Threat Detection

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

The following scenarios provide step-by-step instructions to help you understand a few key ways we want you to use Wiz to identify and locate real-time risks.

Use cases exploring Cloud Detection & Response:

- Detect brute force attacks
- Create custom Rules based on cloud events
- Detect anomalous behavior
- Prioritize and triage CSP findings
- Troubleshoot using cloud events
- Correlate detections from external security solutions with Wiz context

Use cases that combine Cloud Detection & Response and Runtime Sensor detections:

- Detect malicious activity in real-time
- Detect malware execution in real-time
- Detect threats originating from a malicious IP/domain
- Detect lateral movement from workloads to the cloud control plane
- Investigate & respond to threats using Runtime Execution Data (RED)
- Ignore container-drift detections
- Export Runtime Sensor detections to your SIEM
- Use a response playbook to isolate a compromised node
- Harden production environments using runtime policies

Cloud Detection & Response

Detect brute force attacks

A brute force attack is an example of an ongoing attack that cannot be identified by a single event but by correlating multiple events.

1. In Wiz, go to the Issue page.
2. Filter for Type is Threat Detection.
3. Choose an Issue indicative of a brute force attack, such as Large number of failed logins followed by a successful login to your AWS Console by a highly privileged user (direct link), and click to open the details drawer:
   - Inspect the Issue evidence to understand what the user has done
   - Inspect the primary resource for further remediation

Create custom Rules based on cloud events

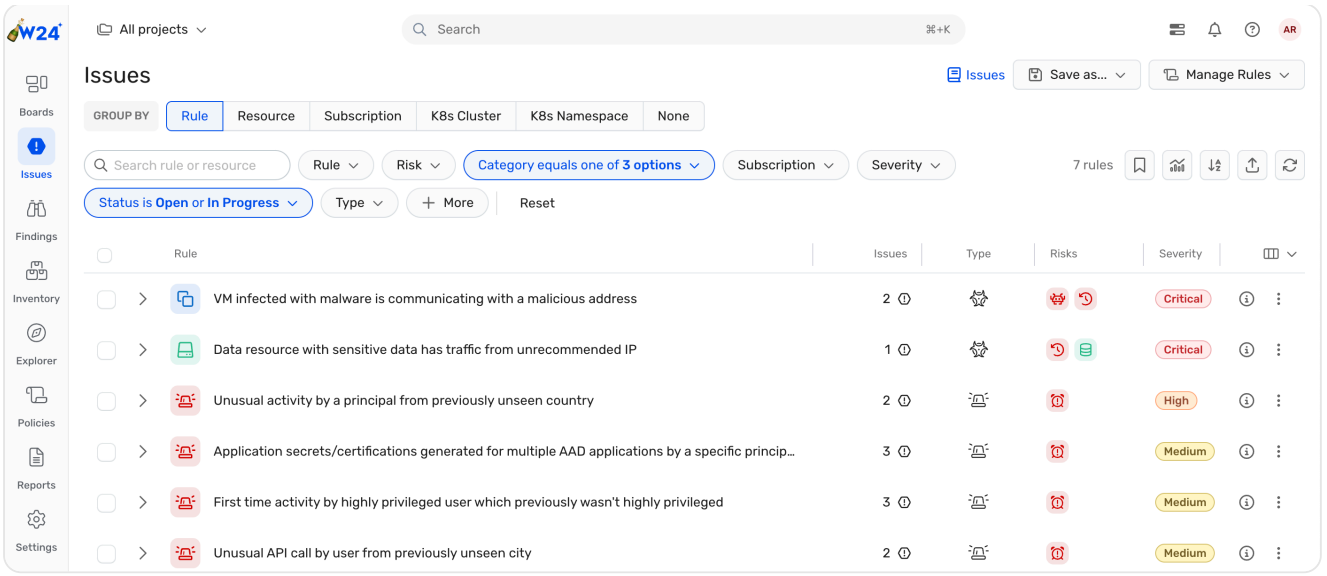
You can create a custom Threat Detection Rule using cloud events filters, including filtering on specific paths in the cloud event's raw json file. When a Threat Detection Rule is matched, it creates a result you or your team can review.

