

ThreatQ Splunk Implementation Guide

Version 1.0.0

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 © 2019 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.

Last Updated: Tuesday, March 5, 2019

Contents

ThreatQ Splunk Implementation Guide	1
Warning and Disclaimer	2
Contents	4
Versioning	7
App Version	7
Supported Splunk Version	7
Supported ThreatQuotient Version	7
Features	7
Distributed Deployment	7
Support for Splunk's Common Information Model (CIM) and Enterprise Security (ES) ..	8
Export Indicators from ThreatQ using Score and Status Filters	8
Detect Sightings and Return to ThreatQ	8
Contextualize ThreatQ Data	8
Workflow Actions in Splunk to Interact with ThreatQ Data	9
Dashboard for Visualization	9
Installation	10
Deployment	10
Configuration	12

ThreatQuotient Add-on	12
Authentication with ThreatQ	13
Authentication with the Use of Self Signed Certificates in ThreatQ	13
Data Extraction from ThreatQuotient	14
Data Loading in Splunk	16
ThreatQuotient App	16
Sightings and Feedback to ThreatQ	16
Separation of Data	17
Macros	17
Saved Searches	19
Saved Searches Documentation	21
Reporting Sightings in ThreatQ	25
Putting Everything Together	26
Workflow Actions	28
ThreatQ: Add Indicator	28
ThreatQ: Add to Whitelist	29
ThreatQ: Lookup Indicator	29
ThreatQ: Mark as False Positive	29
ThreatQ: Mark as True Positive	29
Enterprise Security Support	29

ThreatQ Indicators to Splunk Lookup Mapping Table (using CIM)	29
Saved Searches for CIM Mapping	31
Dashboards	33
Cumulative Counts	33
Score Breakdown	34
Type Breakdown	34
Adversaries Breakdown	35
Static Table View	36
Top 10 By Sightings	36
Troubleshooting	38

Versioning

App Version

- TA-threatquotient-add-on: 1.0.0
- ThreatQAppforSplunk: 1.0.0

Supported Splunk Version

These apps have been tested with Splunk versions 7.0.x, 7.1.x and 7.2.x.

Supported ThreatQuotient Version

These apps require ThreatQ version 4.16.0 or higher. They will NOT work with a ThreatQ version prior to 4.16.0.

Features

The ThreatQuotient App for Splunk provides the following capabilities:

Distributed Deployment

The solution is packaged as two separate Splunk packages:

- **ThreatQuotient Add-on for Splunk:** Deployed on Splunk heavy forwarder and search head.
- **ThreatQuotient App for Splunk:** Deployed on Splunk search head.

Support for Splunk's Common Information Model (CIM) and Enterprise Security (ES)

ES Support: Indicator Data exported from ThreatQuotient is mapped using Splunk CIM in the Splunk ES.

Export Indicators from ThreatQ using Score and Status Filters

- **Score Filter:** You can choose to export indicators with scores greater than or equal to the value configured in the score filter.
- **Status Filter:** You can choose to export indicators with statuses matching the ones configured in the status filter.

Detect Sightings and Return to ThreatQ

- **Detect Sightings:** Indicators from ThreatQ are matched against raw events in Splunk looking for evidence of sightings.
- **Report Sightings:** Sightings are reported back to ThreatQ as events that contain the most up to date information.

Contextualize ThreatQ Data

All data exported from ThreatQ is highly contextualized for Splunk. Context provided for exported indicators includes:

- Indicator sources
- Indicator adversaries
- Indicator attributes
- Indicator status, score and type

Workflow Actions in Splunk to Interact with ThreatQ Data

This App provides the following workflow actions to an analyst to interact with ThreatQ:

- Add Indicator to ThreatQ
 - The user provides indicator type, status and source
- Whitelist an indicator in ThreatQ
- Look up an indicator in ThreatQ
 - Additional context is fetched if this indicator exists in ThreatQ
- Mark an indicator **False Positive** in ThreatQ
- Mark an indicator **True Positive** in ThreatQ

Dashboard for Visualization

The dashboard provides a rich set of real time updated widgets and tables to summarize information, including (but not limited to):

- Total exported indicators and sightings filtered by time range, type and score
- Top 10 indicators with sightings
- Top 10 sources and adversaries (due to the context available from ThreatQ) with sightings
- Static tables summarizing indicators and sightings filtered by time range, type and score

Installation

From the main Splunk interface:

1. Click on the **Down** arrow on the Apps menu located in the main navigation bar.
2. Select the **Find More Apps** option.

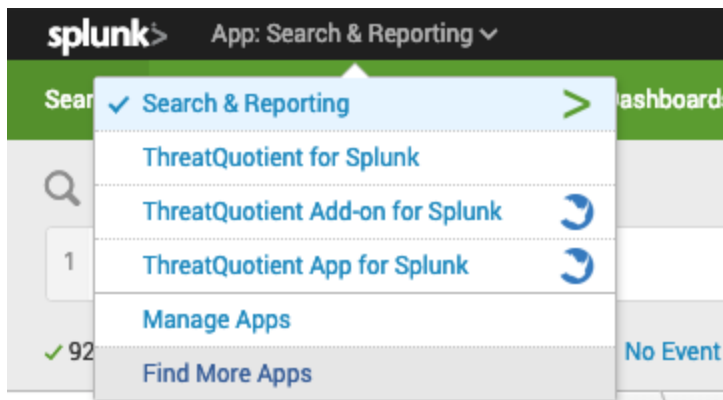


Figure 1: Installation from the Splunk App

3. Search for “ThreatQuotient” and follow the onscreen prompts to install the ThreatQuotient App and ThreatQuotient Add-on.

Deployment

Two Splunk packages need to be deployed for the App to work.

- **TA-threatquotient-add-on:** This package needs to be deployed both on the Splunk **heavy forwarder** and Splunk **search head**.
 - On the heavy forwarder, the add-on App extracts indicators from the ThreatQ appliance and forwards them to the configured splunk index.

- On the search head, the App provides support for ThreatQuotient workflow actions in Splunk.
- **ThreatQAppforSplunk:** This package needs to be deployed only on the Splunk search head.

The picture below demonstrates how the two packages are deployed in a distributed Splunk Environment.

