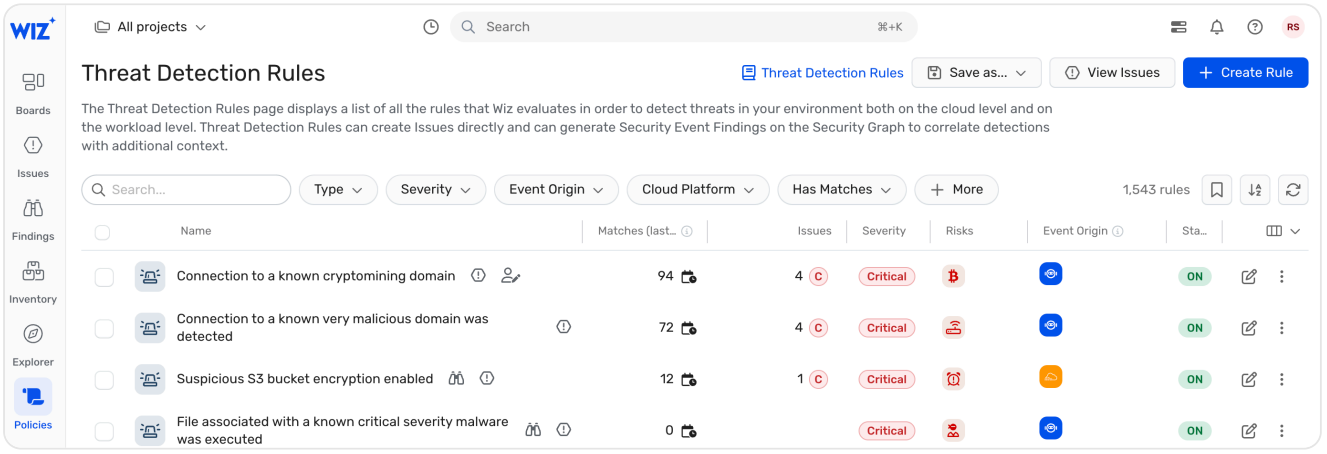
# Threat Detection Rules

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

The Threat Detection Rules page displays a list of all the rules that Wiz evaluates in order to detect threats, anomalies, unexpected events, unauthorized access, or risky change of configurations in near real-time on the cloud control plane and workloads in your environment. This allows security teams to get a new dimension of visibility in Wiz and helps reduce detection noise and prioritize remediation.

Learn about the different types of Threat Detection Rules.




From the Policies > Threat Detection Rules page, you can:

- View, filter, sort, or reorder Threat Detection Rules
- Generate Issues
- Generate Findings on the Security Graph
- Create a custom Threat Detection Rule
- Edit a Threat Detection Rule
- Create an Automation Rule from Threat Detection Rules

Runtime Sensor rules are available only when you have Wiz Runtime Sensors installed.

## View, filter, sort, or reorder Threat Detection Rules

By default, the Threat Detection Rules page lists all enabled and disabled rules ordered by severity.

- Click a Rule to view it and open its details drawer, listing all relevant information such as description, associated frameworks, any matches, and when it was last updated.

To search for, filter, sort, or reorder Threat Detection Rules:

