ThreatQuotient

A Securonix Company

ThreatQ Signature Operation

Version 1.0.0

August 12, 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

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	>= 6.11.2
Support Tier	ThreatQ Supported

Introduction

The ThreatQ Signature Operation integration is designed to streamline the transformation and deployment of detection logic by converting Sigma rules (Custom Type signatures in ThreatQ) into KQL (Kusto Query Language) signatures. These KQL signatures can be seamlessly exported to Microsoft Azure Sentinel for immediate operational use. This simplifies detection rule management, enhances interoperability, and helps security teams accelerate threat response within their existing threat intelligence workflows.

The integration performs the following actions:

- **Convert –** transforms a Sigma rule into a KQL (Kusto Query Language) query and creates a new signature linked to the original object.
- **Export to Sentinel –** deploys the generated KQL rule to Microsoft Azure Sentinel and saves it in the specified workspace for use under the Log Queries tab.

The integration is compatible with ThreatQ Custom type signatures.

Prerequisites

The following required to run the **Export to Sentinel** action:

- An Azure Sentinel Workspace.
- Microsoft Azure Credentials including:
    - Azure Tenant ID
    - Azure Client ID
    - Azure Client Secret
    - Azure Subscription ID
    - Azure Resource Group
    - Azure Workspace Name

> ⚠ The user account needs to have the **Log Analytics Contributor** and **Log Analytics Reader** roles added.

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

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

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

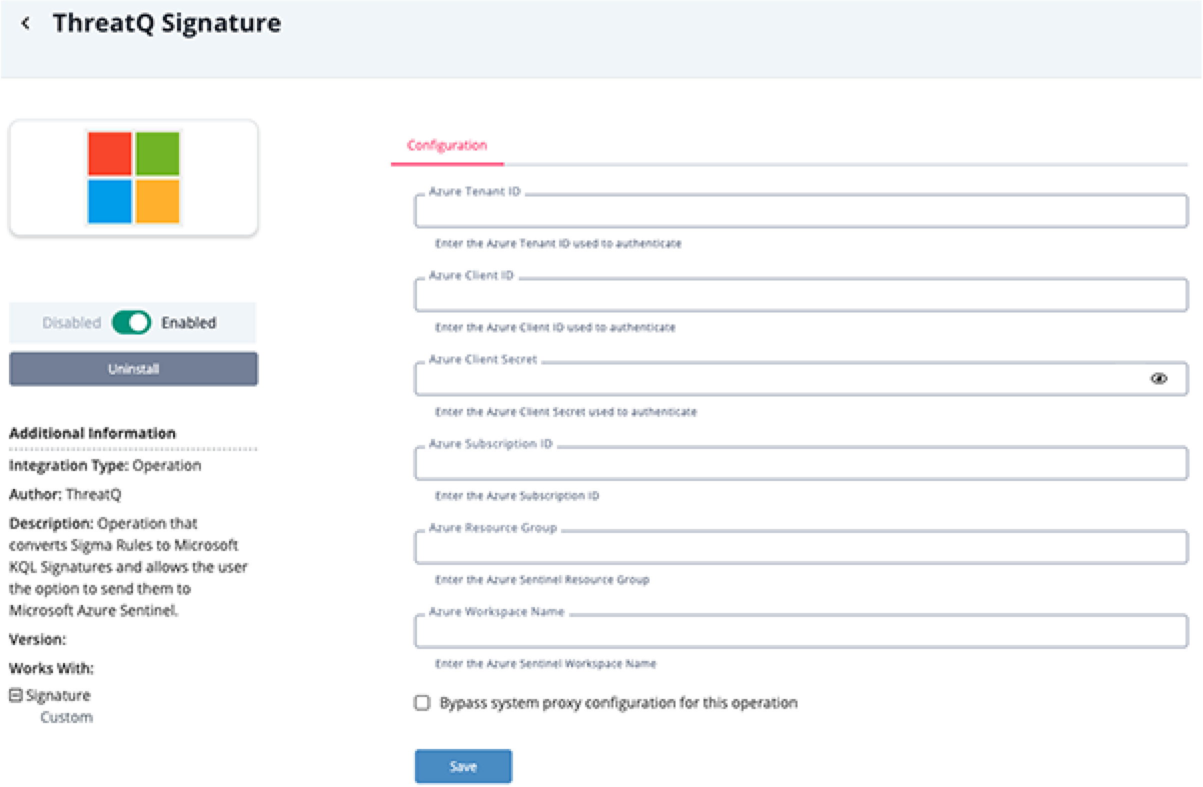
Configuration

> 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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Azure Tenant ID	The Directory (Tenant) ID for your Azure Active Directory.
Azure Client ID	The Application (Client) ID for the registered Azure app used to authenticate.
Azure Client Secret	The Client Secret associated with the Azure app. This is used for secure authentication.
Azure Subscription ID	The Subscription ID under which the Azure Sentinel resources are deployed.
Azure Resource Group	The name of the Resource Group containing the Azure Sentinel workspace.
Azure Workspace Name	The name of the Azure Sentinel (Log Analytics) workspace.



