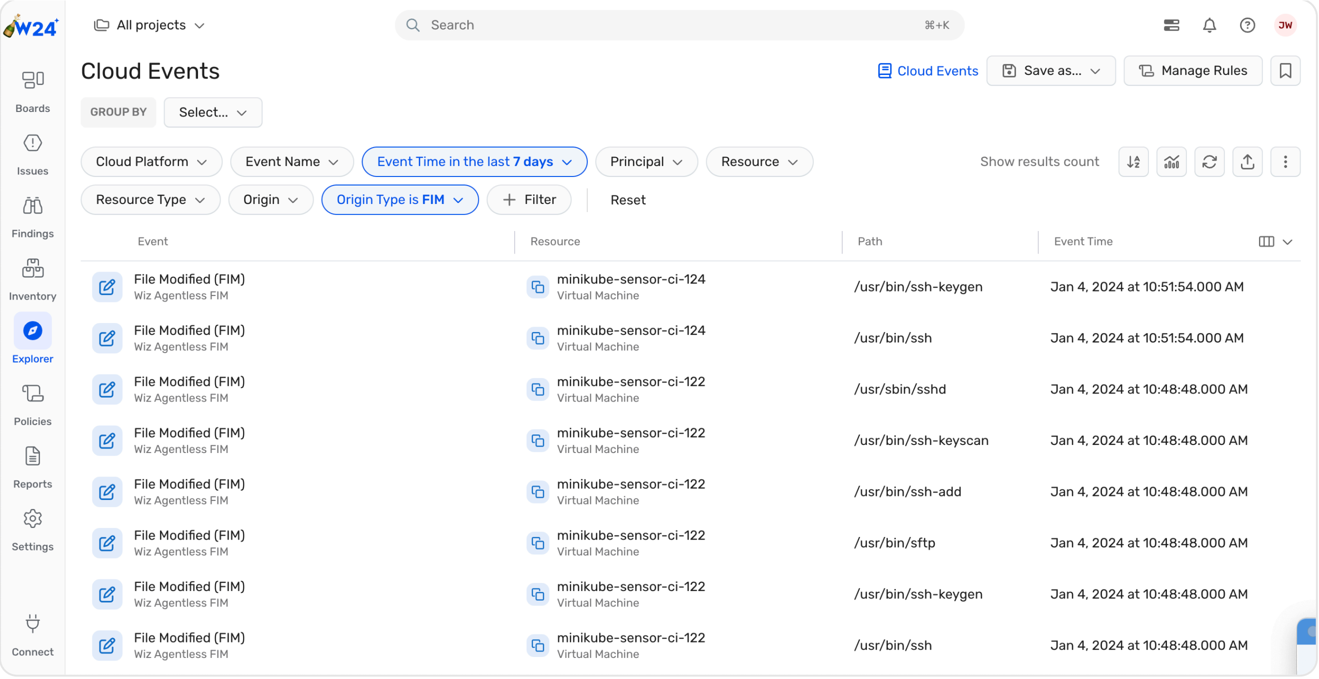
✓ This feature requires a Wiz/Gov Advanced license. Learn more.

File Integrity Monitoring (FIM) detects and alerts on unauthorized changes to important files on your VMs. By periodically scanning and comparing files to previous scans, Wiz can detect if a file was created, deleted, or modified.

Other tools provide FIM by installing an agent or externally monitoring VMs by network access. This approach can be challenging to maintain in large, dynamic cloud environments. Wiz utilizes its agentless capabilities for FIM, giving you near-complete monitoring of important file changes without having to maintain agents or external scanners.

How it works

When scanning a VM, Wiz analyzes the files by policy and compares them to the previous scan to identify any changes that have occurred. When a file was created, deleted, or modified compared to the previous scan, Wiz creates a File Modified (FIM) event on the Explorer > Cloud Events page.



