ThreatQuotient

A Securonix Company

Intel 471 Vulnerability Enrichment Action

Version 1.0.0

May 18, 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

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: 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	1.0.0
Compatible with ThreatQ Versions	>= 5.29.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Intel 471 Vulnerability Enrichment action enables ThreatQ users to enhance Vulnerability objects with intelligence and contextual reporting from Intel 471. By querying the Intel 471 Vulnerability Report stream, the action retrieves relevant threat intelligence and enriches existing Vulnerability objects in ThreatQ with additional attributes and report context. This integration helps analysts gain deeper insight into vulnerabilities, supporting improved prioritization, investigation, and threat analysis workflows.

The integration provides the following action:

- **Intel 471 - Enrich Vulnerabilities** - queries the Intel 471 Vulnerability Report stream for the submitted vulnerability and enriches the corresponding ThreatQ object with available Intel 471 report context as attributes.

The integration is compatible with Vulnerability objects and provides enrichment data for supported vulnerabilities.

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing the vulnerability objects.
- An Intel471 API Client ID and Secret.

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

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

You will still need to configure the action.

Configuration

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

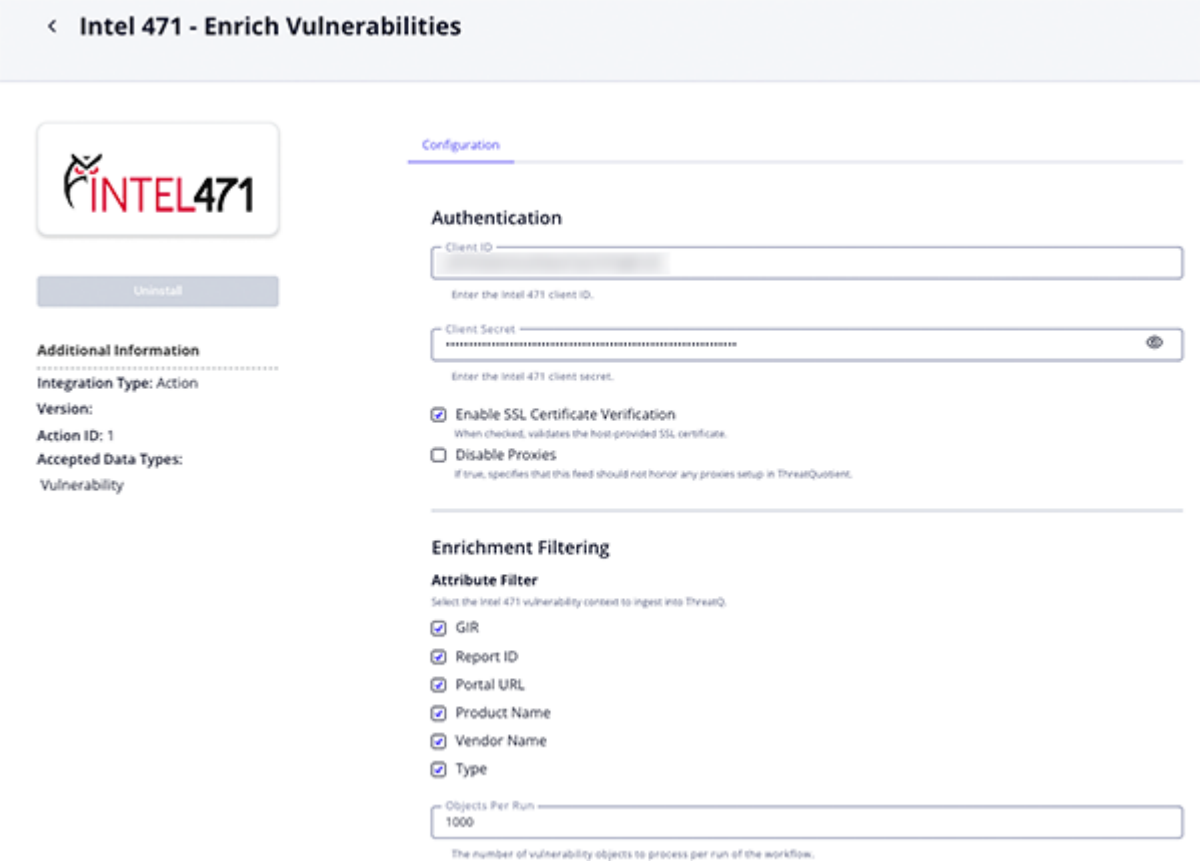
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