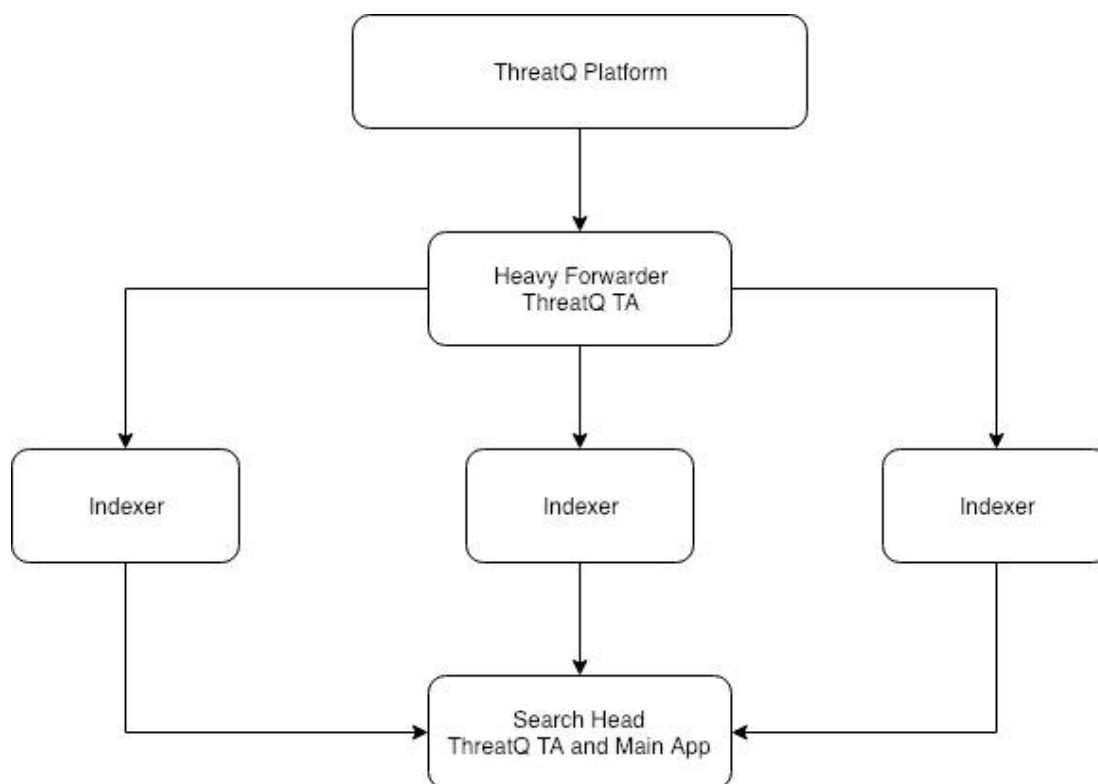


Figure 2: Deployment of Splunk App in Distributed Environment

The table below summarizes the deployment in the distributed Splunk environment:

	Heavy Forwarder	Indexer	Search Head
ThreatQuotient Add-on	Yes	No	Yes

	Heavy Forwarder	Indexer	Search Head
	• Requires configuration with ThreatQuotient credentials • Requires creating the data collection job		• Requires configuration with ThreatQuotient credentials • Must not be configured with data collection job
ThreatQuotient App	No	No	Yes • No configuration is required

Table 1: Deployment Matrix for Distributed Environment

**Advanced Configuration**

If you desire to configure multiple heavy forwarders for a single ThreatQuotient App - this is not typical since the indicators exported from ThreatQ do not exceed a few thousand at most - you would have to make multiple copies of the default ThreatQ Splunk Export, and use a different Export ID on each heavy forwarder. This way, the ThreatQ server can keep track of incremental indicator changes as seen by each distinct Export.

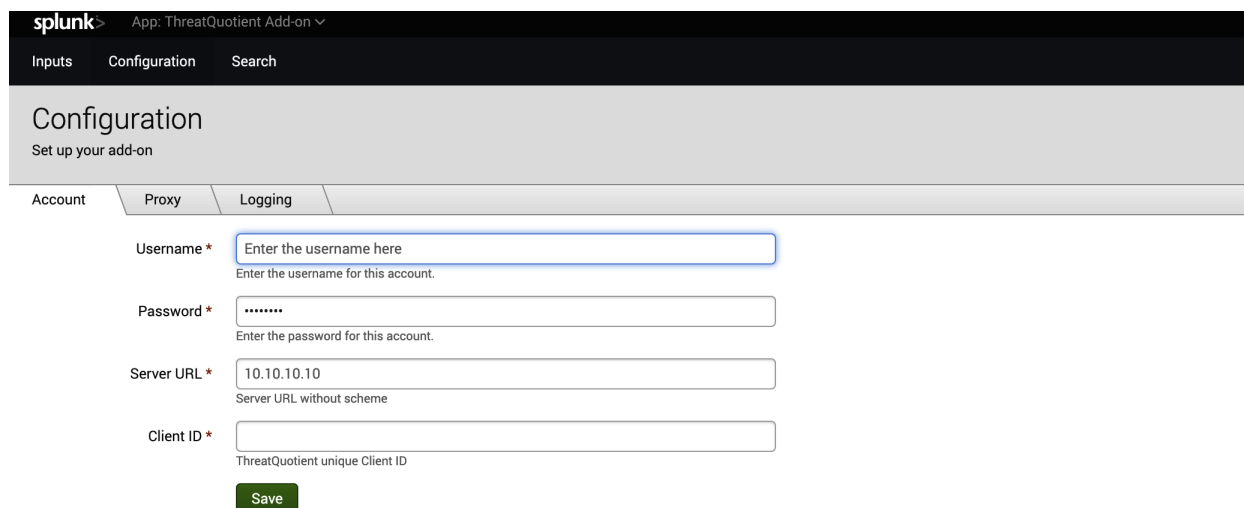
Configuration

ThreatQuotient Add-on

The ThreatQuotient add-on is responsible for the following:

Authentication with ThreatQ

On the **Configuration** tab, fields are presented to configure the ThreatQ account authentication as shown below.



The screenshot shows the Splunk interface for configuring the ThreatQuotient Add-on. The top navigation bar includes 'splunk', 'App: ThreatQuotient Add-on', and tabs for 'Inputs', 'Configuration', and 'Search'. The 'Configuration' tab is active, showing the title 'Configuration' and the subtitle 'Set up your add-on'. Below this are three sub-tabs: 'Account', 'Proxy', and 'Logging'. The 'Account' sub-tab is selected, displaying four configuration fields: 'Username *' with a placeholder 'Enter the username here' and description 'Enter the username for this account.', 'Password *' with a masked password '*****' and description 'Enter the password for this account.', 'Server URL *' with the value '10.10.10.10' and description 'Server URL without scheme', and 'Client ID *' with an empty field and description 'ThreatQuotient unique Client ID'. A green 'Save' button is located at the bottom of the form.

Figure 3: Configuration of Authentication Parameters

Upon clicking the **Save** button, you can see the status of the Authentication action. If the ThreatQuotient appliance is down, and/or the authentication parameters are invalid, an error message will be displayed. Unless the appliance is up and the authentication parameters are valid, this App will not work.

Authentication with the Use of Self Signed Certificates in ThreatQ

It is typical for many ThreatQuotient users to use self signed certificates. If you are doing this, you must perform the following additional configuration steps in the Splunk Add-On App.