Cloud Events

Event Time in the last **7 days**

Origin Type is **FIM**

Event	Resource	Path	Event Time
File Modified (FIM) Wiz Agentless FIM	minikube-sensor-ci-124 Virtual Machine	/usr/bin/ssh-keygen	Jan 4, 2024 at 10:51:54.000 AM
File Modified (FIM) Wiz Agentless FIM	minikube-sensor-ci-124 Virtual Machine	/usr/bin/ssh	Jan 4, 2024 at 10:51:54.000 AM
File Modified (FIM) Wiz Agentless FIM	minikube-sensor-ci-122 Virtual Machine	/usr/sbin/sshd	Jan 4, 2024 at 10:48:48.000 AM
File Modified (FIM) Wiz Agentless FIM	minikube-sensor-ci-122 Virtual Machine	/usr/bin/ssh-keyscan	Jan 4, 2024 at 10:48:48.000 AM
File Modified (FIM) Wiz Agentless FIM	minikube-sensor-ci-122 Virtual Machine	/usr/bin/ssh-add	Jan 4, 2024 at 10:48:48.000 AM
File Modified (FIM) Wiz Agentless FIM	minikube-sensor-ci-122 Virtual Machine	/usr/bin/sftp	Jan 4, 2024 at 10:48:48.000 AM
File Modified (FIM) Wiz Agentless FIM	minikube-sensor-ci-122 Virtual Machine	/usr/bin/ssh-keygen	Jan 4, 2024 at 10:48:48.000 AM
File Modified (FIM) Wiz Agentless FIM	minikube-sensor-ci-122 Virtual Machine	/usr/bin/ssh	Jan 4, 2024 at 10:48:48.000 AM

This event provides information about the specific file that was modified, including its path, event time, and the type of modification that occurred.

Validation

Since files are constantly changing, the number of events that surface can be quite overwhelming. This is why Wiz includes a validation process that helps you to gain additional insight into the origin of the new file or its modified content. This validation process is different for Windows and Linux:

› Windows verification process

› Linux verification process

For example, if a file was modified during an official Windows or Linux package update, this would be expected behavior and would not indicate any suspicious activity. However, if a file was modified and was not signed or known to be published by the official vendor, Wiz would not mark this change as `Verified`.

Monitored files

FIM monitors the following Windows, Linux and MacOS files:

Windows	Linux and MacOS
• `C:\autoexec.bat` • `C:\boot.ini`	• `/bin` • `/boot`

English ▲

Windows	Linux and MacOS

`C:\config.sys`
`C:\Windows\system.ini`
`C:\Windows\win.ini`
`C:\Windows\regedit.exe`
`C:\Windows\System32\userinit.exe`
`C:\Windows\explorer.exe`
`C:\Program Files\Microsoft Security Client\msseces.exe`
Under `C:\Windows\System32\`, the following file types are monitored:
`bat`
`cfg`
`conf`
`config`
`dll`
`exe`
`ini`
`sys`
	`/etc`
	`/sbin`
	`/usr/bin`
	`/usr/local/bin`
	`/usr/local/sbin`
	`/usr/sbin`
	`/usr/share/keyrings`
	`/var/spool/cron`
	`/opt/bin`
	`/opt/sbin`
	`/var/share/keyrings`
	`/var/share/cron`

File monitoring is recursive, meaning that Wiz processes files that are located in subfolders or nested directories within a folder. For example, if `/etc/` is listed, then the following files are also monitored:

- `/etc/file.config`
- `/etc/foo/file.config`
- `/etc/foo/bar/file.config`

Create FIM Event Policies and Automations

Isolate the most important FIM Events by creating a custom FIM Modified Threat Detection Rule. Creating a custom FIM Modified Threat Detection Rule allows you to:

