

ThreatQuotient

A Securonix Company



Splunk Lookup Action

Version 1.0.3

September 21, 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	3
Support	4
Integration Details	5
Introduction	6
Prerequisites	7
Installation	8
Configuration	9
Actions	11
Splunk Lookup	12
Authentication	12
Username and Password	12
Splunk Bearer Token	12
Search Requests	12
Splunk 9 (Default)	12
Splunk 10	12
Get Sighting Information Supplemental Call	18
Enriched Data	20
Use Case Example	21
Change Log	22

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 © 2026 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.

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	1.0.3
Compatible with ThreatQ Versions	>= 5.6.0
Compatible with Splunk Versions	Enterprise and Cloud 9.3.x, 9.4.x, 10.0.x
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Splunk Lookup Action for ThreatQ allows an analyst to query Splunk for more information about a given IOC.

The integration provides the follow action:

- **Splunk Lookup** - performs a lookup within Splunk to locate logs related to the submitted indicator as well as optionally create events based on related sighting information.

The action is compatible with the following indicator types:

- CVE
- FQDN
- IP Address
- IPv6 Address
- MD5
- SHA-1
- SHA-256
- SHA-384
- SHA-512
- URL

The action returns the following enriched object types:

- Events
- Identities
- Indicators



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.
- An active Splunk instance on Splunk Enterprise or Cloud versions 9.3.x, 9.4.x, 10.0.x.
- A Splunk username and password.
- A Splunk authentication token with access to the required REST API and indexes
- A data collection containing at least one of the following indicator types:
 - CVE
 - FQDN
 - IP Address
 - IPv6 Address
 - MD5
 - SHA-1
 - SHA-256
 - SHA-384
 - SHA-512
 - URL

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 IP	The IP Address of the Splunk server.
Splunk Web Port	The port that the Splunk web app is running on. The default port is 8000.
Splunk API Port	The port that the Splunk API endpoints are running on. The default port is 8089.
Authentication Method	Select how to authenticate with Splunk. Options include: ◦ Username and Password (default) ◦ Splunk Bearer Token
Splunk Username	Your Splunk username you use to log into the Splunk web app.

PARAMETER	DESCRIPTION
	 This parameter is only accessible if you have selected Username and Password option for the Authentication Method parameter.
Splunk Password	The password associated with the username above.  This parameter is only accessible if you have selected Username and Password option for the Authentication Method parameter.
Splunk Bearer Token	Enter the Splunk authentication token used to access the REST API. Enter only the token value; do not include the Bearer prefix.  This parameter is only accessible if you have selected Splunk Bearer Token option for the Authentication Method parameter.
Days to Search	The historical timeframe to search. The default setting is 60 days from present.
Splunk Version 10	Enable this parameter to use the Splunk 10 v2 Search API. Leave it disabled when using Splunk 9.
Verify Host SSL	If enabled, the action will validate the server's certificate and confirm that the server's hostname match.
Ingest Event	Enable this option to create an event that contains the related sighting information.
Objects Per Run	The max number of objects to submit per run.

- 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 Lookup	Performs a lookup within Splunk to locate logs related to the submitted indicators.	Indicator	IP Address, FQDN, URL, CVE, IPv6 Address, MD5, SHA-1, SHA-256, SHA-384, SHA-512

Splunk Lookup

The Splunk Lookup action searches Splunk for logs associated with the submitted indicator.

Authentication

Username and Password

When **Username and Password** authentication is selected, the action obtains a session key using the following request:

```
POST https://{{splunk_ip}}:{{splunk_api_port}}/services/auth/login
```

Subsequent requests include the session key in the authorization header:

```
Authorization: Splunk <session_key>
```

Splunk Bearer Token

When **Splunk Bearer Token** authentication is selected, the login request is skipped. Subsequent requests include the configured token in the authorization header:

```
Authorization: Bearer <token>
```

Splunk token authentication must be enabled. The token must be issued to an existing Splunk user with roles that provide access to the required searches and indexes.

