

ThreatQuotient

A Securonix Company



Wiz CDF

Version 1.1.0

September 08, 2026

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 **ThreatQ Supported**

Support

Email: tq-support@securonix.com

Web: <https://ts.securonix.com>

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
Support	4
Integration Details	5
Introduction	6
Prerequisites	7
Installation	8
Configuration	9
Wiz Issues Configuration Parameters	9
Wiz Threat Detections Configuration Parameters	11
ThreatQ Mapping	13
Wiz Issues	13
Wiz Value to ThreatQ Value Mapping	20
Wiz Threat Detections	21
Average Feed Run	23
Wiz Issues	23
Wiz Threat Detections	23
Change Log	24

Warning and Disclaimer

ThreatQuotient, Inc. provides this document "as is", without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein.

ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2026 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: tq-support@securonix.com

Support Web: <https://ts.securonix.com>

Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.1.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The Wiz CDF integration retrieves security issues and threat detection findings from Wiz. Retrieved data can be filtered by project, severity, and issue type.

The integration provides the following feeds:

- **Wiz Issues** - ingests Wiz security issues.
- **Wiz Threat Detections** - ingests Wiz Threat Detection findings.

The integration ingests the following object types:

- Attack Patterns
- Incidents
 - Incident Attributes
- Indicators
- Vulnerabilities

Prerequisites

The following is required in order to run the integration:

- Wiz Hostname
- Wiz Client ID
- Wiz Client Secret
- Optional - mapping Wiz MITRE TIDs to MITRE ATT&CK attack patterns requires prior ingestion of the data via the MITRE ATT&CK CDF integration.

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the file on your local machine



ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

The feed will be added to the integrations page. You will still need to [configure and then enable](#) the feed.

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

Wiz Issues Configuration Parameters

PARAMETER	DESCRIPTION
Wiz Hostname	Enter the Wiz Hostname to connect to the API. Do not include the protocol (http/https). Commercial Tenants - you can use the regional endpoints. For example: <code>api.<region>.app.wiz.io</code>. Replace the <code><region></code> tag with your region: <code>us1</code>, <code>us2</code>, <code>eu1</code>, or <code>eu2</code>. GovCloud Tenants - you can use <code>api.<region>.gov.wiz.io</code>.
Client ID	Enter your Wiz Service Account's Client ID to authenticate with the API.
Client Secret	Enter your Wiz Service Account's Client Secret to authenticate with the API.

PARAMETER	DESCRIPTION
Project ID Filter	Optional - Enter a line-separated list of Project IDs to filter the issues by.  This allows you to only ingest issues that affect specific projects.
Type Filter	Select which issue types to ingest. Options include: ◦ Toxic Combination (<i>default</i>) ◦ Cloud Configuration (<i>default</i>) ◦ Threat Detection (<i>default</i>)
Severity Filter	Select which severity levels an issue must have to be ingested. Options include: ◦ Critical (<i>default</i>) ◦ High (<i>default</i>) ◦ Medium (<i>default</i>) ◦ Low (<i>default</i>) ◦ Informational
Ingest Security Subcategories as Attributes	Enable this parameter to ingest security subcategories as attributes. This is disabled by default to prevent attribute pollution as there can be many subcategories. Enable this option if you plan to do analytics around the subcategories.
Ingest Project Names as Attributes	Enable this parameter to ingest project names as attributes. This is disabled by default to prevent attribute pollution in the case of an issue affecting many projects. Enable this option if you plan to do analytics around the affected projects.(
Ingest CVEs As	Select which entity/object type to ingest the CVEs as. Options include:

PARAMETER	DESCRIPTION
	◦ Vulnerabilities (<i>default</i>) ◦ Indicators (Type: CVE)
Enable SSL Certificate Verification	Enable or disable verification of the server's SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

Wiz Threat Detections Configuration Parameters

PARAMETER	DESCRIPTION
Wiz Hostname	Enter the Wiz Hostname to connect to the API. Do not include the protocol (http/https). Commercial Tenants - you can use the regional endpoints. For example: <code>api.<region>.app.wiz.io</code>. Replace the <code><region></code> tag with your region: <code>us1</code>, <code>us2</code>, <code>eu1</code>, or <code>eu2</code>. GovCloud Tenants - you can use <code>api.<region>.gov.wiz.io</code>.
Client ID	Enter your Wiz Service Account's Client ID to authenticate with the API.
Client Secret	Enter your Wiz Service Account's Client Secret to authenticate with the API.
Project ID Filter	Optional - Enter a line-separated list of Project IDs to filter the detections by.