1. In Wiz, go to the Explorer > Cloud Events page.
2. Choose the filters for your new rule. For example, to detect when a security group rule is added with the IP range 0.0.0.0/0 (direct link).
3. On the top bar, click Save As > Threat Detection Rule.
4. Fill in the rule name, description, and configuration. Learn more about these options.
5. Click Save.

Detect anomalous behavior

Wiz can detect anomalies in your cloud environment by comparing cloud events with historical data, and alert when an unusual event (based on parameters like IP address, user agent, and more) is detected.

1. In Wiz, go to the Issues page.
2. In the Status filter, filter for Open or In Progress Issues.
3. In the Category filter, select the following options under the "Wiz for Threat Detection" framework: Anomalous execution, Anomalous credential usage, and Abnormal sourced communication (direct link).
4. Review the list of Issues and investigate to determine if the behavior that triggered the anomaly is malicious. For example, Wiz can detect unusual activity by a highly-privileged principal from a previously unseen country.



Prioritize and triage CSP findings

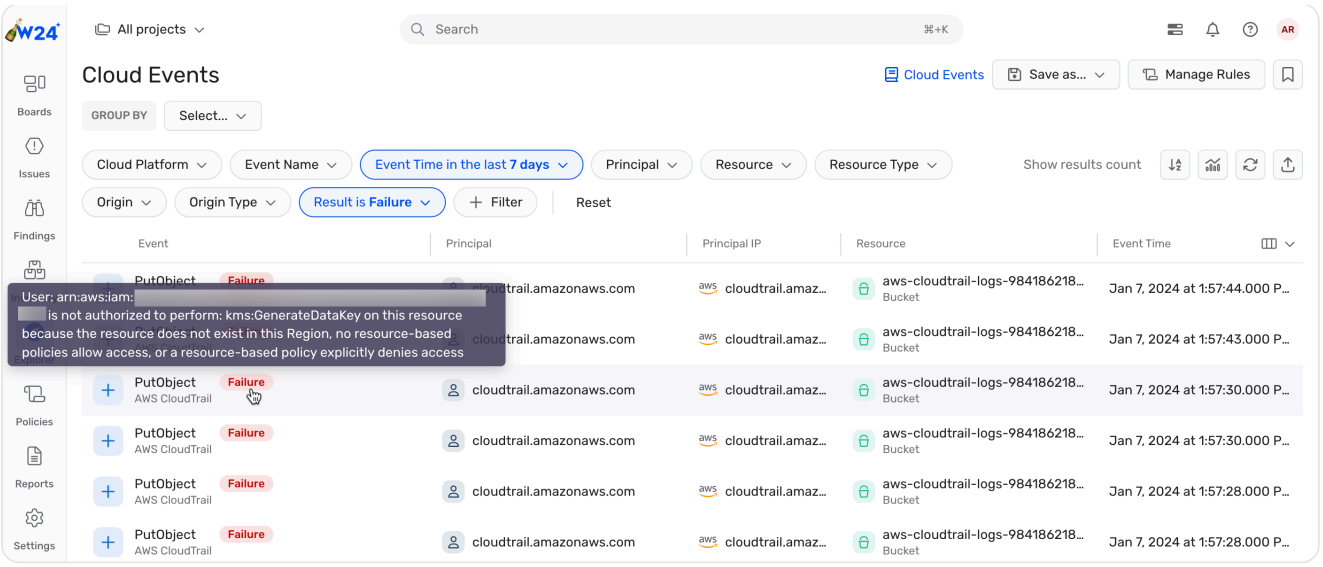
Using Controls, Wiz correlates the Security Graph data (i.e. external exposure and privilege escalation) with threat detections ingested from your CSP. This correlation provides additional context to help you prioritize and remediate these Issues.

