ThreatQuotient

Splunk SOAR App for ThreatQ

Version 2.3.2

April 01, 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

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.

App Details

ThreatQuotient provides the following details for this app:

Current Integration Version	2.3.2
Compatible with ThreatQ Versions	>= 4.30.0
Splunk Products	SOAR On-Prem, SOAR Cloud
SOAR Versions	>= 5.3.0
Support Tier	ThreatQ Supported
Python Version	3

Introduction

The Splunk SOAR App for ThreatQ allows a user to execute a variety of actions on ThreatQ from a Phantom playbook.

> Splunk SOAR App for ThreatQ replaces the Phantom App for ThreatQ application.

With ThreatQ as a single source of truth for Threat Intelligence, you will be able to accurately triage a sighting, and ultimately, make quicker decisions. This allows you to increase your response time and improve your ROI by focusing on what's important to your organization, instead of being inundated with sightings of non-malicious indicators.

The app provides the following actions:

- **Test Connectivity** - Validates the asset configuration for connectivity.
- **Query Indicators** - Queries a list of indicators against ThreatQ.
- **Create Indicators** - Creates indicators in ThreatQ.
- **Create Task** - Creates a task in ThreatQ.
- **Create Event** - Creates an event in ThreatQ based on the Phantom container metadata.
- **Upload Spearphish** - Creates a spearphish event in ThreatQ based on a spearphish email in the Phantom vault.
- **Upload File** - Creates a file attachment in ThreatQ.
- **Start Investigation** - Creates a ThreatQ Investigation in the ThreatQ platform.
- **Create Adversaries** - Creates adversaries in ThreatQ.
- **Create Custom Objects** - Creates custom objects in ThreatQ.
- **Add Attribute** - Adds an attribute to a list of custom objects.
- **Set Indicator Status** - Sets the status of an indicator in ThreatQ.
- **Get Related Objects** - Queries ThreatQ for an object's relationships.
- **Create Signature** - Create a signature within ThreatQ.
- **Add Tag** - Adds a tag to an object in ThreatQ.
- **Add Comment** - Adds a comment to an object in ThreatQ.

> See the App Actions chapter of this guide for more details on these actions.

Installation

This section will describe how you can install the app into your Phantom instance.

> ⚠ Splunk SOAR App v2.0.0 has fundamentally changed how the App operates. If you are upgrading from v1.x, please refer to the Upgrading from 1.x to 2.x section under the Additional App Instructions chapter.

1. Download the **Splunk SOAR App for ThreatQ (tar.gz)** from Splunkbase: https://splunkbase.splunk.com/app/6082/
2. Log into your Phantom instance.
3. Select **Apps** from your navigation dropdown.
4. Click on the **Install App** button at the top right of your Apps page.
5. Select the **Splunk SOAR App for ThreatQ tar.gz** file.

The app will now be installed but still needs to be configured.

Configuration

Once the app is installed, you will see a ThreatQ logo on your Apps page. You can also locate the app by searching for `ThreatQ` in the search bar.

1. Click on the **Configure New Asset** button located next to the ThreatQ logo.
2. Enter following information in the *Asset Info* tab.

FIELD	VALUE
Asset Name	threatq
Asset Description	Integration with the ThreatQ Threat Intelligence Platform.
Product Vendor	ThreatQuotient
Product Name	ThreatQ

3. Click on **Save**.
4. Enter the following information in the *Asset Settings* tab.

FIELD	VALUE
Server IP/ Hostname	Enter the hostname or IP address for your ThreatQ instance.
Client ID	Enter your API Credentials found under your **My Account** page in ThreatQ.
Username	Enter your username to authenticate with ThreatQ.
Password	Enter your password to authenticate with ThreatQ.
Trust SSL Certificate	Check this box if you want to trust the ThreatQ certificate. This option is checked by default.

5. Click on **Save**.
6. Click the **Test Connectivity** button to test your connection information.

> If this test fails, verify that your Phantom instance has access to your ThreatQ instance and confirm that your credentials are correct.

The ThreatQ App will now be configurable within a playbook.

App Actions

The following actions come out of the box with the Splunk SOAR App for ThreatQ.

