ThreatQuotient

A Securonix Company

Splunk Export IOC Action

Version 1.0.0

July 07, 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	>= 6.5.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Splunk Export IOC Action enables ThreatQ users to export supported indicators directly to Splunk using the Splunk HTTP Event Collector (HEC). Each indicator is sent as an individual JSON event enriched with relevant ThreatQ context, including status, confidence, score, source information, tags, timestamps, and other metadata, allowing security teams to correlate threat intelligence with operational data in Splunk for investigation and detection workflows.

The integration provides the following action:

- **Splunk - Export Indicators** - exports supported ThreatQ indicators and associated threat intelligence context to Splunk as individual JSON events through the Splunk HEC.

The integration is compatible with the following indicator types:

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

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 at least one of the following indicator types:
  - CVE
  - Email Address
  - FQDN
  - IP Address
  - IPv6 Address
  - MD5
  - SHA-1
  - SHA-256
  - URL
- A Splunk instance with HTTP Event Collector enabled.
- A valid Splunk HEC token with permission to write to the configured index. See the documentation on the Splunk Docs website for more setup information: https://docs.splunk.com/Documentation/Splunk/8.2.9/Data/UsetheHTTPEventCollector

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
Splunk Hostname/ IP	Enter the hostname or IP address of the Splunk server.
HEC Port	Enter the port used by the Splunk HTTP Event Collector (HEC). The default value is 8088.
Use HTTPS	Select this option to connect to the Splunk HTTP Event Collector (HEC) using HTTPS. Enabled by default.
Splunk HEC Token	Enter the authentication token for the Splunk HTTP Event Collector (HEC).
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.

PARAMETER	DESCRIPTION
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Splunk Index	Specify the Splunk index where exported indicator events will be written. The default value is `threatq`.
Splunk Source	Specify the value assigned to the HEC `source` field for each exported event. The default value is `ThreatQ`.
Splunk Sourcetype	Specify the value assigned to the HEC `sourcetype` field for each exported event. The default value is `threatq:indicators`.
Splunk Event Host	Specify the value assigned to the HEC `host` field for each exported event. The default value is `ThreatQ`.
Export Tags	Select this option to include ThreatQ tags in the exported event payload. Enabled by default.
Export Attributes	Select this option to include ThreatQ indicator attributes in the exported event payload. Enabled by default.
Objects Per Run	Specify the maximum number of indicators to export during a single execution. The default value is `10000`.

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
Splunk - Export Indicators	Exports supported ThreatQ indicators to Splunk	Indicator	CVE, Email Address, FQDN, IP Address, IPv6 Address, MD5, SHA-1, SHA-256, URL

Splunk - Export Indicators

The Splunk – Export Indicator action exports supported indicators from a ThreatQ data collection to Splunk as individual JSON events through the Splunk HTTP Event Collector (HEC). Each event includes relevant ThreatQ context to support security monitoring, correlation, and analysis in Splunk.

This action is an outbound export action only. It does not ingest or synchronize data from Splunk into ThreatQ; its sole purpose is to export supported ThreatQ indicators and associated context to Splunk.

`POST https://<splunk-host>:8088/services/collector/event`

Sample Body:

```
{
  "host": "ThreatQ",
  "source": "ThreatQ",
  "sourcetype": "threatq:indicators",
  "index": "threatq",
  "event": {
    "ioc": "1.1.1.1",
    "ioc_type": "ip",
    "type": "IP Address",
    "status": "Active",
    "source": "ThreatQ",
    "sources": [
      "ThreatQ"
    ],
    "confidence": 90,
    "rating": 5,
    "score": 85,
    "tags": [
      "APT29",
      "Malware"
    ],
    "attributes": [
      {
        "name": "Country",
        "value": "US"
      }
    ],
    "created_at": "2026-06-29T10:00:00Z",
```

```
    "updated_at": "2026-06-29T12:00:00Z"
  }
}
```

Sample Response:

```
{
  "text": "Success",
  "code": 0
}
```

Use Case Example

1. A Threat Analyst curates a ThreatQ data collection containing high-confidence indicators that should be made available in Splunk for operational use.
2. The analyst adds the **Splunk – Export Indicators** action to a workflow.
3. The analyst configures the Splunk HTTP Event Collector (HEC) connection, target index, and optional export settings such as tags and attributes.
4. The workflow runs and exports each supported indicator as an individual JSON event to Splunk.
5. Security teams search, correlate, and investigate the enriched ThreatQ intelligence alongside operational security data in Splunk to support threat hunting, detection, and incident response.

Known Issues / Limitations

- Splunk-side field extraction, indexing, and retention behavior depend on the target Splunk environment.
- Splunk is a write-once, read-many log aggregator so update is not possible here.

Change Log

- **Version 1.0.0**
  - Initial release