PARAMETER	DESCRIPTION
	 This allows you to only ingest issues that affect specific projects.
Severity Filter	Select which severity levels a detection must have to be ingested. Options include: ◦ Critical (<i>default</i>) ◦ High (<i>default</i>) ◦ Medium (<i>default</i>) ◦ Low (<i>default</i>)
Enable SSL Certificate Verification	Enable or disable verification of the server's SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

- Review any additional settings, make any changes if needed, and click on **Save**.
- Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Wiz Issues

The Wiz Issues feed ingests Wiz security issues.

POST <https://{hostname}/graphql>

Sample Request:

```
{
  "query": "query IssuesTable($filterBy: IssueFilters, $first: Int, $after: String, $orderBy: IssueOrder) { issues:issuesV2(filterBy: $filterBy, first: $first, after: $after, orderBy: $orderBy) { nodes { id sourceRule{ __typename ... on Control { id name controlDescription: description resolutionRecommendation securitySubCategories { title category { name framework { name } } } risks } ... on CloudEventRule{ id name cloudEventRuleDescription: description sourceType type risks } ... on CloudConfigurationRule{ id name cloudConfigurationRuleDescription: description remediationInstructions serviceType risks } } createdAt updatedAt dueAt type resolvedAt statusChangedAt projects { id name slug businessUnit riskProfile { businessImpact } } status severity entitySnapshot { id type nativeType name status cloudPlatform cloudProviderURL providerId region resourceGroupExternalId subscriptionExternalId subscriptionName subscriptionTags tags createdAt externalId } serviceTickets { externalId name url } notes { createdAt updatedAt text user { name email } serviceAccount { name } } } pageInfo { hasNextPage endCursor } } }",
  "variables": {
    "first": 100,
    "filterBy": {
      "statusChangedAt": {
        "after": "2025-03-27T10:41:00Z",
        "before": "2025-03-28T10:41:00Z"
      },
      "type": ["CLOUD_CONFIGURATION", "TOXIC_COMBINATION", "THREAT_DETECTION"],
      "project": ["83b76efe-a7b6-5762-8a53-8e8f59e68bd8"]
    },
    "orderBy": {
      "field": "STATUS_CHANGED_AT",
      "direction": "DESC"
    }
  }
}
```

```
    },  
    "after": null  
  }  
}
```

Sample Response:

```
{
  "data": {
    "issues": {
      "nodes": [
        {
          "id": "00bcdd4f-d4ab-461d-b6de-173cc5b69ccc",
          "sourceRule": {
            "__typename": "Control",
            "id": "wc-id-2118",
            "name": "Application endpoint exposing technology
allowing unauthorized access",
            "controlDescription": "This application endpoint exposes
a technology that has a high severity unauthorized access host
configuration finding. This may allow an attacker to access the
technology served by this endpoint without needing to provide valid
credentials.\n\nPublicly exposed resources are more easily accessible
to attackers than internal ones. This may allow an attacker to
utilize unauthorized access to compromise your environment
remotely.",
            "resolutionRecommendation": "### Limit external
exposure\n* Identify the resource that is publicly exposed and
restrict access to it. When searching for the resource behind this
application endpoint, check your other environments or perform
enumeration techniques. For instance, use DNS and Whois queries to
better understand how this endpoint relates to your organizations'
compute or storage resources.\n* Ensure that exposed ports allow only
encrypted communications.\n\n### Enforce authentication and
authorization\n* Implement authentication and authorization
mechanism.\n* Use Multi-Factor Authentication (MFA) if possible.\n*
Monitor and audit user access for suspicious activity.\n* Use strong
password policies and discourage password reuse.\n\n### Ensure secure
configuration\n* Ensure the application is configured in accordance
with the best security practices.\n* Follow the remediation guidance
on the related host configuration finding.",
            "securitySubCategories": [
              {
                "title": "3.1.2 Limit system access to the types of
transactions and functions that authorized users are permitted to
execute.",
                "category": {
                  "name": "3.1 Access Control",
```

```

        "framework": {
          "name": "NIST 800-171 Rev.2"
        }
      },
    {
      "title": "T1021.007 Remote Services: Cloud Services",
      "category": {
        "name": "TA0008 Lateral Movement",
        "framework": {
          "name": "MITRE ATT&CK Matrix"
        }
      }
    }
  ],
  "risks": [],
},
"createdAt": "2025-03-28T08:33:47.144958Z",
"updatedAt": "2025-03-28T08:50:48.811341Z",
"dueAt": null,
"type": "TOXIC_COMBINATION",
"resolvedAt": null,
"statusChangedAt": "2025-03-28T08:50:48.78439Z",
"projects": [
  {
    "id": "83b76efe-a7b6-5762-8a53-8e8f59e68bd8",
    "name": "Project 2",
    "slug": "project-2",
    "businessUnit": "",
    "riskProfile": {
      "businessImpact": "MBI"
    }
  }
],
"status": "IN_PROGRESS",
"severity": "HIGH",
"entitySnapshot": {
  "id": "a4120d36-c274-5a54-9542-4448ea64a4ff",
  "type": "ENDPOINT",
  "nativeType": "",
  "name": "http://sample-aws-mongodb-backup-20230402093554120600000004.s3.us-east-1.amazonaws.com:80",