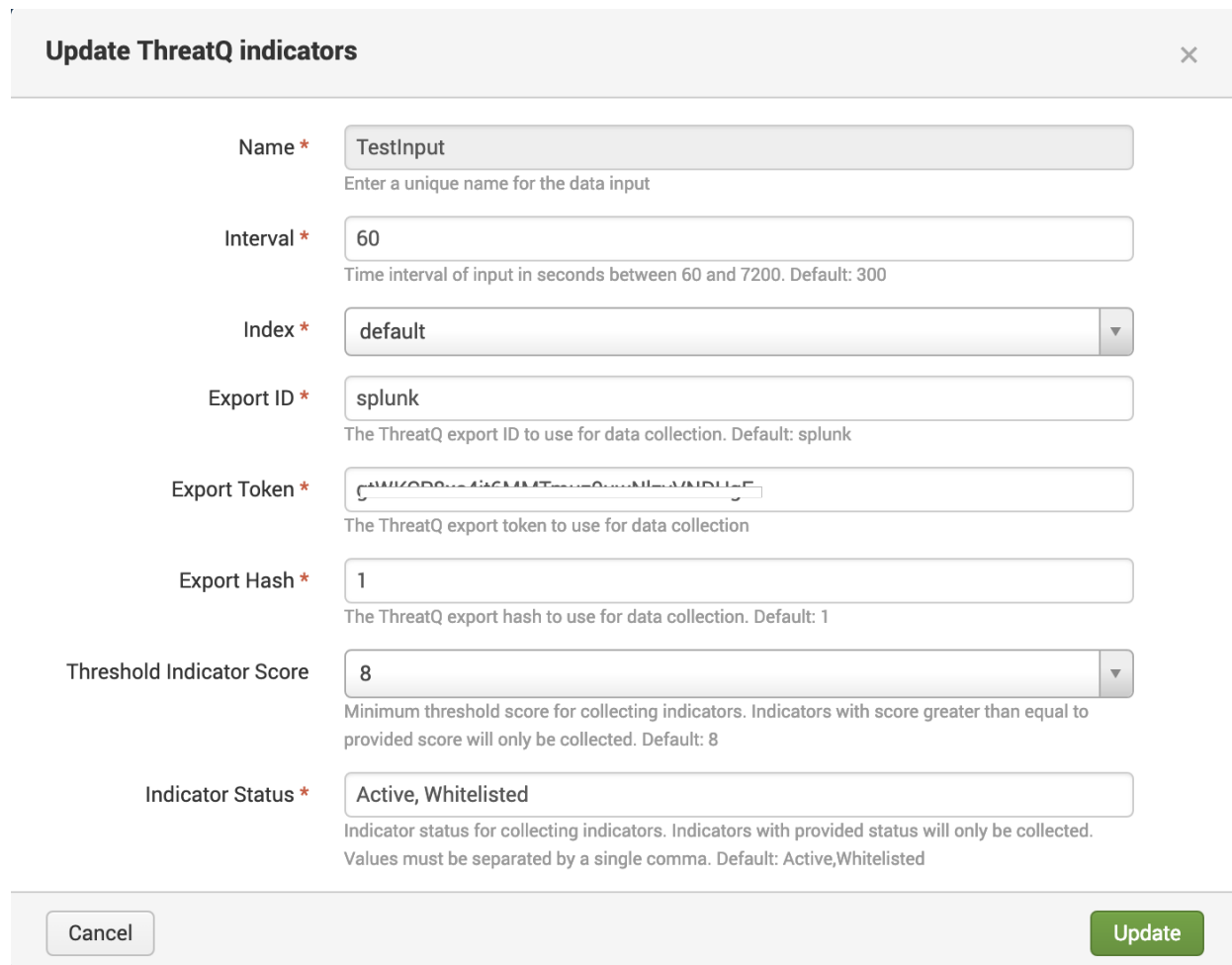
In `${SPLUNK_HOME}/etc/apps/TA-threatquotient-add-on/default/ta_threatquotient_add_on_settings.conf`, make the following configuration change:

Splunk Search for Listing TQ Indicators

```
[additional_parameters]
verify_cert = false
```

Data Extraction from ThreatQuotient

On the **Inputs** tab, you can click **Create New Input** to add a data collection job as shown below.



Update ThreatQ indicators ×

Name *
Enter a unique name for the data input

Interval *
Time interval of input in seconds between 60 and 7200. Default: 300

Index *

Export ID *
The ThreatQ export ID to use for data collection. Default: splunk

Export Token *
The ThreatQ export token to use for data collection

Export Hash *
The ThreatQ export hash to use for data collection. Default: 1

Threshold Indicator Score
Minimum threshold score for collecting indicators. Indicators with score greater than equal to provided score will only be collected. Default: 8

Indicator Status *
Indicator status for collecting indicators. Indicators with provided status will only be collected. Values must be separated by a single comma. Default: Active,Whitelisted

Figure 4: Configuration of Input Data Extraction

ThreatQ instances starting with versions **4.16.0** are shipped with an **Export** that this App uses. Upon the first execution of this job, it results in the export of all indicators. Every sub-

sequent run of this job only results in getting new indicators as well as previously exported indicators that have since changed. Various configuration parameters are described below.

- **Interval:** The frequency of this job. For a faster detection and response, this value can be reduced. Minimum allowed is 60 seconds.
- **Threshold Indicator Score:** Any indicator below this score is not indexed in Splunk. This threshold is very useful to reduce the data being indexed in the ThreatQuotient App. **Default: 8**
- **Indicator Status:** Similar to the score threshold, any indicator not matching the status configured here is not indexed in Splunk. Again, this technique is useful for reducing indexed data. **Default: Active, Whitelisted**
- **Export ID:** Defaulted to **splunk** if you are using the default Splunk export in ThreatQ. If you make a copy of the export, you must configure the ID of the export in this field as seen on the ThreatQ instance.
- **Export Token:** On the ThreatQ appliance, find the export named as **Splunk Indicators Export** and click **Connection Settings**. The token is available in the following configuration screen. See the picture below for reference.



Figure 5: Splunk Export in ThreatQuotient

- **Export Hash:** Defaults to 1. In the event you want to re-export all indicators from ThreatQ for any reason (such as installing a new Splunk instance), use this configuration. You can configure a different alphanumeric value of length up to 32 and cause exporting all indicators from ThreatQuotient again.



Limitations

- Reducing the set of indicators in Splunk comes at the expense of inability to detect change of scores and/or statuses in indicators. We recommend that users use the "Whitelisted" status in ThreatQ to



mark indicators as false positives rather than reducing the indicator score or using custom statuses.

- It is possible to configure custom indicator statuses (other than Active and Whitelisted) and use those statuses in the workflow for interaction with the **ThreatQuotient Add-on**.
- If you want to use advanced filters (such as adversaries, attributes or sources) to export only a subset of indicators from ThreatQuotient to Splunk, there are two ways to do it:
 - Duplicate the default export, and configure advanced filters. On the Splunk Add-On App, configure scoring filter in such a way that all indicators are accepted (i.e. value of 0).
 - Configure a scoring policy to influence indicator scores on certain adversaries, sources or attributes only. On the Splunk Add-On App, configure the scoring filter to accept only certain scores (i.e. value ≥ 8 for example).

Data Loading in Splunk

As shown in Figure 4, the **Index** parameter allows you to map the data extracted from a job in a predetermined Splunk index. You can create multiple jobs and map them to different Splunk indexes as desired.

ThreatQuotient App

This App does not require any configuration.

Sightings and Feedback to ThreatQ

One of the primary features of this solution is to identify sightings and report them back to ThreatQ.

