

ThreatQuotient



Secureworks Action

Version 1.0.1

March 18, 2024

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

- Support 3
- Warning and Disclaimer 4
- Integration Details..... 5
- Introduction 6
- Prerequisites 7
- Installation..... 8
- Configuration 9
- Actions 11
 - Secureworks - Upsert Indicators 11
- Known Issues / Limitations 12
- Change Log 13

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.

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 © 2024 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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.1
Compatible with ThreatQ Versions	>= 5.20.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Secureworks Action submits data collections containing IOCs to Secureworks' API.

The integration provides the following action:

- **Secureworks - Upsert Indicators** - submits a selected data collection (IOCs) to Secureworks.

The action is compatible with the following indicator types:

- IP Address
- IPv6 Address
- URL
- FQDN
- MD5
- SHA-1
- SHA-256

This action does not ingest any data back into the ThreatQ platform.



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.
- Secureworks credentials:
 - Client ID
 - Client Secret
 - Client Tenant
- A data collection containing at least one of the following indicator types:
 - IP Address
 - IPv6 Address
 - URL
 - FQDN
 - MD5
 - SHA-1
 - SHA-256

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
Secureworks API Hostname	Your Secureworks Hostname.
Client ID	Your Secureworks Client ID.
Client Secret	Your Secureworks Client Secret.
Client Tenant	Your Secureworks Client Tenant.
ThreatQ Hostname	Enter your ThreatQ hostname.
Objects Per Run	The number of objects to process per workflow run. The default value is set to 1,000.

< Secureworks - Upsert Indicators



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 5

Accepted Data Types:

Indicators

IP Address
IPv6 Address
FQDN
URL
SHA-1
SHA-256
MD5

Configuration

Secureworks API Hostname

Enter the hostname to use for the Secureworks API

Client ID

Enter your Secureworks Client ID to authentication with the API

Client Secret

Enter your Secureworks Client Secret to authentication with the API

Client Tenant

Enter your Secureworks Client Tenant to authentication with the API

ThreatQ Hostname

Objects Per Run

The max number of objects to send to this action, per run.

Save

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
Secureworks - Upsert Indicators	Submits a data collection containing IOCs to Secureworks.	Indicator	IP Address, IPv6 Address, URL, FQDN, MD5, SHA-1, SHA-256

Secureworks - Upsert Indicators

The Upsert Indicators action submits a data collection to the Secureworks' API.



You will need to check the Secureworks Audit Log to verify the uploaded indicators.

`https:// https://api.ctpx.secureworks.com/graphql`

Sample Response:

```
{
  "data": {
    "upsertIndicators": {
      "accepted_indicators": [
        {
          "id": "1c2e80f8-299e-5121-ba0b-dc4b42e08bd9",
          "object_type": "ip",
          "name": "ip name test1",
          "description": null,
          "value": "5.5.5.1",
          "updated_at": "2023-11-23T09:57:21.488495Z"
        }
      ],
      "rejected_indicators": null
    }
  }
}
```

Known Issues / Limitations

- You will need to check the Secureworks Audit Log to verify the uploaded indicators.

Change Log

- **Version 1.0.1**
 - Descriptions containing the source and a URL link have been added to exported IoCs.
 - Added new user configuration field: **ThreatQ Hostname**.
- **Version 1.0.0**
 - Initial release