```

```

        "status": null,
        "cloudPlatform": "AWS",
        "cloudProviderURL": "",
        "providerId": "http://sample-aws-mongodb-
backup-20230402093554120600000004.s3.us-east-1.amazonaws.com:80/",
        "region": "",
        "resourceGroupExternalId": "",
        "subscriptionExternalId": "998231069301",
        "subscriptionName": "wiz-integrations",
        "subscriptionTags": {},
        "tags": {},
        "createdAt": null,
        "externalId": "http://sample-aws-mongodb-
backup-20230402093554120600000004.s3.us-east-1.amazonaws.com:80/"
    },
    "serviceTickets": [
        {
            "externalId": "slackThread/TSYNK6AJ3/
C08E7P8R4P4/1743150839.682219",
            "name": "Wiz (C08E7P8R4P4) - 1743150839.682219",
            "url": "https://wiz-sec.slack.com/archives/C08E7P8R4P4/
p1743150839682219"
        }
    ],
    "notes": [
        {
            "createdAt": "2025-03-28T08:50:48.784396Z",
            "updatedAt": "2025-03-28T08:50:48.785283Z",
            "text": "New incident created - RQ22603535",
            "user": null,
            "serviceAccount": {
                "name": "reliaquest"
            }
        }
    ]
},
"pageInfo": {
    "hasNextPage": false,
    "endCursor":
"eyJmaWVsZHMl0lt7IkZpZWxkIjoiU3RhdHVzQ2hhbmdlZEF0IiwiaWVmFsdWUiOiIyMDI1
LTAzLTl3VDIwOjA4OjUxLjcxOTQyOVoiSx7IkZpZWxkIjoiSWQiLCJWYX1ZSI6IjA2Z

```

```
WYzMDExLWUwOTEtNGZlZS04ZDBhLWFjMDg0OTI3YzRlOSJ9XX0="
    }
  }
}
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.type, .sourceRule.name, .severity, .id	Incident Value	Incident	.createdAt	Toxic Combination: Application endpoint exposing technology ...	Value formatted from values specified in the path column using ThreatQ value from the Wiz Values to ThreatQ Values mapping table below for type
.notes	Incident Description	N/A	N/A	N/A	Description formatted using context information like Metadata, Affected Projects, Entity Data, Notes
.sourceRule.securitySubCategories.title	Related Attack Pattern Value	Attack Pattern	.createdAt	T1021.007	Value with T*. format, linked to a ThreatQ MITRE Attack Pattern. The relationship is established based on the common ID (eg: T1071.005), while the rest of the value can differ.
.entitySnapshot.name	Related Vulnerability/Indicator Value	Vulnerability/ CVE	.createdAt	N/A	Values that start with CVE. User-Configurable
.id	Incident Attribute	Issue ID	.createdAt	00bcd4f-d4ab-461d-b6de-173cc5b69ccc	N/A
.type	Incident Attribute	Issue Type	.createdAt	TOXIC_COMBINATION	User-Configurable
.projects[.name]	Incident Attribute	Affected Project	.createdAt	Project 2	User-Configurable
.severity	Incident Attribute	Severity	.createdAt	HIGH	User-Configurable. Updatable
.status	Incident Attribute	Status	.createdAt	IN_PROGRESS	Updatable
.entitySnapshot.type	Incident Attribute	Entity Type	.createdAt	ENDPOINT	N/A
.entitySnapshot.cloudPlatform	Incident Attribute	Entity Cloud Platform	.createdAt	AWS	N/A
.entitySnapshot.region	Incident Attribute	Entity Region	.createdAt	N/A	N/A
.sourceRule.name	Incident Attribute	Control Rule	.createdAt	Application endpoint exposing technology allowing unauthorized access	N/A
.sourceRule.risks[]	Incident Attribute	Risk	.createdAt	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.dueAt</code>	Incident Attribute	Due At	<code>.createdAt</code>	N/A	Timestamp. Updatable
<code>.statusChangedAt</code>	Incident Attribute	Last Status Change	<code>.createdAt</code>	2025-03-28T08:50:48.78439Z	Timestamp. Updatable
<code>.sourceRule.securitySubCategories.category.name</code>	Incident Attribute	Tactic	<code>.createdAt</code>	Lateral Movement	Inserts values without the TA and the numeric sequence after it, if the value starts with TA and <code>.sourceRule.securitySubCategories.category.framework.name</code> is MITRE ATT&CK Matrix
<code>.sourceRule.securitySubCategories[].title</code>	Incident Attribute	Security Subcategory	<code>.createdAt</code>	IN_PROGRESS	User-Configurable

Wiz Value to ThreatQ Value Mapping

The following shows the mapping for Wiz values to ThreatQ values.

WIZ VALUE	THREATQ VALUE
TOXIC_COMBINATION	Toxic Combination
CLOUD_CONFIGURATION	Cloud Configuration
THREAT_DETECTION	Threat Detection

Wiz Threat Detections

The Wiz Threat Detections feed ingests Wiz detection findings.

POST `https://{hostname}/graphql`

Sample Request (truncated):