Sighting in this context is defined as evidence that a **ThreatQ Indicator** was discovered in one or more of the events in Splunk collected via other sources. Recording these sightings

and reporting them back to ThreatQ provides analysts with important context around indicators included in their threat intelligence holdings. This section describes various user configurations (in form of macros and saved searches) available to the user to achieve this, and concludes with a summary diagram that describes the whole process.

Separation of Data

ThreatQ indicator data is separated from the rest of the data in this App using a specific **sourcetype**. You can use the following Splunk search query to discover all indicators exported from ThreatQuotient.

Splunk Search for Listing TQ Indicators

```
sourcetype="threatq:indicators"
```



Note that the same indicator can be exported multiple times if it experienced a change of status and/or score.

Macros

The following macros are used in most of the saved searches this App is configured with (available under **Settings > Advanced Search > Search Macros**).

Search macros				
Advanced search » Search macros				
App context ThreatQuotient App For Splunk				
☒ Show only objects created in this app context Learn more				
New				
Showing 1-7 of 7 items				
Name	Definition	Arguments	Owner	App
threatq_format_epoch_time(1)	strftime(timestamp\$, "%Y-%m-%d %H:%M:%S")	timestamp	No owner	ThreatQAppforSplunk
threatq_index	index=main		No owner	ThreatQAppforSplunk
threatq_match_indices	(index="*)		No owner	ThreatQAppforSplunk
threatq_match_sourcetypes	()		No owner	ThreatQAppforSplunk
threatq_parse_updated_at(1)	strftime(updated_at\$, "%Y-%m-%d %H:%M:%S %Z")	updated_at	No owner	ThreatQAppforSplunk
threatq_score_filter	(score=>0)		No owner	ThreatQAppforSplunk
threatq_status_filter	(status=*)		No owner	ThreatQAppforSplunk

Figure 6: Configurable Macros in ThreatQuotient App

The description of some of these search macros is below.

Saved Search Macro	Description
threatq_index	Configures the name of the Splunk index that all ThreatQ indicators are mapped to.
threatq_match_indices	Configures which Splunk indices are considered for matching. The users can apply more specific filters here.
threatq_match_sourcetypes	Configures which sourcetypes should be excluded from matching (the sourcetype threatq:indicators is automatically excluded).
threatq_score_filter	Configures a score filter for all indexed indicators from ThreatQ that should be considered for detecting sightings.
threatq_status_filter	In conjunction with the score filter, configures a

Saved Search Macro	Description
	status filter for all indexed indicators from ThreatQ to be considered for detecting sightings.

[Table 2: Configurable Macros]

Saved Searches

The Splunk App uses saved searches for discovering sightings and reporting them back to ThreatQ. The App is preconfigured with saved searches, which are periodic processes (registered to the crontab) designed to map indicators to specific Splunk indices and match these indicators to events. Saved search processes also move older indicators out of the main lookup tables and for ES customers, move indicators to specific ES lookup tables according to the mapping described in this document.

The table below describes some of the saved searches this App is preconfigured with.

Saved Search	Description	Default Period
<code>threatq_update_master_lookup</code>	Fetch ThreatQ indicators from the default index and link them against the master lookup table . This prepares the indicators for detecting evidence of sightings.	15 mins
<code>threatq_match_indicators</code>	Finds evidence of sightings for all indicators in the master lookup table . If sightings are detected, indicators are moved to the match lookup table .	30 mins

Saved Search	Description	Default Period
<code>threatq_cleanup_indicators_on_indicators_change</code>	If indicator status changes from Active to Whitelisted (or any other status not considered for finding evidence of sightings), or if the indicator score drops below a threshold (making the indicator ineligible for finding evidence of sightings), removes those indicators from both master lookup table and match lookup table .	15 mins
<code>threatq_update_matched_indicators</code>	Finds evidence of sightings for all indicators in the match lookup table .	30 mins
<code>threatq_consume_indicators</code>	Creates events in ThreatQ for all newly detected sightings.	15 mins
<code>threatq_update_retired_indicators</code>	Clean up indicators that haven't been matched on in the last 90 days from both master lookup table and match lookup table .	1440 mins

[Table 3: Saved Searches for Discovering and Reporting of Sightings]



Editability rules

Because of the way sightings are found in Splunk using two saved searches (**threatq_match_indicators** and **threatq_update_matched_indicators**), their frequency must be the same if edited. The default frequency for both saved searches is 30 mins.

Saved Searches Documentation

The following table documents the macros for saved searches as configured by default on the ThreatQuotient App.

Saved Search	Default Macro
threatq_update_master_lookup	<pre>`threatq_index` source- type="threatq:indicators" `threatq_ score_filter` `threatq_status_filter` dedup value eval ioc_id=id, ioc_value=value, sources='sources{}.value', adversar- ies='adversaries{}.value' table value, updated_at, status, type, score, ioc_id, ioc_value, sources, adversaries outputlookup key_field=value master_ lookup join ioc_value [inputlookup threatq_matched_indic- ators table ioc_value, match_time, first_ seen, last_seen, match_count, sid] eval value=ioc_value table ioc_id, ioc_value, value, match_time, first_seen, last_seen, match_count, score, status, type, updated_at, sources,</pre>

Saved Search	Default Macro
	adversaries, sid outputlookup key_ field=value threatq_matched_indic- ators
threatq_cleanup_ indicators_on_indic- ators_change	inputlookup master_lookup search NOT [search `threatq_index` source- type="threatq:indicators" dedup value search [inputlookup mas- ter_lookup table ioc_value rename ioc_value as value format] NOT (`threatq_score_filter` `threatq_status_filter`) table value rename value as ioc_value format] outputlookup master_lookup join ioc_value [inputlookup threatq_matched_indicators table ioc_value, match_time, first_seen, last_seen, match_count, sid] out- putlookup threatq_matched_indicators
threatq_match_indic- ators	`threatq_match_indices` `threatq_ match_sourcetypes` source- type!="threatq:indicators" threatqmatchiocs

Saved Search	Default Macro
threatq_update_matched_indicators	<code>`threatq_match_indices` `threatq_match_sourcetypes` source-type!="threatq:indicators" threatqmatchiocs is_update=true</code>
threatq_consume_indicators	<code> inputlookup threatq_matched_indicators eval start_time=relative_time(now(), "-16m") where last_seen > start_time threatqconsumeindicators</code>

Saved Search	Default Macro
threatq_update_ retired_indicators	<pre> inputlookup master_lookup search NOT [inputlookup master_lookup search NOT [inputlookup threatq_ matched_indicators search NOT [inputlookup threatq_ matched_indicators eval threshold_ time=now()-7776000, value=ioc_value where last_seen < threshold_time outputlookup key_field=value threatq_ retired_matched_indicators table ioc_value format] outputlookup threatq_ matched_indicators table ioc_value format] eval threshold_time=now()-7776000, updated_at_epoch=`threatq_parse_ updated_at(updated_at)`, value=ioc_ value where updated_at_epoch < threshold_ time outputlookup key_field=value threatq_retired_indicators table ioc_value format] outputlookup master_lookup</pre>

[Table 4: Saved Search Macros]