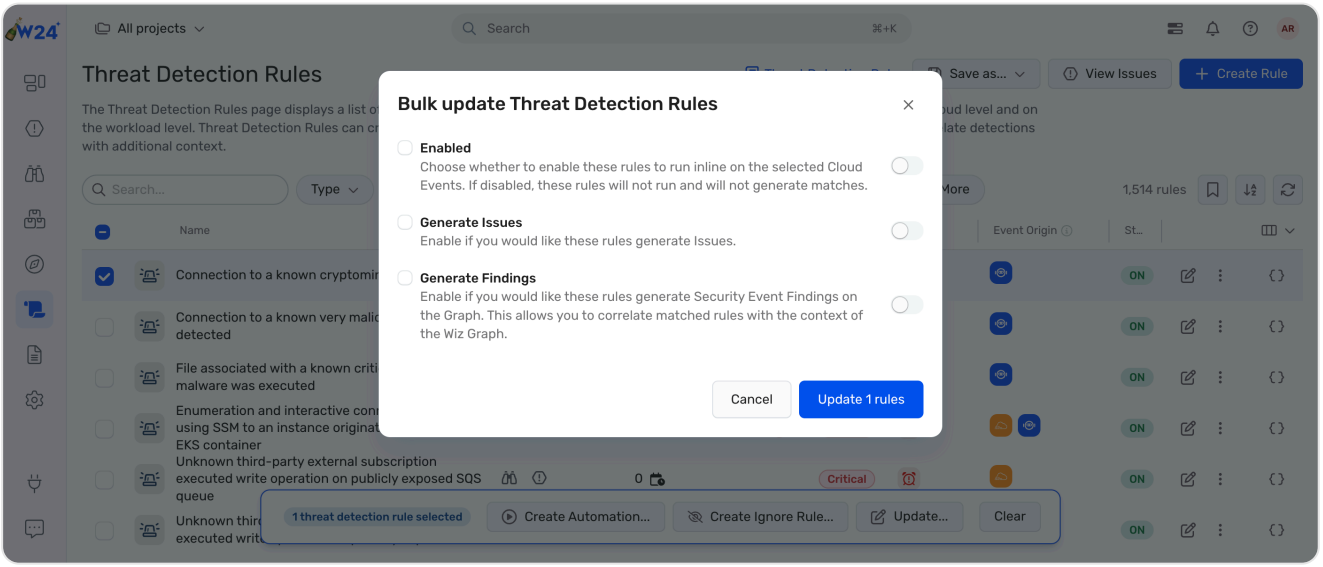
- Click the search bar and enter the name of a Threat Detection Rule
- Filter by Type, Cloud Platform, Target Event Name, Severity, Category, and more.
- Click + More for more filters
- On the right, click Order Options, then select a different ordering

For example, to view all Runtime Sensor rules, select Event Origin includes all Wiz Sensor (direct link).

## Generate Issues

If you want to investigate and prioritize certain Threat Detection Rules along with Wiz's other Issues, you can generate Issues from a rule. This further allows you to leverage Wiz's automation and remediation capabilities.

1. Navigate to the Policies > Threat Detection Rules page.
2. Review the list of rules. Select one or more rules you'd like Wiz to create Issues for, and click Update (at the bottom of the page).




3. Select Generate Issues, and click Update to save.
4. The next time this rule is matched, Wiz will generate an Issue. Click the rule to open the details drawer and review the related events, associated frameworks, and click to View on Graph.

## Generate Findings on the Security Graph

Some Threat Detection Rules can be noisy without all the relevant context. Wiz allows you to overlay threat detections with the Security Graph to add context and get higher fidelity correlated detections.

1. Navigate to the Policies > Threat Detection Rules page.
2. Review the list of rules. Select one or more rules you'd like to see on the Security Graph, and click Update (at the bottom of the page).
3. Select Generate Findings, and click Update to save.
4. A Security Event Finding is added to the graph.
5. You can also search for any Security Event Findings (direct link).

## Create a custom Threat Detection Rule

When a Threat Detection Rule is matched, it creates a result you or your team can review. You can generate Cloud Event rules or Workload Runtime Rules, which requires a Wiz Runtime Sensor version 1.0.3828 or later.

> Learn about Threat Detection Rules and their detection rate limits to understand what to expect once you create a Rule.

1. Navigate to the Policies > Threat Detection Rules page, then click Create Rule.
2. Select the rule Type–Cloud Event or Workload Runtime.
3. Give the event rule a meaningful name and a description.
4. Assign the rule a severity (from info to critical).
5. (Optional) Associate the Rule with a sub-category of a compliance framework.

   > This is for reference and filtering purposes only. Threat Detection Rules (whether built-in or custom) do not appear on the Reports > Compliance for Single Framework page nor affect your compliance scores.

