ThreatQuotient

Wiz CDF

Version 1.0.0

April 08, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer **3**
Support **4**
Integration Details **5**
Introduction **6**
Prerequisites **7**
Installation **8**
Configuration **9**
ThreatQ Mapping **12**
Wiz Issues 12
Wiz Value to ThreatQ Value Mapping 17
Average Feed Run **18**
Change Log **19**

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.

Support

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

Support Email: support@threatq.com
Support Web: https://support.threatq.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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The Wiz CDF integration retrieves security issues from Wiz that can be filtered by specific projects, severity, and type.

The integration provides the following feed:

- **Wiz Issues** - ingests Wiz security issues.

The feed supplied 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:

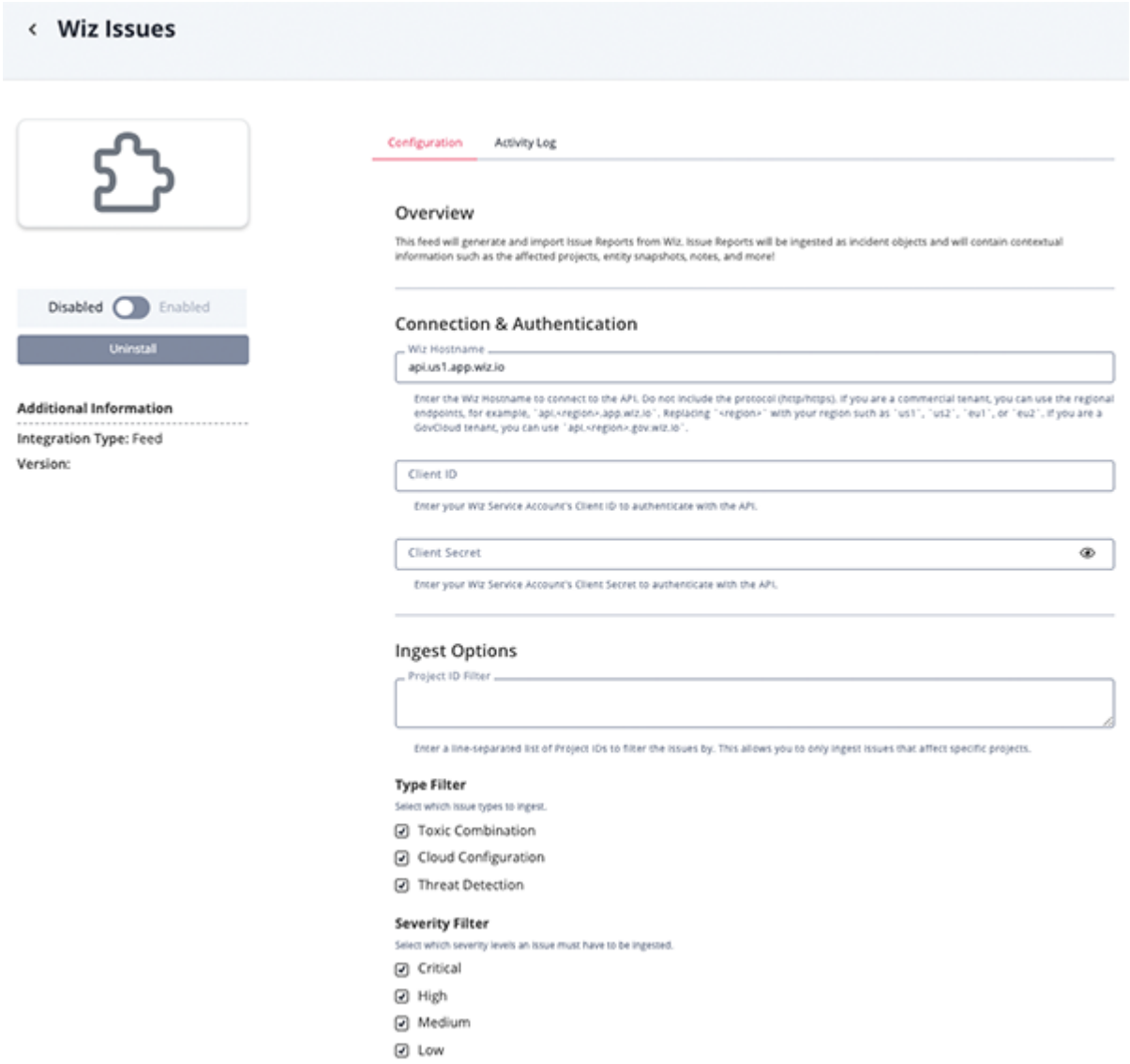
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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:

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: `api.<region>.app.wiz.io`. Replace the `<region>` tag with your region: `us1`, `us2`, `eu1`, or `eu2`. **GovCloud Tenants** - you can use `api.<region>.gov.wiz.io`.
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 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 *(default)*

PARAMETER	DESCRIPTION
	◦ Cloud Configuration *(default)* ◦ Threat Detection *(default)*
Severity Filter	Select which severity levels an issue must have to be ingested. Options include: ◦ Critical *(default)* ◦ High *(default)* ◦ Medium *(default)* ◦ Low *(default)* ◦ 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: ◦ Vulnerabilities *(default)* ◦ 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.



5. Review any additional settings, make any changes if needed, and click on **Save**.
6. 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":
"eyJmaWVsZHMiOlt7IkZpZWxkIjoiU3RhdHVzQ2hhbmdlZEF0IiwiVmFsdWUiOiIyMDI1LTAzLTI3VD
IwOjA4OjUxLjcxOTQyOVoifSx7IkZpZWxkIjoiSWQiLCJWYWx1ZSI6IjA2ZWYzMDExLWUwOTEtNGZlZ
S04ZDBhLWFjMDg0OTI3YzRlOSJ9XX0="
      }
    }
  }
}
```


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`	`00bcdd4f-d4ab-461d-b6de-173cc5b69ccc`	N/A

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

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.

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

Change Log

- **Version 1.0.0**
  - Initial release