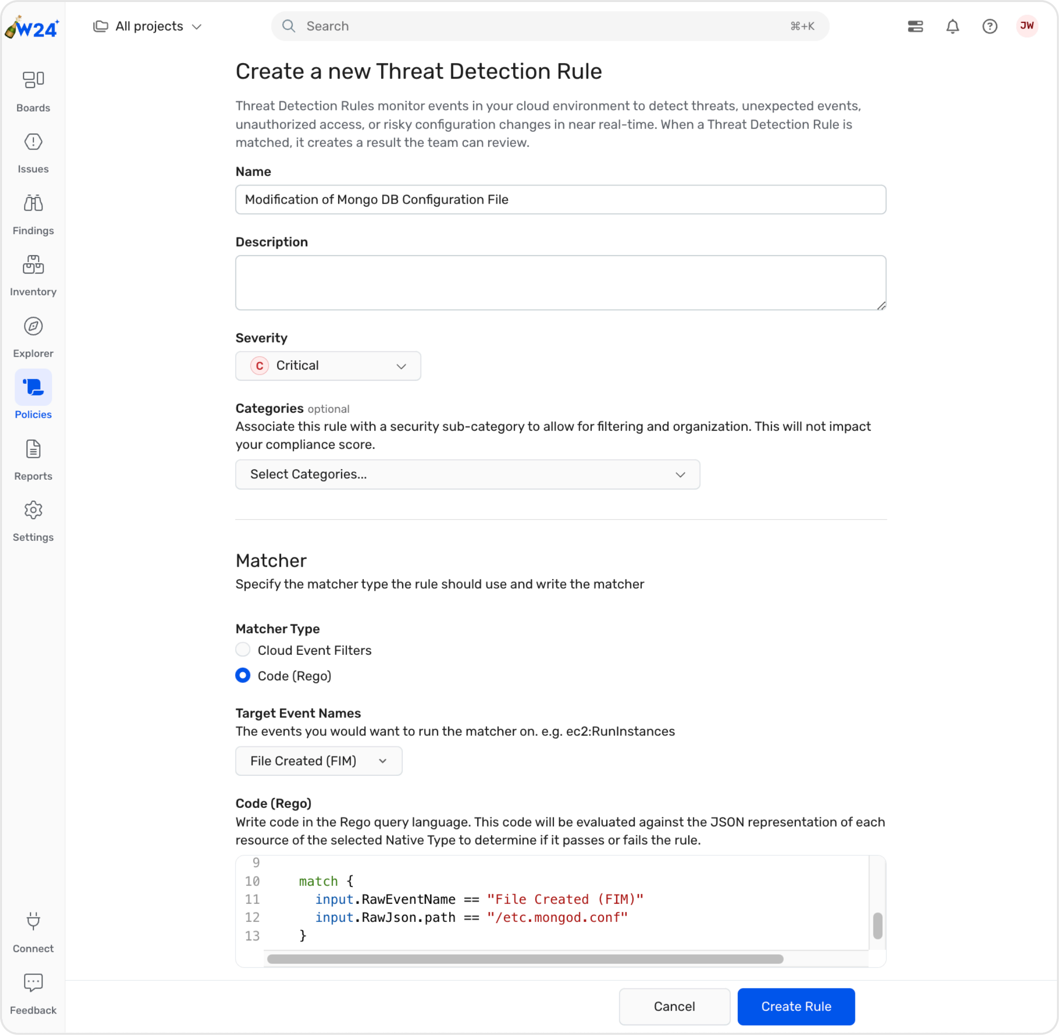
- Quickly identify any FIM-related issues that occur.
- Define Automation Rules to send notifications or create event tickets for high-priority FIM events.

Example workflow

Create a custom Threat Detection Rule, then create an Automation Rule to trigger the Action when the cloud event is detected:

1. [Create a custom Threat Detection Rule]() with a Target Event Name of File Modified (FIM).

   For example, create a custom FIM Modified Threat Detection Rule with a Critical severity to instantly send notifications on any modifications made to a MongoDB configuration file located in `/etc/mongod.conf` in your Production Project.



Create a new Threat Detection Rule

Threat Detection Rules monitor events in your cloud environment to detect threats, unexpected events, unauthorized access, or risky configuration changes in near real-time. When a Threat Detection Rule is matched, it creates a result the team can review.

Name

Modification of Mongo DB Configuration File

Description

Severity

C Critical

Categories optional

Associate this rule with a security sub-category to allow for filtering and organization. This will not impact your compliance score.

Select Categories...

Matcher

Specify the matcher type the rule should use and write the matcher

Matcher Type

○ Cloud Event Filters

● Code (Rego)

Target Event Names

The events you would want to run the matcher on. e.g. ec2:RunInstances

File Created (FIM)

Code (Rego)