6. Define the rule's matcher/conditions:

   For a Cloud Event Rule, select a Matcher Type:

   - Cloud Event Filters–Create or select a predefined filter. Using a filter allows you, for example, to include in the Rule also cloud events that are not currently present in your environment as well as filter according to the event's raw Json provided by the CSP.
   - Code (Rego)–

a. Click Target Event Names and select an event to target.

b. (Optional) Click the Code (Rego) code window to open the editor. See the detailed guide on Rego basics.

For a Workload Runtime Rule, define the Conditions:

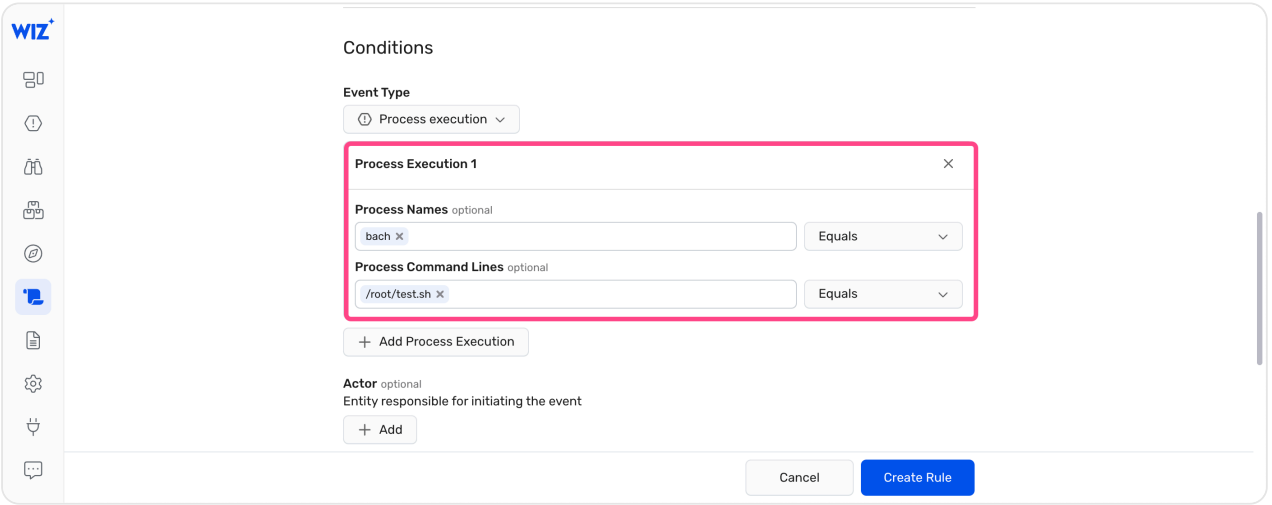
i.Event Type–(Mandatory) The specific type of event the Sensor monitors. A rule can be triggered by one of the following events: process execution, network connection, DNS query, or network listen.

### Process Execution

Use this event type to detect when certain processes are being executed. The detection is performed based on the process name (i.e. `bash`), the command line executing it (`cron -f /test.sh`), or a combination of both:

- Each separate parameter (Process Names / Process Command Lines) supports multiple values, which are evaluated using the `OR` operator. For example, you can detect Process Names `bash` or `zsh` or `ksh`.
- You can use Regex to define the parameters. For example, use '*' in a file path. Learn more about Regex.
- If you define both parameters (Process Names / Process Command Lines), then they are evaluated using the `AND` operator.

In the example screenshot below, the rule detects the `Bash` process which executed `/root/test.sh` as part of its command line.