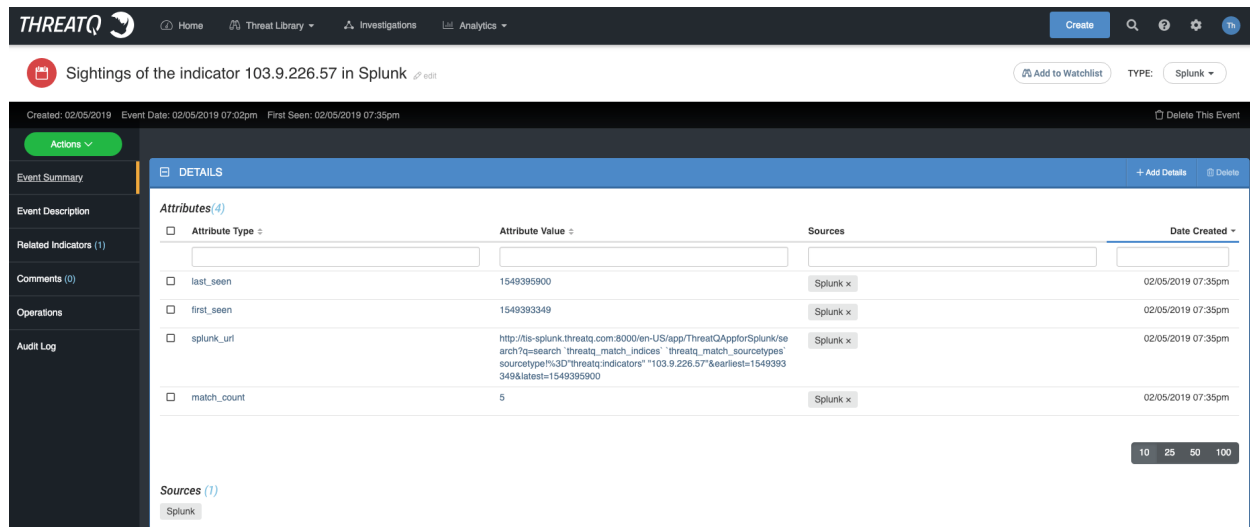
Reporting Sightings in ThreatQ

A sighting in Splunk is evidence that an indicator from ThreatQ was seen in one or more events in Splunk. To an analyst, this is important information that can be reported back in form of an Event.

ThreatQuotient captures all sightings for an indicator in a single event. When more sightings are detected for the same indicator, certain attributes for that event are updated - this allows the analyst to gather context on sightings for that indicator. The following 4 attributes are recorded for the event.

- **First Seen:** Timestamp when the first sighting for this indicator was recorded in Splunk. This attribute does not change.
- **Last Seen:** Timestamp when the latest sighting for this indicator is recorded in Splunk. This attribute updates as newer sightings are detected.
- **Count:** The total count of all sightings recorded for this indicator starting from the time **First Seen** until **Last Seen**.
- **Splunk URL:** The URL that allows the analyst to view all sightings for this indicator in Splunk starting from **First Seen** until **Last Seen**.

The screen capture below shows an example event recorded in ThreatQuotient by the Splunk App.



Created: 02/05/2019 Event Date: 02/05/2019 07:02pm First Seen: 02/05/2019 07:35pm

Actions

Event Summary

Event Description

Related Indicators (1)

Comments (0)

Operations

Audit Log

DETAILS

Attributes (4)

Attribute Type	Attribute Value	Sources	Date Created
last_seen	1549395900	Splunk x	02/05/2019 07:35pm
first_seen	1549393349	Splunk x	02/05/2019 07:35pm
splunk_url	http://ts-splunk.threatq.com:8000/en-US/app/ThreatQAppForSplunk/search?q=search%20threatq_match_indices%20threatq_match_sourcetypes%20sourceip%3D%20103.9.226.57&earliest=1549393349&latest=1549395900	Splunk x	02/05/2019 07:35pm
match_count	5	Splunk x	02/05/2019 07:35pm

Sources (1)

Splunk

Figure 7: Example Event in ThreatQ

Putting Everything Together

The following steps summarize how indicators are stored in Splunk and how sightings are reported back to ThreatQ.

1. The Input job configured on **ThreatQuotient Add-on** (on the heavy forwarder) pulls indicators from ThreatQ.
2. The heavy forwarder sends the indicators to the indexer which indexes the indicators to the **default** index (user can override).
3. The periodic saved search job **threatq_update_master_lookup** maps the newly indexed ThreatQ indicators to the **master lookup table**.
4. The periodic saved search job **threatq_match_indicators** finds evidence of sightings of all indicators in the **master lookup table** against all events in Splunk (as filtered via various configurable macros described above in this section).
 - a. If evidence of sightings is found for a specific indicator, it is moved to the **match lookup table**.

5. Simultaneously, another periodic saved search job **threatq_update_matched_indicators** finds more sightings for all indicators from the **match lookup table** against all events in Splunk (as filtered by the same configurable macros).
6. A periodic saved search **threatq_consume_indicators** will create events in ThreatQ to represent evidence of sightings in Splunk.
7. The periodic saved search job **threatq_update_retired_indicators** takes all indicators that are not updated in the past 90 days out of both the **master lookup table** and **matched lookup table**.

The following diagram summarizes this process.

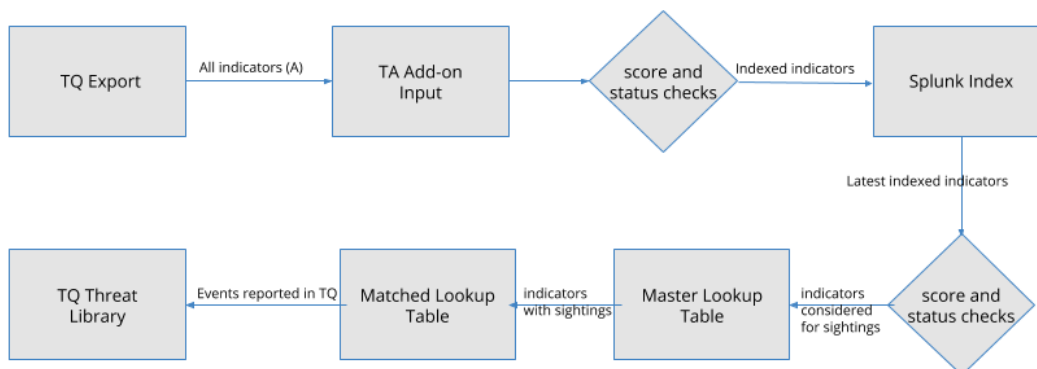


Figure 8: Detecting and Reporting Indicator Matches to ThreatQ

Workflow Actions

The **ThreatQuotient Add-on** provides five user workflow actions to the analysts for providing interactivity with the ThreatQuotient platform from Splunk. As shown on the diagram below, the actions can be invoked on any Splunk event by expanding the event view and clicking on the downarrow in the column below **Action**.