ACTION	DESCRIPTION
Test Connectivity	Validates the asset configuration for connectivity.
Query Indicators	Queries a list of indicators against ThreatQ.
Create Indicators	Creates indicators in ThreatQ.
Create Task	Creates a task in ThreatQ.
Create Event	Creates an event in ThreatQ based on the Phantom container metadata.
Upload Spearphish	Creates a spearphish event in ThreatQ based on a spearphish email in the Phantom vault.
Upload File	Creates a file attachment in ThreatQ.
Start Investigation	Creates a ThreatQ Investigation in the ThreatQ platform.
Create Adversaries	Creates adversaries in ThreatQ.
Create Custom Objects	Creates custom objects in ThreatQ.
Add Attribute	Adds an attribute to a list of custom objects.
Set Indicator Status	Sets the status of an indicator in ThreatQ.
Get Related Objects	Queries ThreatQ for an object's relationships.

ACTION	DESCRIPTION
Create Signature	Create a signature within ThreatQ.
Add Tag	Add a tag to an object in ThreatQ.
Add Comment	Add a comment to an object in ThreatQ.

Test Connectivity

FIELD	DETAILS
Type	test
Description	Validate the asset configuration for connectivity.

Query Indicators

FIELD	DETAILS
Name	query_indicators
Type	investigate
Description	Query a list of indicators against ThreatQ

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
indicator_list	required	A comma-separated or line-separated list of indicator values	string	`domain` `ip` `email` `url` `hash` `sha256` `string` `file name` `file path` `host name` `md5` `process name` `sha1` `user name`
exact	optional	Do we want to find an exact match or an approximate match?	boolean	
with_all_relationships	optional	Should we fetch all relationships with this action?	boolean	

Output

DATA PATH	TYPE	CONTAINS
action_result.parameter.exact	boolean	
action_result.parameter.indicator_list	string	`domain` `ip` `email` `url` `hash` `sha256` `string` `file name` `file path` `host name` `md5` `process name` `sha1` `user name`
action_result.parameter.with_all_relationships	boolean	
action_result.data.*.adversaries.*.name	string	
action_result.data.*.attack_pattern.*.value	string	
action_result.data.*.attributes	string	
action_result.data.*.campaign.*.value	string	
action_result.data.*.course_of_action.*.value	string	
action_result.data.*.events.*.title	string	
action_result.data.*.exploit_targets.*.value	string	
action_result.data.*.identity.*.value	string	
action_result.data.*.incident.*.value	string	
action_result.data.*.indicators.*.value	string	
action_result.data.*.intrusion_set.*.value	string	
action_result.data.*.malware.*.value	string	

DATA PATH	TYPE	CONTAINS
action_result.data.*.report.*.value	string	
action_result.data.*.score	numeric	
action_result.data.*.signatures.*.name	string	
action_result.data.*.signatures.*.value	string	
action_result.data.*.sources.*.name	string	
action_result.data.*.status.name	string	
action_result.data.*.tool.*.value	string	
action_result.data.*.ttp.*.value	string	
action_result.data.*.type.name	string	
action_result.data.*.value	string	
action_result.data.*.vulnerability.*.value	string	
action_result.status	string	
action_result.message	string	
action_result.summary.total	numeric	
summary.total_objects	numeric	
summary.total_objects_successful	numeric	

Create Indicators

FIELD	DETAILS
Name	create_indicators
Type	Generic
Description	Create indicators in ThreatQ
Formatting	See the Formatting an Indicator List section.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
indicator_list	required	A comma-separated or line-separated list of indicators and indicator type (optional) name/value pairs (e.g.: IP Address: 1.1.1.1)	string	`domain` `ip` `email` `url` `hash` `sha256` `string` `file name` `file path` `host name` `md5` `process name` `sha1` `user name`
indicator_status	optional	The default status for the indicators uploaded to ThreatQ	string	

Output

DATA PATH	TYPE	CONTAINS
action_result.parameter.indicator_list	string	`domain` `ip` `email` `url` `hash` `sha256` `string` `file name` `file path` `host`

DATA PATH	TYPE	CONTAINS
		`name` `md5` `process name` `sha1` `user name`
action_result.parameter.indicator_status	string	
action_result.data.*.value	string	
action_result.status	string	
action_result.message	string	
action_result.summary.total	numeric	
summary.total_objects	numeric	
summary.total_objects_successful	numeric	

Create Task

FIELD	DETAILS
Name	create_task
Type	Generic
Description	Create a task in ThreatQ
Formatting	See the Formatting an Indicator List section.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
task_prefix	optional	Prefix for the task name	string	
task_name	required	Task name	string	
assigned_to	optional	ThreatQ user to assign the task to	string	
task_status	required	Task status in ThreatQ	string	
task_priority	required	Task priority in ThreatQ	string	
task_description	optional	Task description in ThreatQ	string	
indicator_list	optional	List of indicator values (use format node)	string	`domain` `ip` `email` `url` `hash` `sha256` `string` `file name` `file path` `host name` `md5` `process`