Search Requests

Splunk 9 (Default)

The action submits the following GET request:

```
GET https://{{splunk_ip}}:{{splunk_api_port}}/services/search/jobs/export?search=search "{{object.value}}" sourcetype!
="threatq:indicators" earliest=-{{days_to_search}}d latest=now |
table host, source, sourcetype, _raw, _time&output_mode=xml
```

Splunk 10

The action submits a POST request to the following endpoint:

```
POST https://{{splunk_ip}}:{{splunk_api_port}}/services/search/v2/jobs/export
```

The request sends the `search` value and `output_mode=xml` as form data.

Sample Response:

```
<?xml version='1.0' encoding='UTF-8'?>
<results preview='0'>
  <meta>
    <fieldOrder>
      <field>_bkt</field>
      <field>_cd</field>
      <field>_indextime</field>
      <field>_raw</field>
      <field>_serial</field>
      <field>_si</field>
      <field>_sourcetype</field>
      <field>_time</field>
      <field>host</field>
      <field>index</field>
      <field>linecount</field>
      <field>source</field>
      <field>sourcetype</field>
      <field>splunk_server</field>
    </fieldOrder>
  </meta>
  <messages>
    <msg type="INFO">Your timerange was substituted based on your
search string</msg>
  </messages>
  <result offset='0'>
    <field k='_bkt'>
      <value>
        <text>main~1~71D38691-066C-4C7C-B5BB-C082AAB8C4D9</
text>
      </value>
    </field>
    <field k='_cd'>
      <value>
        <text>1:12577</text>
      </value>
    </field>
    <field k='_indextime'>
      <value>
        <text>1715845581</text>
      </value>
```

```

    </field>
    <field k='_raw'>
      <v xml:space='preserve' trunc='0'>117.21.246.164 - - [16/May/2024:09:45:05] "GET /category.screen?categoryId=ACCESSORIES&JSESSIONID=SD9SL6FF8ADFF5015 HTTP/1.1" 200 689 "http://www.buttercupgames.com/oldlink?itemId=EST-7" "Googlebot/2.1 (http://www.googlebot.com/bot.html)" 673
    </v>
  </field>
  <field k='_serial'>
    <value>
      <text>0</text>
    </value>
  </field>
  <field k='_si'>
    <value>
      <text>localhost.localdomain</text>
    </value>
    <value>
      <text>main</text>
    </value>
  </field>
  <field k='_sourcetype'>
    <value>
      <text>TQDemo</text>
    </value>
  </field>
  <field k='_time'>
    <value>
      <text>2024-05-16 09:45:05.000 CEST</text>
    </value>
  </field>
  <field k='host'>
    <value>
      <text>127.0.0.1</text>
    </value>
  </field>
  <field k='index'>
    <value>
      <text>main</text>
    </value>
  </field>

```

```

    </field>
    <field k='linecount'>
      <value>
        <text>2</text>
      </value>
    </field>
    <field k='source'>
      <value>
        <text>TQDemo_data</text>
      </value>
    </field>
    <field k='sourcetype'>
      <value>
        <text>TQDemo</text>
      </value>
    </field>
    <field k='splunk_server'>
      <value>
        <text>localhost.localdomain</text>
      </value>
    </field>
  </result>
  <result offset='1'>
    <field k='_bkt'>
      <value>
        <text>main~1~71D38691-066C-4C7C-B5BB-C082AAB8C4D9</
text>
      </value>
    </field>
    <field k='_cd'>
      <value>
        <text>1:12566</text>
      </value>
    </field>
    <field k='_indextime'>
      <value>
        <text>1715845581</text>
      </value>
    </field>
    <field k='_raw'>
      <v xml:space='preserve' trunc='0'>209.160.24.63 - - [16/
May/2024:09:43:27] &quot;GET /oldlink?

```

```
itemId=EST-6&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 1748
"http://www.buttercupgames.com/oldlink?itemId=EST-6"
"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML,
like Gecko) Chrome/19.0.1084.46 Safari/536.5" 731
</v>
```

```

    </field>
    <field k='_serial'>
      <value>
        <text>1</text>
      </value>
    </field>
    <field k='_si'>
      <value>
        <text>localhost.localdomain</text>
      </value>
      <value>
        <text>main</text>
      </value>
    </field>
    <field k='_sourcetype'>
      <value>
        <text>TQDemo</text>
      </value>
    </field>
    <field k='_time'>
      <value>
        <text>2024-05-16 09:43:27.000 CEST</text>
      </value>
    </field>
    <field k='host'>
      <value>
        <text>127.0.0.1</text>
      </value>
    </field>
    <field k='index'>
      <value>
        <text>main</text>
      </value>
    </field>
    <field k='linecount'>
      <value>
        <text>2</text>
      </value>