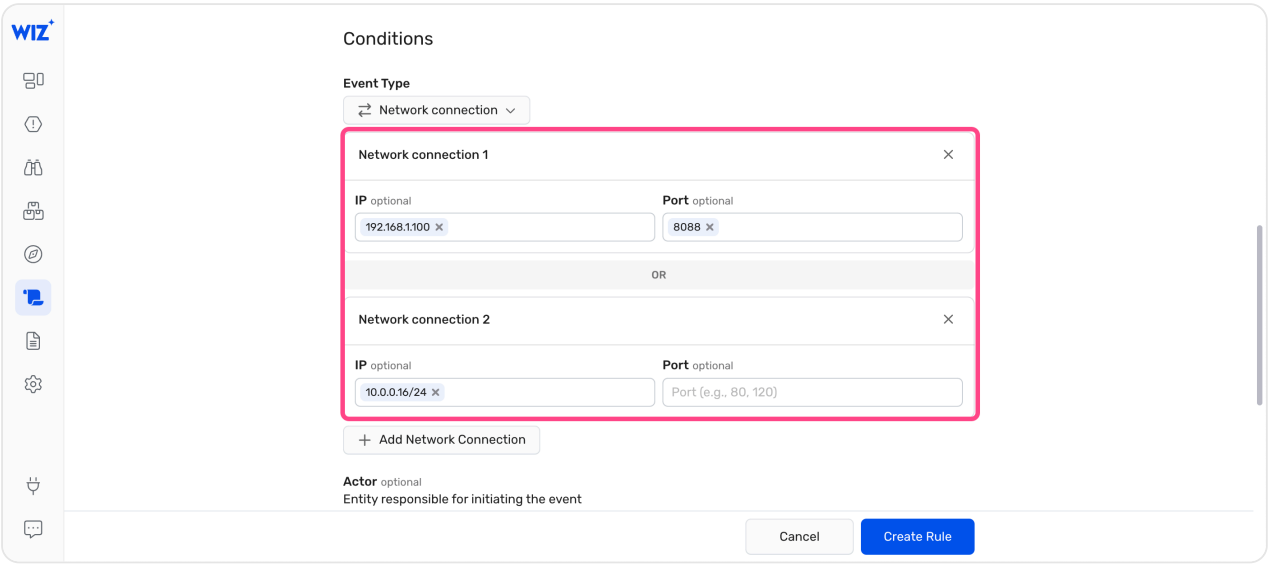

### Network Connection

Use this event type to detect outbound network connections established from your environment. The detection is performed based on outbound IP connections, outbound Ports, or a combination of both.

- Each separate parameter (IP / Port) supports multiple values, which are evaluated using the `OR` operator.

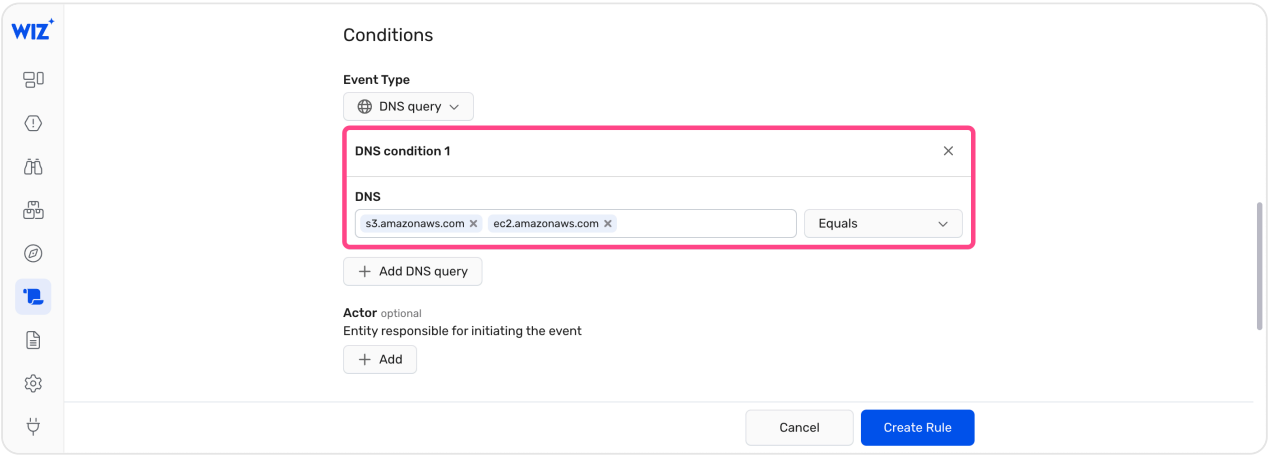
- If you define both parameters (IP / Port), then they are evaluated using the `AND` operator.