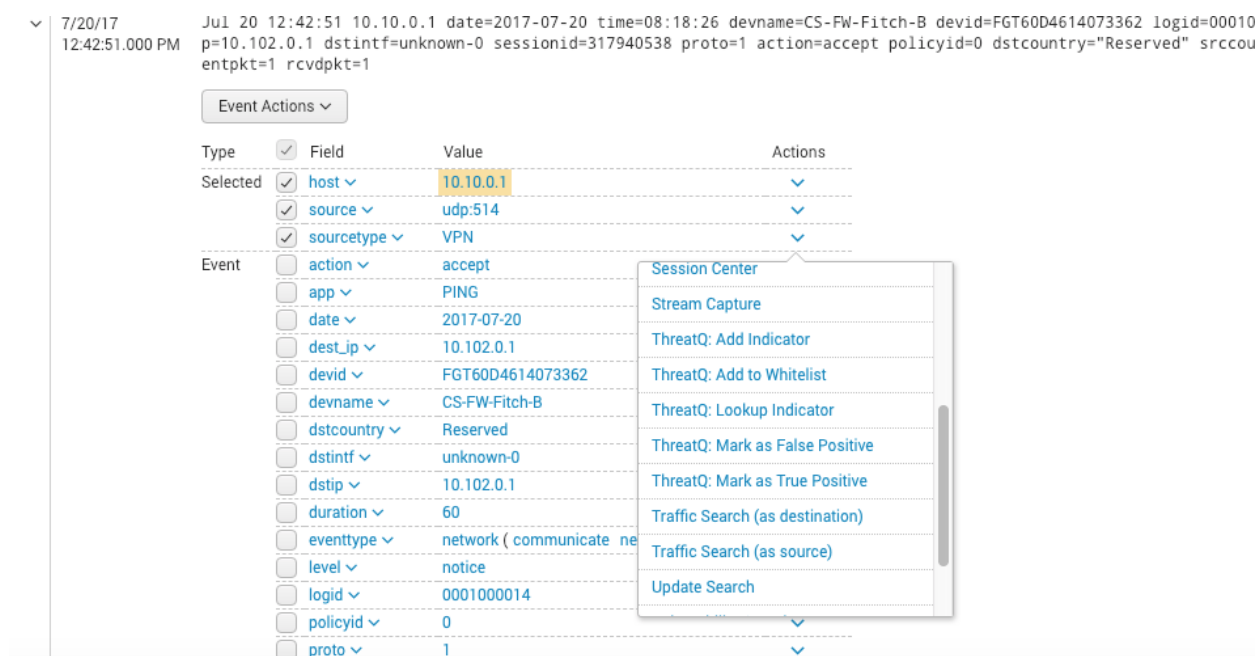


Figure 10: ThreatQuotient Workflow Actions

The actions are described below.

ThreatQ: Add Indicator

This workflow action adds the indicator to ThreatQ. You are presented with UI inputs that allow you to select indicator type, status and source. If the data and type do not match, an error is reported. Successful completion of this workflow action results in the indicator being successfully added to the ThreatQ Threat Library.

ThreatQ: Add to Whitelist

This workflow action sets the status of the indicator to **Whitelisted** in ThreatQ. If the indicator does not exist in ThreatQ, an error is reported.

ThreatQ: Lookup Indicator

This workflow action searches for an indicator in ThreatQ and pulls additional context for that indicator. If the indicator does not exist in ThreatQ, an error is reported.

ThreatQ: Mark as False Positive

This workflow action adds the attribute key-value "**False Positive: True**" to the indicator in ThreatQ. If the indicator does not exist in ThreatQ, an error is reported.

ThreatQ: Mark as True Positive

This workflow action adds the attribute key-value "**True Positive: True**" to the indicator in ThreatQ. If the indicator does not exist in ThreatQ, an error is reported.

Enterprise Security Support

ThreatQ Indicators to Splunk Lookup Mapping Table (using CIM)

The App provides support to the Splunk Enterprise Security (ES) customers by making ThreatQ data more accessible using Splunk's native ES lookup tables. The following table provides how ThreatQ data is mapped to the Splunk ES lookup tables. This data is then available in various ES dashboards.

ThreatQ type	Threat intelligence type
CIDR Block	local_ip_intel
Email Address	local_email_intel
Email Subject	local_email_intel
File Name	local_file_intel
FQDN	local_domain_intel
Fuzzy Hash	local_file_intel
GOST Hash	local_file_intel
IP Address	local_ip_intel
MD5	local_file_intel
Registry Key	local_registry_intel
Service Name	local_service_intel
SHA-1	local_file_intel
SHA-256	local_file_intel

ThreatQ type	Threat intelligence type
SHA-384	local_file_intel
SHA-512	local_file_intel
x509 Serial	local_certificate_intel
x509 Subject	local_certificate_intel
URL	local_http_intel
URL Path	local_http_intel
Username	local_user_intel

[Table 5: ThreatQ indicator mapping
using Splunk Common Information
Model (CIM)]

To view the events and indicators, navigate to **Enterprise Security > Security Intelligence > Threat Intelligence**.

- **Threat Activity:** Shows the list of event which are compatible with CIM apps.
- **Threat Artifacts:** Shows the list of indicators fetched from the ThreatQ

Saved Searches for CIM Mapping

In addition to the core saved searches, the following saved searches apply for Enterprise Security (ES) customers. The saved searches listed run once a day and map ThreatQ indicators by type to Splunk ES lookup tables as described in the **Mapping Table** section of the document.

ES Saved Search	Description
threatq_update_threat_intelligence_lookup_email_address	Map ThreatQ type 4 indicators to local_email_intel
threatq_update_threat_intelligence_lookup_email_subject	Map ThreatQ type 6 indicators to local_email_intel
threatq_update_threat_intelligence_lookup_file_name	Map ThreatQ type 9 indicators to local_file_intel
threatq_update_threat_intelligence_lookup_fqdn	Map ThreatQ type 10 indicators to local_domain_intel
threatq_update_threat_intelligence_lookup_hash	Map ThreatQ type [11,12,15,20,21,22,23] indicators to local_file_intel
threatq_update_threat_intelligence_lookup_ip	Map ThreatQ type 14 indicators to local_ip_intel
threatq_update_threat_intelligence_lookup_registry	Map ThreatQ type 18 indicators to local_registry_intel
threatq_update_threat_intelligence_lookup_service	Map ThreatQ type 19 indicators to local_service_intel
threatq_update_threat_intelligence_lookup_certificate_serial	Map ThreatQ type 25 indicators to local_certificate_intel

ES Saved Search	Description
threatq_update_threat_intelligence_lookup_certificate_subject	Map ThreatQ type 26 indicators to local_certificate_intel
threatq_update_threat_intelligence_lookup_url	Map ThreatQ type 27 indicators to local_http_intel
threatq_update_threat_intelligence_lookup_user	Map ThreatQ type 30 indicators to local_user_intel

[Table 6: Saved Searches for Mapping ThreatQ Indicator data to Splunk's CIM]

Dashboards

Preconfigured dashboards are packaged with **ThreatQuotient App** to allow the analyst versatile visual representation of all indicator data from ThreatQ and the corresponding sightings.