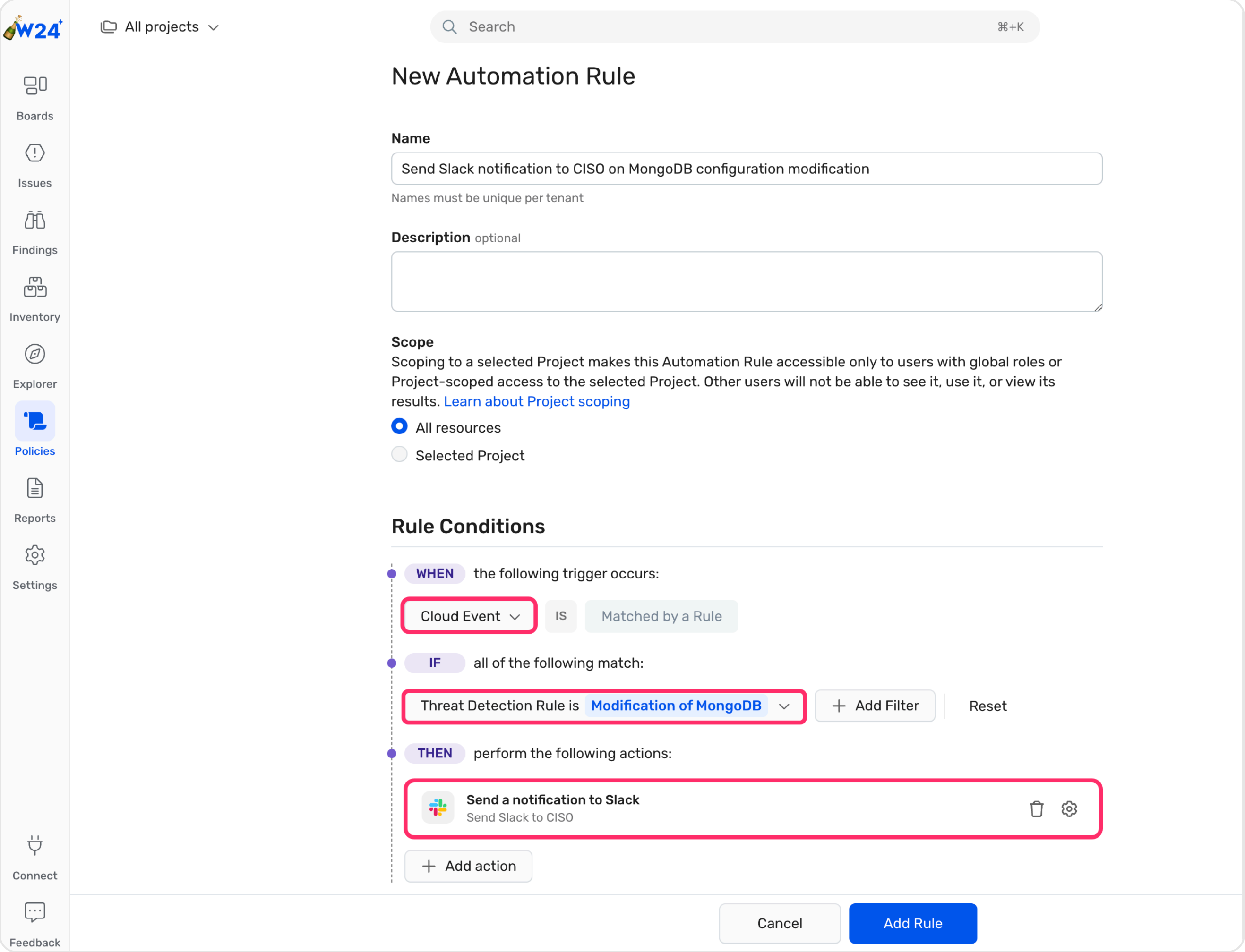
Write code in the Rego query language. This code will be evaluated against the JSON representation of each resource of the selected Native Type to determine if it passes or fails the rule.

```

  match {
    input.RawEventName == "File Created (FIM)"
    input.RawJson.path == "/etc.mongod.conf"
  }
```

2. [Create an Automation Rule from a Threat Detection Rule](). After creating a Custom Threat Detection Rule, you can then create an Automation Rule to trigger an Action when a cloud event is detected. In the following screenshot, an Automation Rule is created that will send a Slack notification to the SOC team when the custom rule to detect MongoDB configuration file modification is detected.

English ▲



New Automation Rule

Name

Send Slack notification to CISO on MongoDB configuration modification

Names must be unique per tenant

Description optional

Scope

Scoping to a selected Project makes this Automation Rule accessible only to users with global roles or Project-scoped access to the selected Project. Other users will not be able to see it, use it, or view its results. Learn about Project scoping

● All resources

○ Selected Project

Rule Conditions

WHEN the following trigger occurs:

Cloud Event IS Matched by a Rule

IF all of the following match:

Threat Detection Rule is Modification of MongoDB

THEN perform the following actions:

Send a notification to Slack
Send Slack to CISO

FAQ

Have a question? See the FAQ.

Updated 28 days ago

← Supported Resources for Cloud Configuration Rules

Agentless Software Bill of Materials (SBOM) →

Did this page help you? Yes No

English ▲