In the example screenshot below, the rule detects either an outgoing connection to IP and Port `192.168.1.100:8088`, or an outbound connection to an IP address within the `10.0.0.16/24` Classless Inter-Domain Routing (CIDR).




## DNS Query

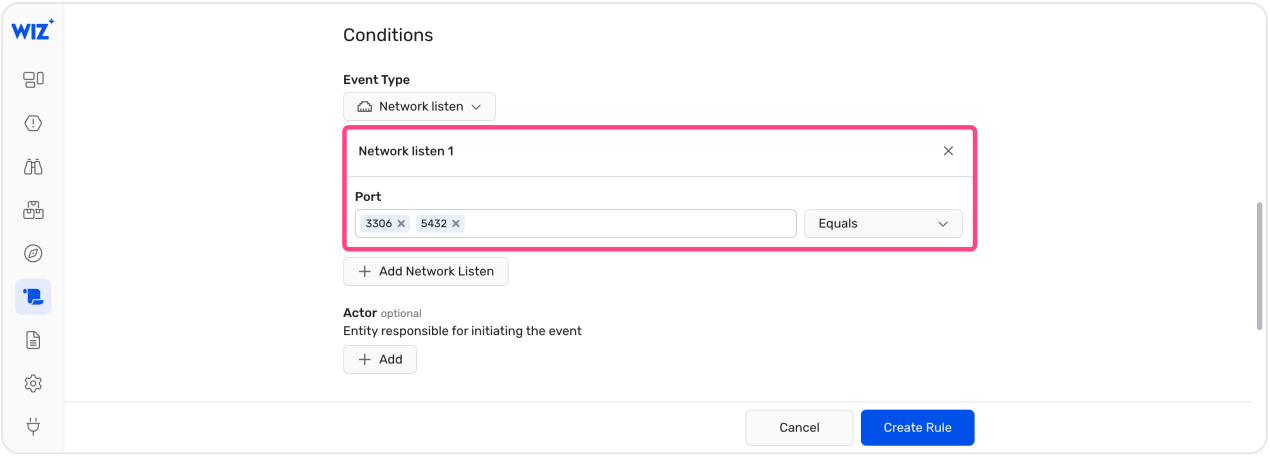
Use this event type to detect any DNS-lookup activity for selected DNS queries. You can use Regex to define the DNS, such as `\*.google.com`. Learn more about Regex.
In the example screenshot below, the rule detects the process' lookup activities to S3 buckets or EC2 instances.




## Network Listen

Use this event type to detect processes that are waiting for incoming connections from specific ports. You can use Regex to define the port numbers, if you want for example to define a range. Learn more about Regex.

In the example screenshot below, the rule detects incoming connections to either MySQL (port 3306) or PostgreSQL (port 5432) databases.




ii. Actor–(Optional) The container and/or process performing the event. Some events are legitimate unless performed by a specific actor. By adding the actor to the rule conditions you can really focus on the actual threats and reduce noise. The actor determines which processes, command lines, or containers are initiated by the event, and is also part of the detection. For example, create a rule that detects network listen events to either `MySQL` or `PostgreSQL` databases, which were initiated from an `ngnix` container.

7. Configure the following:
   i. Enable or disable the Rule to run inline on the selected cloud events.
   ii. Generate Issues.
   iii. Generate Findings.
   iv. Define the Project Scope. Learn about Project scoping.
8. Click Create Rule.
9. (Optional) Track the new Rule directly from the Sensor by navigating to the Deployments > Sensor page, selecting a specific Sensor within the deployment, and opening the details drawer. In the Custom Workload Runtime Rules column you can see the status of each Rule.

## Edit a Threat Detection Rule

1. For the rule you want to edit, click Editor Duplicated.
2. Edit the relevant information.
3. Click Save.

The update takes effect within a few minutes.