Cumulative Counts

The top section of the dashboard shows total count for all ThreatQ indicators in the **master lookup table** (on the left) and the **match lookup table** (in the right) (all time and the last 24 hours). It is important to note that the data displayed as Sightings are not the total sightings; rather it is the total number of indicators for which evidence of sightings has been found. Example screen capture below.



Figure 10: Dashboard: Cumulative Counts

Score Breakdown

The next section shows the distribution of indicator scores for indicators in master and match lookup tables as bar charts. Example screenshot below. These charts do not have a time filter. The counts for individual score breakdown represent the cumulative indicator count. As an example, notice that there are two indicators with sightings each with score 9 (which matches up with the cumulative sightings count of 2 in the chart above).

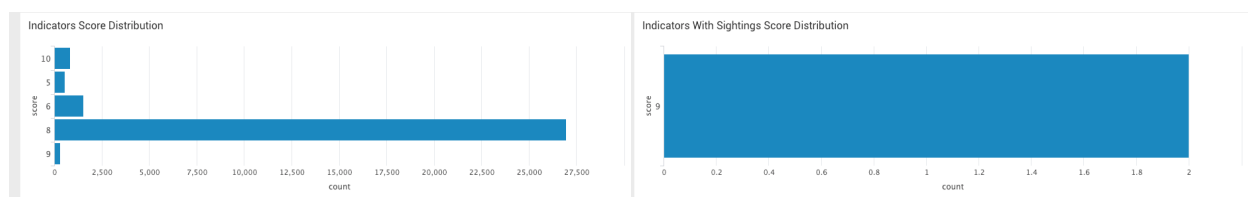


Figure 11: Dashboard: Score Breakdown

Type Breakdown

This section shows the distribution of indicator types for indicators in master and match lookup tables as pie charts. As the score distributions above, these are cumulative

distributions. Example screenshot below. Hovering over each portion of the pie chart will display the indicator count for that specific portion.

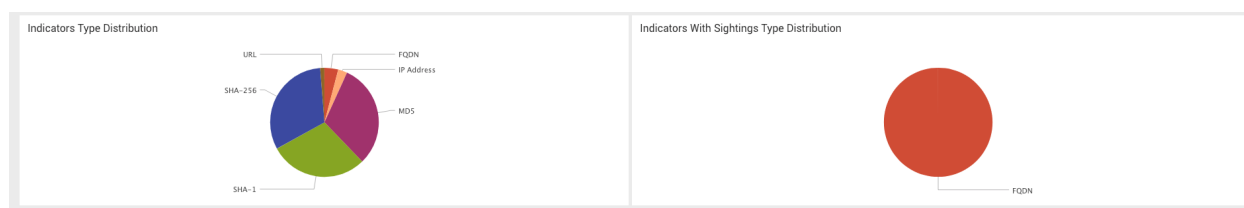


Figure 12: Dashboard: Type Breakdown
Source Breakdown

This section shows the breakdown of indicators and sighted indicators by sources. Example screenshot below. One thing to note here is that all indicators must have at least one source, but some indicators may have more than one. For this reason, the cumulative counts in the charts below may exceed the total number of indicators and sighted indicators in the lookup tables.

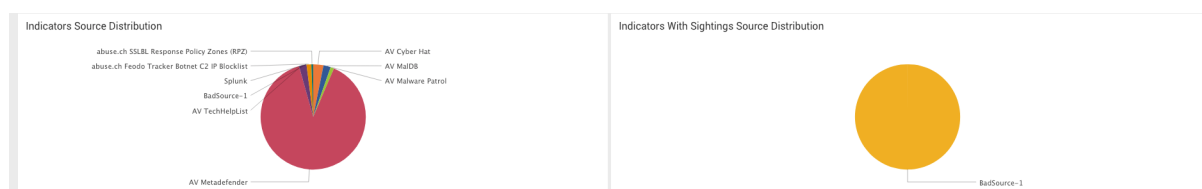


Figure 13: Dashboard: Source Breakdown

Adversaries Breakdown

This section shows the breakdown of indicators and sighted indicators by adversaries. Example screenshot below. One thing to note here is that not all indicators have adversaries; although some indicators may have more than one. Depending upon how many indicators have adversaries, the total cumulative counts in the charts below may be less or more than the total indicators and sighted indicators in the lookup tables. For the example dataset below, there is only one adversary assigned to a few indicators, and those same indicators are sighted.

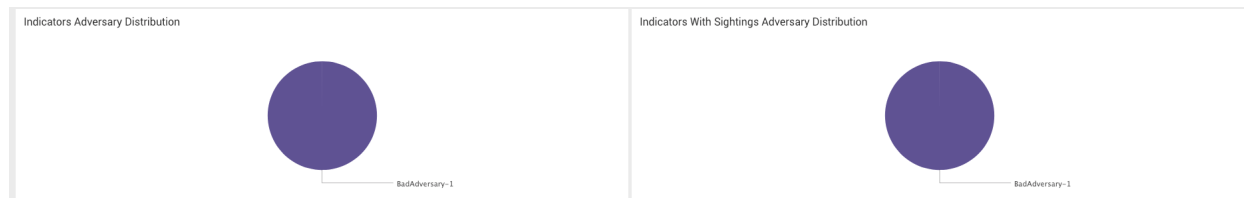


Figure 14: Dashboard: Adversary Breakdown

Static Table View

This section shows all indicators and sightings in static tables - time filters are provided and defaulted to the last 24 hours. Score and type filters are also available for both. This information gives a threat analyst a single place to view all sightings in Splunk. In the screenshot below, notice there are two indicators sighted, each with 2 sightings.

Indicators

Time range

Score

Type

All Time

0

All

Value	Score	Type	Updated Time	Sources	Adversaries
0007993095dc455ac9073acfe3af2	8	MD5	2019-02-07 21:49:44	AV Metadefender	
000a5e550012e11821873dbdb5e5e4e98f550dee4feb81154087e9059d0005	8	SHA-256	2019-02-07 21:47:41	AV Metadefender	
000a8fa388691a52a5304402a62a26a4	8	MD5	2019-02-07 22:23:13	AV Metadefender	
000c3d90c784b2ad494648dc7d547afcd03071bab0214a948e49ffa5997ad46	8	SHA-256	2019-02-07 21:37:36	AV Metadefender	
000fbc24a7f6c2dcfcad40bda3944	8	MD5	2019-02-07 22:28:50	AV Metadefender	
00116019e25024d10979516c32fa3f01afb5116	8	SHA-1	2019-02-07 22:12:28	AV Metadefender	
001233329f99040f18664c541b0e3e83ca0c14f6474d7324d3bc23f2f8	8	SHA-256	2019-02-07 21:50:24	AV Metadefender	
0012889417c3d00bfa37a5633c23f03ae7512e1a	8	SHA-1	2019-02-07 22:12:44	AV Metadefender	
00155fa3e7cd0a05c0756230ef6c0c8a	8	MD5	2019-02-07 21:50:59	AV Metadefender	
0015b54e073494c9fb12e1b07235ad6e933fcd2446560071b9a0d27da7854	8	SHA-256	2019-02-07 21:52:51	AV Metadefender	