1. In Wiz, go to the Issues page.
2. Filter for events in Status Open or In Progress, where the Risk includes any suspicious event (direct link).
3. Review the list of Issues (such as SSH Brute Force attempts on an admin publicly exposed VM) and investigate to determine if the behavior that triggered the rule is malicious.

Troubleshoot using cloud events

You can leverage Wiz Cloud Events to investigate and troubleshoot failed actions in your CSP control plane.

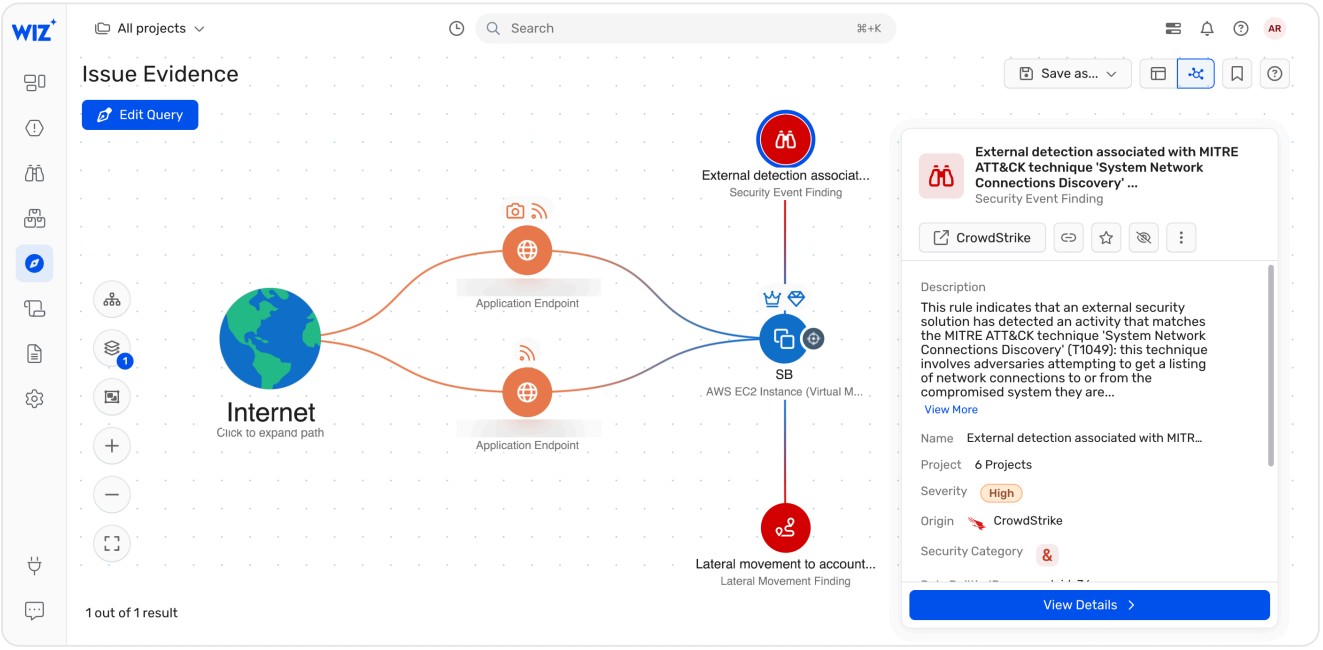
1. In Wiz, go to the Explorer > Cloud Events page.
2. Select or search for the cloud event you want to investigate. If the cloud event failed, hover over its badge to see the error message and remediate accordingly.



Correlate detections from external security solutions with Wiz context

Using Threat Detection Rules and Controls, Wiz correlates Cloud Events and Security Graph data (i.e. sensitive data and lateral movement) with threat detections imported for external security solutions (e.g. CrowdStrike). This correlation provides additional context and visibility to help prioritize and remediate these threats and issues.