```
{
  "query": "query Detections(...) { detections(...) { nodes { id
startedAt endedAt severity type description ... } pageInfo
{ hasNextPage endCursor } } }",
  "variables": {
    "first": 100,
    "exactCount": true,
    "enforceTimestampContinuity": true,
    "filterBy": {
      "updatedAt": {
        "after": "2025-03-27T10:41:00Z",
        "before": "2025-03-28T10:41:00Z"
      },
      "severity": {
        "equals": ["CRITICAL", "HIGH"]
      },
      "projectId": ["83b76efe-..."]
    },
    "orderBy": {
      "field": "CREATED_AT",
      "direction": "DESC"
    },
    "after": null
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	NOTES
<code>.type, .id</code>	Incident Value	Incident	<code>.startedAt</code>	Value formatted as `Threat Detection: <type> : <id>
<code>.description</code>	Incident Description	N/A	N/A	Wiz detection description, including embedded resource references and detection context
<code>.id</code>	Incident Attribute	ID	<code>.startedAt</code>	Unique Wiz detection identifier
<code>.type</code>	Incident Attribute	Type	<code>.startedAt</code>	Wiz detection category

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	NOTES
.severity	Incident Attribute	Severity	.startedAt	Detection severity, user-configurable and updatable
.createdAt	Incident Attribute	Created At	.startedAt	Detection creation timestamp
.updatedAt	Incident Attribute	Updated At	.startedAt	Detection last update timestamp, user-configurable and updatable
.startedAt	Incident Attribute	Started At	.startedAt	Detection start timestamp
.endedAt	Incident Attribute	Ended At	.startedAt	Detection end timestamp, user-configurable and updatable
.ignored	Incident Attribute	Ignored	.startedAt	Whether the detection is ignored
.isRetroactive	Incident Attribute	Retroactive	.startedAt	Whether the detection was generated retroactively
.issue.id	Incident Attribute	Wiz Issue ID	.startedAt	Linked Wiz issue ID, when available
.issue.type	Incident Attribute	Wiz Issue Type	.startedAt	Expected to be THREAT_DETECTION
.issue.status	Incident Attribute	Status	.startedAt	Expected to be OPEN for active detections, user-configurable and updatable
.primaryActor.id	Incident Attribute	Primary Actor ID	.startedAt	Primary actor associated with the detection
.primaryActor.type	Incident Attribute	Primary Actor Type	.startedAt	Primary actor type, for example SERVICE_ACCOUNT
.primaryResource.id	Incident Attribute	Primary Resource ID	.startedAt	Primary resource associated with the detection
.primaryResource.type	Incident Attribute	Primary Resource Type	.startedAt	Primary resource type, for example CONTAINER_IMAGE
.projects[].name	Incident Attribute	Affected Project	.startedAt	Comma-separated project names from the detection response
.resources[].name	Incident Attribute	Related Resource	.startedAt	Comma-separated resource names from the detection response
.cloudAccounts[].name	Incident Attribute	Cloud Account	.startedAt	Comma-separated cloud account names from the detection response
.cloudOrganizations[].name	Incident Attribute	Cloud Organization	.startedAt	Comma-separated cloud organization names from the detection response

Average Feed Run



Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Wiz Issues

METRIC	RESULT
Run Time	1 minute
Incidents	22
Incident Attributes	100
Vulnerabilities	2

Wiz Threat Detections

METRIC	RESULT
Run Time	1 minute
Incidents	22
Incident Attributes	100

Change Log

- **Version 1.1.0**
 - Added a new feed, **Wiz Threat Detections**, to ingest Wiz threat detection findings through the GraphQL `detections` query.
- **Version 1.0.0**
 - Initial release