+ prev

1

2

3

4

5

6

7

8

9

10

next >

Top 10 Indicators By Sightings

Value	Score	Type	Sources	Adversaries	First Seen	Last Seen	Sightings
baddomain.com	9	FQDN	BadSource-1	BadAdversary-1	2019-01-31 15:57:17	2019-02-01 16:00:00	2
baddomain2.com	9	FQDN	BadSource-1	BadAdversary-1	2019-01-31 15:57:17	2019-02-01 16:00:00	2

Indicators With Sightings

Time range

Score

Type

All Time

0

All

Value	Score	Type	Sources	Adversaries	First Seen	Last Seen	Sightings
baddomain.com	9	FQDN	BadSource-1	BadAdversary-1	2019-01-31 15:57:17	2019-02-01 16:00:00	2
baddomain2.com	9	FQDN	BadSource-1	BadAdversary-1	2019-01-31 15:57:17	2019-02-01 16:00:00	2

Figure 15: Dashboard: Static Indicators and Sighted Indicators Tables

Top 10 By Sightings

The final section displays top 10 indicators by sightings, top 10 sources by sightings and top 10 adversaries by sightings in form of a static table, bar chart and bar chart respectively. This information gives an analyst a quick view of the indicators sources and adversaries with the most matches within Splunk.

Top 10 Indicators By Sightings							
Value	Score	Type	Sources	Adversaries	First Seen	Last Seen	Sightings
badomain.com	9	FQDN	BadSource-1	BadAdversary-1	2019-01-31 15:57:17	2019-02-01 16:00:00	2
badomain2.com	9	FQDN	BadSource-1	BadAdversary-1	2019-01-31 15:57:17	2019-02-01 16:00:00	2

Figure 16: Dashboard: Top 10 Indicators by Sightings Sources

Example screenshot below. Notice the source **BadSource-1** appears as the top source with sightings corresponding to the sighted indicators as displayed in the static table above. Also notice that the sightings count is 4, which corresponds to 2 sightings each for the sighted indicators.

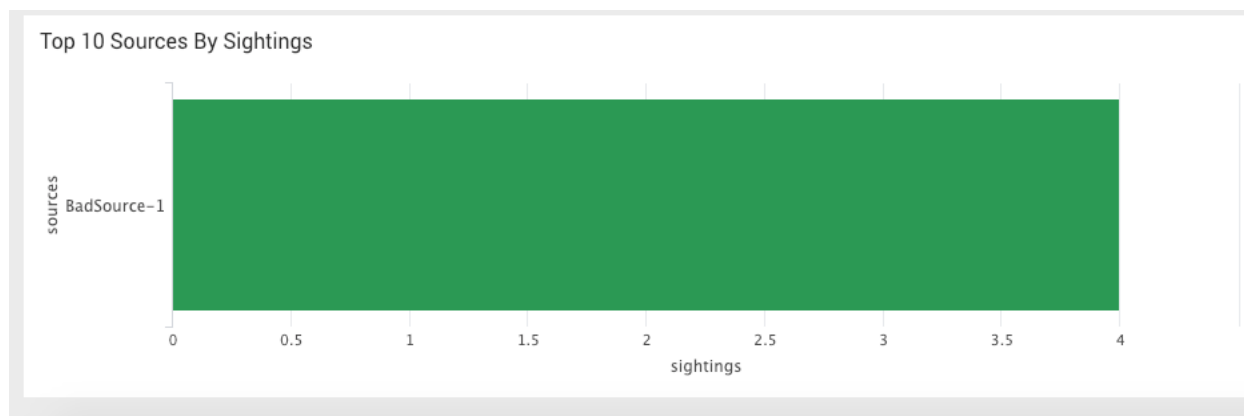


Figure 17: Dashboard: Top 10 Sources by Sightings Adversaries

Example screenshot below. Notice the source **BadAdversary-1** appears as the top adversary with sightings corresponding to the sighted indicators as displayed in the static table above. Also notice that the sightings count is 4, which corresponds to 2 sightings each for the sighted indicators.

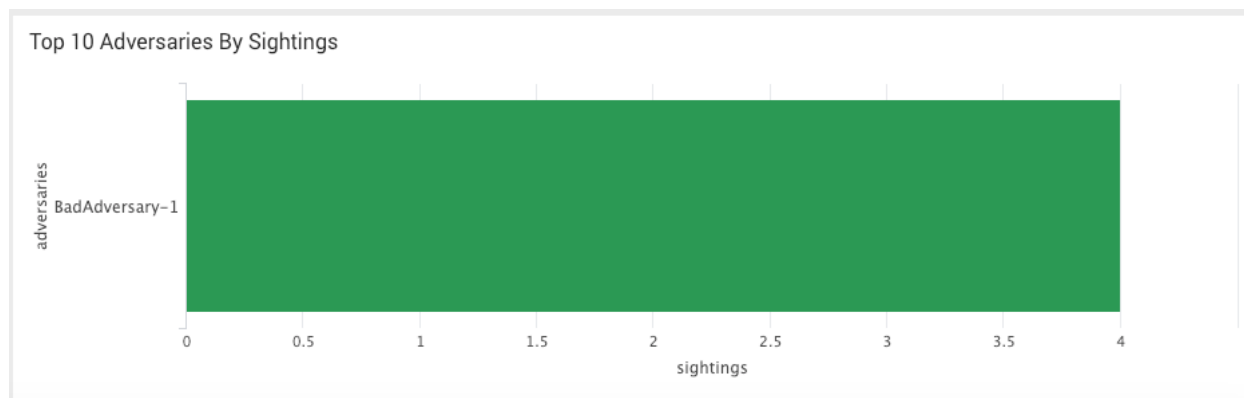


Figure 18: Dashboard: Top 10 Adversaries by Sightings

Troubleshooting

- To troubleshoot **ThreatQuotient Add-on** please check the log file below:

```
$SPLUNK_HOME/var/log/Splunk/ta_threatquotient_  
add_on_threatq_indicators.log
```

- To find all unique indicators indexed in Splunk by the Add-On (Splunk App allows you to select a specific time range):

```
sourcetype="threatq:indicators" | dedup value
```

- To check the data collected by data collection use query like:

```
"index=your_index_name sourcetype=threatq_indic-  
ators"
```

- Make sure all the saved searches are enabled.
- Make sure the macro is updated as per the settings.

- To troubleshoot any behavior with the master table lookup tables (which is used in the dashboards), the following query is useful:

```
index=_internal sourcetype="scheduler" saved-  
search_name=threatq_update_master_lookup status-  
s=success
```

The log file can be found at the following location:

```
/opt/splunk/var/log/splunk/scheduler.log
```

- If the user changes macros for global score and status thresholds, the audit logs can be accessed using the following two saved searches:

Splunk Search for Listing TQ Indicators

```
index=_internal threatq_score_filter source-  
type="splunkd_ui_access"  
index=_internal threatq_score_filter source-  
type="splunkd_access"
```

- Logs for the saved search to update the master lookup table can be accessed using the following query (the same query can be used to check the run statuses of any saved search; just replace with the appropriate saved search name):

```
index=_internal sourcetype=scheduler saved-  
search_id="nobody;threatqappforsplunk;threatq_  
update_master_lookup
```