1. In Wiz, go to the Issues page.
2. Filter for open or in-progress Issues detected on virtual machines, where the Risk includes any suspicious event (direct link).
3. Review the list of Issues (such as VM with a lateral movement finding to admin and discovery attempts detected in runtime) and investigate to determine if the behavior that triggered the rule is malicious.



Cloud Detection & Response and Runtime Ser

> All use case in this section require a Wiz Runtime Sensor

Detect malicious activity in real-time

By looking only at Issues that were originated by the Runtime Sensor and categorized as malicious by Wiz, you can monitor all aspects of the running workload in order to monitor potential threats.

1. In Wiz, go to the Issues page.
2. Click +Filter and select Rule Source is Wiz Sensor.
3. Narrow down the scope to Critical and High severity Issues. (direct link)
4. Review the Issues and find one you want to investigate, such as Process established connection to known cryptomining domain. Click it to open the details drawer:

- Look at the process tree to understand what caused the detection. You can see there the complete execution flow from the virtual machine to the container and the processing running in it.
- Look at the details of the running container for Kubernetes context (such as image name, pod, namespace, and controller).
- Look at the details of the malicious process that was executed (such as file path, file hash, command line, and execution time). You can further verify the file hash in VirusTotal.

Detect malware execution in real-time

You can identify the presence of malware that was executed in your environment.

1. In Wiz, go to the Issues page.
2. Click +Filter and select Rule Source is Wiz Sensor.
3. In the Rule name field, type "File associated" and hit Enter. (direct link)
4. If detected in your environment, you will see up to four different Issues types: "File associated with a known critical/high/medium/low severity threat was executed". Click an Issue to open its details drawer and review them:
   - Look at the event execution time to understand when the event happened.
   - Review the File Reputation details, populated by the Wiz File Reputation Service.

Detect threats originating from a malicious IP/domain

Wiz identifies malicious IP addresses and domains that might be associated with cyber attacks, data breaches, or other malicious activities. Learn how Wiz detects r

IP addresses and domains.

1. In Wiz, go to the Policies > Threat Detection Rules page.
2. From +More filters, select Source is Wiz Sensor. (direct link)
3. Review all the Runtime Sensor rules. Add Has matches equals True.
4. Click a rule you want to investigate, such as Connection to a known very malicious domain was detected. You are directed to the Issues page to review all Issues generated for malicious IP addresses or domains.
5. Review the Issues. Click on one to open its details drawer and investigate the domain reputation and the DNS query that called it. Investigate further the event details–look at the process tree and primary resources.

Detect lateral movement from workloads to the cloud control plane

Wiz can detect malicious activity in your environment by correlating workload activity with cloud control plane activity. This provides visibility and the ability to detect complex lateral movement attacks.

1. In Wiz, go to the Policies > Threat Detection Rules page.
2. Filter for rules originated by the Wiz Sensor, and for example AWS CloudTrail (direct link) or GCP Audit Logs (direct link).
3. Review the list of Issues and investigate to determine if the behavior that triggered the rule is malicious. For example, Wiz can detect Enumeration and RCE execution on instance(s) using the EC2 UserData attribute originated from an EKS container (direct link).

Investigate & respond to threats using Runtime Execution Data (RED)

The Runtime Sensor collects runtime execution data (RED), an aggregated collection of runtime activity recorded from the past 48 hours, that provides visibility into notable activity on both host and container levels. RED includes process executions, command lines, DNS queries, loaded files/modules, and more.

RED allows you to answer questions such as:

- What was the initial access point?
- Did the attacker spread to other resources, and if so, how?
- Did the attacker gain persistence in the environment, and if so, how?

Learn how RED logs for container forensics can help streamline your investigation of a detection, for example, a malware dropper and an XMRig miner.

