ThreatQuotient

Splunk Operation

Version 1.2.1

July 16, 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

Warning and Disclaimer **3**
Support **4**
Integration Details **5**
Introduction **6**
Installation **7**
Configuration **8**
Actions **11**
Splunk Search 11
Action Run Parameters 14
Ingest Event Option 15
Change Log **16**

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	1.2.1
Compatible with ThreatQ Versions	>= 5.16.0
Support Tier	ThreatQ Supported

Introduction

The Splunk Operation performs lookups within Splunk to locate logs related to a selected indicator.

The operation provides the following action:

- **Splunk Search** - submits a custom query for IOCs to Splunk and retrieves the matching results.

The operation is compatible with the follow Indicator types:

- CVE
- Email Address
- 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 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
Splunk IP	The IP of the server that is running Splunk.
Splunk Web Port	The port that the Splunk web app is running on. The default setting is port 8000.
Splunk API Port	The port that the Splunk API endpoints are running on. The default setting is port 8089.
Splunk Username	The username that you use to log into the Splunk web application.
Splunk Password	The password associated with the username above.
Days to Search	The historical timeframe to search through.
Language Code	The language code that is being used in Splunk. The default setting is en-US.
Search Query for CVE IOC	Insert the search query for CVEs in the parameter field provided. Use %s to denote the IOC's value - see the Search Query Parameters note below this table for further details.

PARAMETER	DESCRIPTION
Search Query for Email Address IOC	Insert the search query for Email Addresses in the parameter field provided. Use `%s` to denote the IOC's value - see the Search Query Parameters note below this table for further details.
Search Query for FQDN IOC	Insert the search query for FQDNs in the parameter field provided. Use `%s` to denote the IOC's value - see the Search Query Parameters note below this table for further details.
Search Query for IP Address IOC	Insert the search query for IP Addresses in the parameter field provided. Use `%s` to denote the IOC's value - see the Search Query Parameters note below this table for further details.
Search Query for IPv6 Address IOC	Insert the search query for IPv6 Addresses in the parameter field provided. Use `%s` to denote the IOC's value - see the Search Query Parameters note below this table for further details.
Search Query for MD5 IOC	Insert the search query for MD5s in the parameter field provided. Use `%s` to denote the IOC's value - see the Search Query Parameters note below this table for further details.
Search Query for SHA-1 IOC	Insert the search query for SHA-1s in the parameter field provided. Use `%s` to denote the IOC's value - see the Search Query Parameters note below this table for further details.
Search Query for SHA-256 IOC	Insert the search query for SHA-245s in the parameter field provided. Use `%s` to denote the IOC's value - see the Search Query Parameters note below this table for further details.
Search Query for SHA-384 IOC	Insert the search query for SHA-384s in the parameter field provided. Use `%s` to denote the IOC's value - see the Search Query Parameters note below this table for further details.
Search Query for SHA-512 IOC	Insert the search query for SHA-512s in the parameter field provided. Use `%s` to denote the IOC's value - see the Search Query Parameters note below this table for further details.

PARAMETER	DESCRIPTION
Search Query for URL IOC	Insert the search query for URLs in the parameter field provided. Use %s to denote the IOC's value - see the Search Query Parameters note below this table for further details.

Search Query parameters - specify the table columns/headers you want returned and the operation will create the markup for them.

Example: `search %s sourcetype!="threatq:indicators" | table host, source, sourcetype, _raw, _time`

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 action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Splunk Search	Submits a custom query for IOCs to Splunk and retrieves the results.	Indicator	CVE, Email Address, IP Address, IPv6 Address, MD5, SHA-1, SHA-256, SHA-384, SHA-512, URL

Splunk Search

The Splunk Search action submits a custom query to Splunk for IOCs and retrieves the results.

```
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
```

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] &quot;GET /
category.screen?categoryId=ACCESSORIES&amp;JSESSIONID=SD9SL6FF8ADFF5015 HTTP 1.1&quot; 200 689
&quot;http://www.buttercupgames.com/oldlink?itemId=EST-7&quot; &quot;Googlebot/2.1 (http://
www.googlebot.com/bot.html)&quot; 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 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] &amp;quot;GET /
oldlink?itemId=EST-6&amp;amp;JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1&amp;quot; 200 1748 &amp;quot;http://
www.buttercupgames.com/oldlink?itemId=EST-6&amp;quot; &amp;quot;Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5&amp;quot; 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>
```

Action Run Parameters

The Splunk Search action provides the following run parameter:

ACTION PARAMETER	DESCRIPTION
Days to Override	Optional - This parameter overrides the default value set in the **Days to Search** configuration parameter. You can leave this field blank to use the **Days to Search** setting.
Ingest Event	Enable this option to create an event that contains the related sighting information. See the Ingest Event Option section of this guide for more information.

Ingest Event Option

Enabling the Ingest Event option will result in the creation of an event related to the object.

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

Sample Response:

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

ThreatQuotient provides the following default mapping:

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=-{{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`	N/A

Change Log

- **Version 1.2.1**
  - Added a new action run configuration option, **Ingest Event**, which allows users to create events from related sighting information.
- **Version 1.2.0**
  - Resolved a `"con_error": "name 'client' is not defined"` error by updating the Splunk SDK version utilized by the operation.
  - The operation's Search action now allows the use of custom Splunk queries.
  - Added a new run configuration parameter, **Days to Search (Override)**, that allows you to override the default **Days to Search** configuration parameter.
  - Raw Event has been added to the default search query.
  - Expanded the operation's support for additional indicator types. The following indicator types are now supported by the operation:
    - CVE
    - Email Address
    - FQDN
    - IP Address
    - IPv6 Address
    - MD5
    - SHA-1
    - SHA-256
    - SHA-384
    - SHA-512
    - URL
  - Added the following new configuration parameters:
    - Search Query for CVE IOC
    - Search Query for Email Address IOC
    - Search Query for FQDN IOC
    - Search Query for IP Address IOC
    - Search Query for IPv6 Address IOC
    - Search Query for MD5 IOC
    - Search Query for SHA-1 IOC
    - Search Query for SHA-256 IOC
    - Search Query for SHA-384 IOC
    - Search Query for SHA-512 IOC
    - Search Query for URL IOC
  - Updated the minimum ThreatQ version to 5.16.0
- **Version 1.1.0**
  - Initial release