> Changing the severity of a Threat Detection Rule originating from the Wiz Runtime Sensor only changes the severity of any respective Issues generated

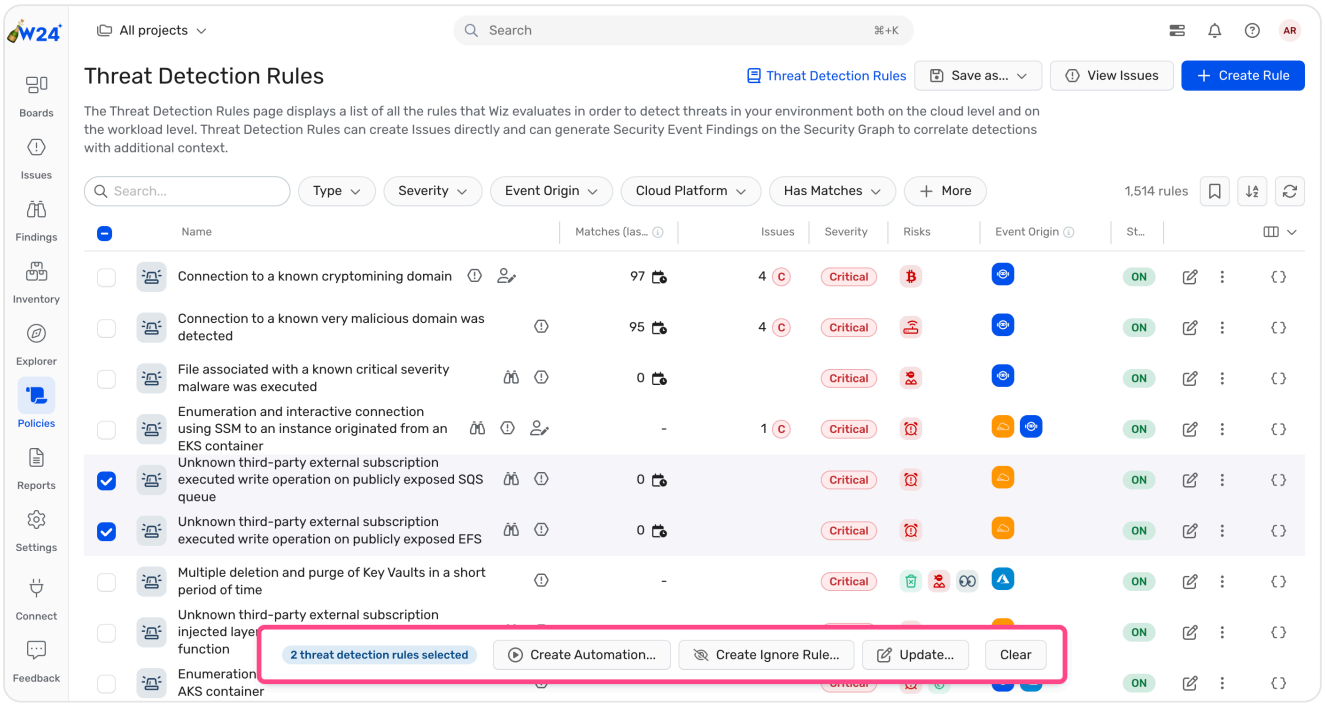
by it, not the severity of the cloud event.

## Create an Automation Rule from Threat Detection Rules

If you've defined an Integration with a third-party tool like Google Chat or Slack (see the guide on response and automation), you can create an Automation Rule to trigger the Action when a cloud event is detected.

To create an Automation Rule from a Cloud Rule:

1. Review the list of rules. Select one or more rules you'd like to see on the Security Graph, and click Create Automation (at the bottom of the page).




2. The New Automation Rule page opens with the Rule Conditions pre-populated.
3. Fill in the details for the new Automation rule. See the Integration-specific guide for the selected third-party tool.

Updated 24 days ago

← Image Trust Rules

Response Actions Catalog →