   The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Client ID	Enter your Intel 471 Client ID.
Client Secret	Enter your Intel 471 Client Secret.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Attribute Filter	Select the Intel 471 vulnerability context to ingest into ThreatQ. Options include: ◦ GIR *(default)* ◦ Report ID *(default)* ◦ Portal URL *(default)*

PARAMETER	DESCRIPTION
	◦ Product Name *(default)* ◦ Vendor Name *(default)* ◦ Type *(default)*
Objects Per Run	Enter the number of vulnerability objects to process per run of the workflow. The Default value is `1000`.



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Intel 471 - Enrich Vulnerabilities	Fetches Intel 471 vulnerability report context for a vulnerability.	Vulnerability	N/A

Intel 471 - Enrich Vulnerabilities

The Intel 471 - Enrich Vulnerabilities action queries the Intel 471 Vulnerability Report stream using the submitted vulnerability value as the text filter. Data is ingested only when the returned Intel 471 report `name` exactly matches the submitted vulnerability value, ensuring accurate and relevant enrichment results.

`GET https://api.intel471.cloud/integrations/intel-report/v1/reports/vulnerability/stream?text_filter={vulnerability}&size=1`

Sample Response:


```
{
  "count": 1,
  "reports": [
    {
      "id": "vulnerability--a59c6e28-93d1-5c35-be6e-c364abb5529c",
      "type": "vulnerability_report",
      "name": "CVE-2026-4670",
      "cve_type": "Authentication bypass",
      "vendor_name": "Progress Software",
      "product_name": "MOVEit Automation",
      "classification": {
        "girs": [
          {
            "path": "2.1",
            "name": "Vulnerabilities"
          },
          {
            "path": "2.1.4.7",
            "name": "Managed file transfer software vulnerabilities"
          },
          {
            "path": "2.1.13",
            "name": "Initial access vulnerabilities"
          }
        ]
      },
      "links": {
        "verity_portal": {
          "href": "https://verity.intel471.com/vulnerabilities/vulnerability--a59c6e28-93d1-5c35-be6e-c364abb5529c"
        }
```

```
        }
      }
    ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.classification.girs[].path, .classification.girs[].name	Vulnerability.Attribute	GIR	N/A	2.1.4.7 - Managed file transfer software vulnerabilities	User-configurable. Multiple GIR values can be added to a vulnerability.
.id	Vulnerability.Attribute	Report ID	N/A	vulnerability--a59c6e28-93d1-5c35-be6e-c364abb5529c	User-configurable. Updatable.
.links.verity_portal.href	Vulnerability.Attribute	Portal URL	N/A	https://verity.intel471.com/vulnerabilities/vulnerability--a59c6e28-93d1...	User-configurable. Updatable.
.product_name	Vulnerability.Attribute	Product Name	N/A	MOVEit Automation	User-configurable. Updatable.
.vendor_name	Vulnerability.Attribute	Vendor Name	N/A	Progress Software	User-configurable. Updatable.
.cve_type	Vulnerability.Attribute	Type	N/A	Authentication bypass	User-configurable. Updatable.

Enriched Data

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

METRIC	RESULT
Run Time	1 minute
Vulnerabilities	1
Vulnerability Attributes	8

Change Log

- **Version 1.0.0**
  - Initial release