```

```

    </field>
    <field k='source'>
      <value>
        <text>TQDemo_data</text>
      </value>
    </field>
    <field k='sourcetype'>
      <value>
        <text>TQDemo</text>
      </value>
    </field>
    <field k='splunk_server'>
      <value>
        <text>localhost.localdomain</text>
      </value>
    </field>
  </result>
</results>

```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
results.result[].field[].value.text	Related Attribute.Value	Host	results.result[].field[].value.text	127.0.0.1	N/A
results.result[].field[].value.text	Related Attribute.Value	Source	results.result[].field[].value.text	TQDemo_data	N/A
results.result[].field[].value.text	Related Attribute.Value	Source Type	results.result[].field[].value.text	TQDemo	N/A
results.result[].field[].value.text	Related Attribute.Value	Raw	results.result[].field[].value.text	209.160.24.63 - [16/May/2024:09:43:27] "GET /oldlin...	N/A

Get Sighting Information Supplemental Call

Splunk 9 (default)

```
GET https://{{splunk_ip}}:{{splunk_api_port}}/services/search/jobs/
export?search=search "{{object.value}}" sourcetype!
="threatq:indicators" earliest=-{{days_to_search}}d latest=now |
table host, source, sourcetype, _time | stats count as Total ,
earliest(_time) as start, latest(_time) as stop | table start, stop,
Total&output_mode=json
```

Splunk 10

```
POST https://{{splunk_ip}}:{{splunk_api_port}}/services/search/v2/
jobs/export
```

The Splunk 10 request sends `search` and `output_mode=json` as form data.

Sample Response:

```
{
  "preview": false,
  "offset": 0,
  "lastrow": true,
  "result": {
    "start": "1720337199",
    "stop": "1720421433",
    "Total": "36"
  }
}
```

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
results.start	Event.Attribute	First Sighting	N/A	2024-07-07 07:26:39+00:00	We use a timestamp filter to convert the epoch time to date
results.stop	Event.Attribute	Last Sighting	N/A	2024-07-08 06:50:33+00:00	We use a timestamp filter to convert the epoch time to date
results.Total	Event.Attribute	Count of total sightings	N/A	36	N/A
N/A	Event.Attribute	Splunk Query Link	N/A	https://{{splunk_ip}}:{{splunk_web_port}}/en-GB/app/search/search?q=search{{object.value}} sourcetype!=threatq:indicators earliest=-	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
				<pre> {{days_to_search}}d latest=now \ table host, source, sourcetype, _time \ stats count as Total , earliest(_time) as start, latest(_time) as stop \ table start, stop, Total&output_mode=json </pre>	

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
Events	6
Event Attributes	6
Identities	6
Indicators	18

Use Case Example

1. A Threat Analyst identifies a collection of supported objects they would like to enrich.
2. The Threat Analyst adds the Splunk Lookup to a Workflow.
3. The Threat Analyst configures the action with the desired parameters, and enables the Workflow.
4. The Workflow executes all Actions in the graph, including Splunk Lookup.
5. The Workflow enriches the objects with Splunk data.

Change Log

- **Version 1.0.3**

- Added support for Splunk 10.0.x using the v2 search export endpoint and POST requests.
- Added support for Splunk bearer token authentication.
- Added the following new configuration parameters:
 - **Authentication Method** - determine how the integration authenticates with Splunk.
 - **Splunk Bearer Token** - provide the token required for authentication when **Splunk Bearer Token** is selected as the authentication method.
 - **Splunk Version 10** - determine which Splunk search export API the integration uses. Enable it for the Splunk 10 v2 API, or leave it disabled to use the Splunk 9 API.

- **Version 1.0.2**

- The action now supports and returns enriched Identity object types.

- **Version 1.0.1**

- Added a new configuration option, **Ingest Event**, which allows users to create events from related sighting information.

- **Version 1.0.0**

- Initial release