‹ ThreatQ Signature

Disabled Enabled

Uninstall

Additional Information

Integration Type: Operation

Author: ThreatQ

Description: Operation that converts Sigma Rules to Microsoft KQL Signatures and allows the user the option to send them to Microsoft Azure Sentinel.

Version:

Works With:

⊟ Signature
Custom

Configuration

Azure Tenant ID

Enter the Azure Tenant ID used to authenticate

Azure Client ID

Enter the Azure Client ID used to authenticate

Azure Client Secret

Enter the Azure Client Secret used to authenticate

Azure Subscription ID

Enter the Azure Subscription ID

Azure Resource Group

Enter the Azure Sentinel Resource Group

Azure Workspace Name

Enter the Azure Sentinel Workspace Name

☐ Bypass system proxy configuration for this operation

Save

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.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Convert	Transforms a Sigma rule into a KQL (Kusto Query Language) query and creates a new signature linked to the original object.	Signature	Custom
Export to Sentinel	Deploys the generated KQL rule to Microsoft Azure Sentinel and saves it in the specified workspace for use under the Log Queries tab.	Signature	Custom

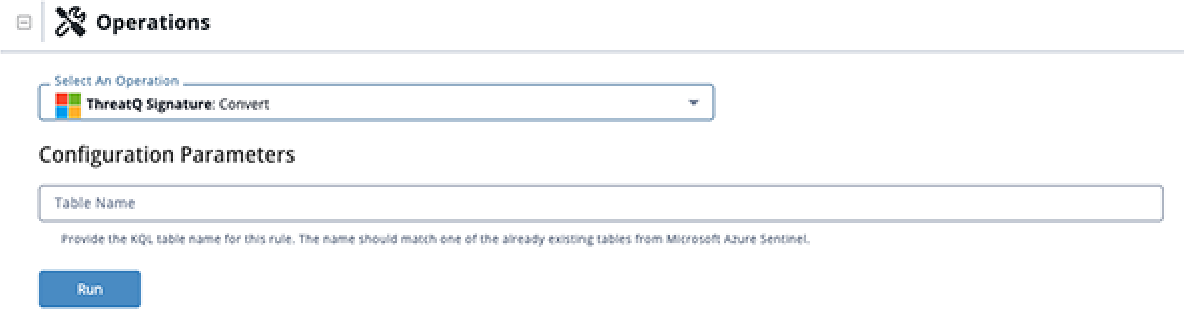
Convert

The Convert action transforms a Sigma rule into a KQL (Kusto Query Language) query and creates a new signature linked to the original object. This new object will be tagged with `kql`.

Configuration Run Parameter

The following configuration run parameter is available after selecting the Convert action.

PARAMETER	DESCRIPTION
Table Name	The KQL table name for this rule. An example of a table name is `RiskyUsers`.



ThreatQ Signature: Convert

Configuration Parameters

Table Name

Provide the KQL table name for this rule. The name should match one of the already existing tables from Microsoft Azure Sentinel.

Export to Sentinel

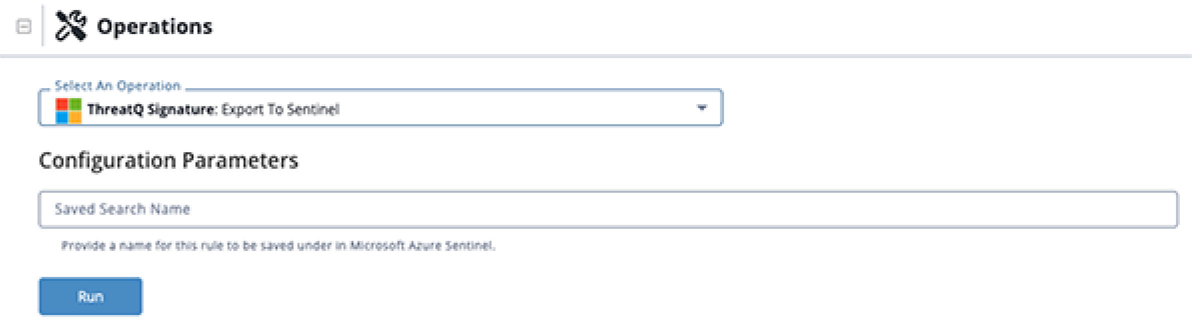
The Export to Sentinel action deploys the generated KQL rule to Microsoft Azure Sentinel and saves it in the specified workspace for use under the Log Queries tab.

> To run the query in Azure, navigate to the Sentinel Workspace > Logs > Queries Hub > Category: Other and then select the query you want to run.

Configuration Run Parameter

The following configuration run parameter is available after selecting the Export to Sentinel action.

PARAMETER	DESCRIPTION
Saved Search Name	The name under which the rule will be saved in Microsoft Azure Sentinel. You can also provide an existing name to update a previous saved search.



Select An Operation: **ThreatQ Signature:** Export To Sentinel

Configuration Parameters

Saved Search Name

Provide a name for this rule to be saved under in Microsoft Azure Sentinel.

Known Issues / Limitations

- Once a Sigma Rule has been converted to KQL and a new signature is created, that existing signature will not be updated by running the convert action.
- You can send a Sigma Rule to Microsoft Azure Sentinel as the ThreatQ platform does not currently support specific Signature types.

Change Log

- **Version 1.0.0**
    - Initial release