Investigate a malware dropper

In this example we start out with a medium severity detection about a dropped payload, and use RED logs to pivot between executions within the resource and collect important artifacts for investigation.

1. In Wiz, go to the Explorer > Cloud Events page.
2. Search for Event name equals File created/modified by an ingress tool that established a remote connection (direct link), a medium severity detection generated by the Sensor when a payload is dropped on a resource/container.
3. Click the event to open the details drawer. Scroll down to the process tree and locate the executed command line. Extract the domain from the command line (i.e. `threat-demo-dropper.s3.amazonaws.com` in our example). Close the details drawer.
4. Now, click the pod to open its details drawer. Locate the associated container under the Contains Container section, and click it. Go to Forensics > Runtime Execution Data tab.
5. Search for the domain in the logs to see what you can uncover. In our example, a `wget` command has dropped a `dropped_malware` file into a temp directory.
6. Continue investigating the `dropped_malware` file to learn what it is communicating with by searching the logs. In our example, we learn that `dropped_malware` has initiated a DNS query to another domain, `threat-demo-c2.s3.amazonaws.com`.

Investigate an XMRig miner

In this example we collect important artifacts to help you investigate a miner incident.

1. In Wiz, go to the Explorer > Cloud Events page.
2. Search for Event name equals Malware Execution (direct link), a detection generated by the Sensor Reputation Service.
3. Click the event to open the details drawer. Scroll down to the process tree and locate the executed command line. Extract the name of the miner executable from the command line (i.e. `xmrig` in our example). Close the details drawer.
4. Now, click the pod to open its details drawer. Locate the associated container under the Contains Container section, and click it. Go to Forensics > Runtime Execution Data tab.
5. Search for the executable to learn which pool it has contacted. For example, `xmrig` contacted `xmr.pool.my-pool123.xyz`.
6. In order to see if there is another miner instance on the resource, search for more processes that may have contacted the pool. In our example, searching f

`xmr.pool.my-pool123.xyz` revealed that there is another miner instance named `cr0nd`. The hash of this miner instance is not known because the miner was compiled with its configuration, and the combination of the wallet and the pool are unique.

Create a RED report and export it to your data storage (S3, GCP Bucket)

Learn how to create and export a RED report to a bucket on an hourly basis. Every hour, Wiz will gather all the new raw data from the scoped machines with a Runtime Sensor and send the report to the selected data storage, allowing you to further streamline it to 3rd party tools such as SIEM. This workflow enables proactive hunting activities and assists with in-depth investigation during incident response.

1. In Wiz, go to My Reports > Create a Report > Runtime Execution Data (RED).
2. Create the new report, and make sure to:
   i. Give the report a meaningful name (for example: Hourly RED export to S3).
   ii. Choose the report scope, allowing you to retrieve RED insights from Sensors located on different machines.
   iii. Select an hourly report scheduling.
   iv. Select the target data storage. The RED report is exported as a JSON and each new file is created with the dedicated timestamp.
3. When you are done setting up the report, click Create Report.

Ignore container-drift detections

Not all container-drift instances in your environment are indicative of threat. Using Ignore Rules, you can set Wiz to ignore the detections for a specific Sensor rule ensuring that legitimate activities are not flagged as incidents (for example, ignore a container drift detection).

> This use case assumes you are familiar with Ignore Rules work and how to create one in Wiz.

In this example, we will create an Ignore Rule for the Sensor rule Container drift–executable not present in container image was executed if it was detected in the "demo-scenarios" (as the primary resource) and the command line contains `legit.app`.

1. In Wiz, go to the Policies > Threat Detection Rules page.
2. Start typing the name of the rule: "Container drift" and hit Enter (direct link). Review the Rule and the Issues it generated, and make sure the details are legitimate and benign.

3. Now, go to the Policies > Ignore Rules page, and click + Create Rule.
4. Follow the steps to create an Ignore Rule, while ensuring to choose the specific rule, primary resource, and command line:
    i. For Target Findings:
        a. In Finding Type, select Threat Detections.
        b. In Threat Detection Rules, choose the specific Sensor rule you want to ignore (in our example, "Container drift–executable not present in container image was executed").
    ii. For Target Resources:
        a. Select Resources matching a filter set.
        b. Add the filter Kubernetes Cluster is demo-scenarios.
    iii. For Target Evidence:
        a. In Additional Event Properties, add Command line contains legit.app.
5. Once you have finished editing all the relevant fields, click Create Rule.

Ignore Rules take effect within an hour. You can later review any ignored findings and edit the Ignore Rule if necessary.

Export Runtime Sensor detections to your SIEM

You can ingest raw threat detections originating from the Runtime Sensor into a third-party tool of your choice, such as a SIEM, for further management and investigation. To do so, you need to set up a new automation action in Wiz.

> This use case assumes you are familiar with Wiz's Automation Rules and Actions and does not provide an in-depth explanation of all parameters and options. For more information or background on this topic, refer to the Automation Rules guide.

1. In Wiz, go to Policies > Automation Rules.
2. Click +Add Rule.
3. Give the rule a meaningful name (e.g. "New critical runtime detections from Wiz"), an optional description, and select the project scope.
4. In Rule Conditions, choose:
    i. WHEN = Cloud Event
    ii. IF = Origin is Wiz Sensor
    iii. THEN = Choose up to 10 actions to perform
5. Scroll to the bottom of the page to preview the existing cloud events that match the selected "IF" filters. Verify that the filter results match your expectations.

> The new Automation Rule will not be triggered for all existing cloud events shown in the preview, only for future ones that meet the selected crite

6. Click Add Rule.

Use a response playbook to isolate a compromised node

- This use case is based on Wiz's Secure Auto-Remediation and requires that you have it set up for AWS along with at least one SNS remediation playbook. Currently, only AWS is supported for cloud-native response playbooks. More CSPs are coming soon!
- Currently supported only for the following [Threat Detection Rules] (https://app.wiz.io/policies/cloud-event-rules#~(filters~(generateIssues~(equals~true))))

This use case demonstrates how to view a detection on a Kubernetes node (VM), inspect it, and use the node isolation playbook to contain the incident, thereby limiting its impact:

1. In Wiz, go to the Issues page.
2. Filter for Threat Detection Issues, for VMs, which are in "Open" or "In progress" status (direct link). This query displays Issues on Kubernetes nodes (aka VMs).
3. Inspect the Issue by opening the details drawer and review the available evidence such as the process tree, context, and forensics to determine the nature of the detection and understand if it constitutes an incident.
4. Once you have identified the incident, click Run Action and select the relevant SNS integration to trigger the response playbook. For example, a playbook that removes IAM roles to restrict permissions and eliminate all security groups to contain the incident.

Harden production environments using runtime policies

One example of hardening your production environment using runtime policies is to terminate a container attempting to connect to a domain that is not in your tenant's allow list. This use case requires the following:

1. In Wiz, go to the Policies > Threat Detection Rules page.
2. Click Create Rule, and create a custom Threat Detection Rule of type Workload Runtime with the following conditions:
3. Select Event Type is DNS Query:
   i. In the DNS field, write the allowed domains. In our example, we use `app.wiz.io` and `auth.wiz.io`.
   ii. As the logical parameter, select not equals.
4. Add an Actor. Under Container Names, add the name of the container you want the Rule enforced on. In our example, we use `login-service`.
5. Configure any other parameters and click Create Rule.

6. The first time the Rule identifies container `login-service` trying to connect to a domain that is not `app.wiz.io` or `auth.wiz.io`, it will generate a match (and Issues/Findings if you defined so). Review the Rule and its matches and tweak it as needed.
7. When you are satisfied with the Rule's matches, create a Runtime Response Policy that blocks this altogether.

Updated about 2 months ago

← Serverless

Securing AI →