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
				`name` `sha1` `user name`

Output

DATA PATH	TYPE	CONTAINS
action_result.parameter.assigned_to	string	
action_result.parameter.indicator_list	string	`domain` `ip` `email` `url` `hash` `sha256` `string` `file name` `file path` `host name` `md5` `process name` `sha1` `user name`
action_result.parameter.task_description	string	
action_result.parameter.task_name	string	
action_result.parameter.task_prefix	string	
action_result.parameter.task_priority	string	
action_result.parameter.task_status	string	
action_result.data.*.value	string	
action_result.status	string	
action_result.message	string	
action_result.summary	string	
summary.total_objects	numeric	

DATA PATH	TYPE	CONTAINS
summary.total_objects_successful	numeric	

Create Event

FIELD	DETAILS
Name	create_event
Type	Generic
Description	Creates an event in ThreatQ, based on the container metadata in Phantom
Formatting	See the Formatting an Indicator List section.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
event_type	required	The event type in ThreatQ	string	
indicator_list	optional	List of comma-separated or line-separated indicator	string	`domain` `ip` `email` `url` `hash` `sha256` `string` `file name` `file path` `host name` `md5` `process name` `sha1` `user name`

Output

DATA PATH	TYPE	CONTAINS
action_result.parameter.event_type	string	
action_result.parameter.indicator_list	string	`domain` `ip` `email` `url` `hash` `sha256` `string` `file name` `file path` `host`

DATA PATH	TYPE	CONTAINS
		`name` `md5` `process name` `sha1` `user name`
action_result.data.*.title	string	
action_result.status	string	
action_result.message	string	
action_result.summary	string	
summary.total_objects	numeric	
summary.total_objects_successful	numeric	

Upload Spearphish

FIELD	DETAILS
Name	upload_spearphish
Type	Generic
Description	Creates a spearphish event in ThreatQ, based on a spearphish email in the Phantom vault

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
vault_id	required	The Vault ID for the spearphish email file	string	`vault id`
indicator_status	optional	Default indicator status. If none selected, Review is used	string	

Output

DATA PATH	TYPE	CONTAINS
action_result.parameter.indicator_status	string	
action_result.parameter.vault_id	string	`vault id`
action_result.data.*.title	string	
action_result.status	string	

DATA PATH	TYPE	CONTAINS
action_result.message	string	
action_result.summary	string	
summary.total_objects	numeric	
summary.total_objects_successful	numeric	

Upload File

FIELD	DETAILS
Name	upload_file
Type	Generic
Description	Creates a file (attachment) in ThreatQ

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
vault_id	required	The Vault ID for the file to upload	string	`vault id`
parse_for_indicators	required	Whether or not to parse the file for indicators	boolean	
indicator_status	optional	Default indicator status. If none selected, Review is used	string	

Output

DATA PATH	TYPE	CONTAINS
action_result.parameter.indicator_status	string	
action_result.parameter.parse_for_indicators	boolean	
action_result.parameter.vault_id	string	`vault id`

DATA PATH	TYPE	CONTAINS
action_result.data.*.name	string	
action_result.status	string	
action_result.message	string	
action_result.summary	string	
summary.total_objects	numeric	
summary.total_objects_successful	numeric	

Start Investigation

FIELD	DETAILS
Name	start_investigation
Type	Generic
Description	Creates an investigation in ThreatQ
Formatting	See the Formatting an Indicator List section.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
investigation_name	required	The investigation name	string	
investigation_priority	required	The investigation's priority	string	
investigation_visibility	required	The investigation's sharing status	string	
investigation_description	optional	The investigation's description	string	
indicator_list	required	List of comma-separated or line-separated indicator	string	`domain` `ip` `email` `url` `hash` `sha256` `string` `file name` `file path` `host name` `md5` `process name`

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
				`sha1` `user name`

Output

DATA PATH	TYPE	CONTAINS
action_result.parameter.indicator_list	string	`domain` `ip` `email` `url` `hash` `sha256` `string` `file name` `file path` `host name` `md5` `process name` `sha1` `user name`
action_result.parameter.investigation_description	string	
action_result.parameter.investigation_name	string	
action_result.parameter.investigation_priority	string	
action_result.parameter.investigation_visibility	string	
action_result.data.*.name	string	
action_result.status	string	
action_result.message	string	
action_result.summary	string	
summary.total_objects	numeric	
summary.total_objects_successful	numeric	

Create Adversaries

FIELD	DETAILS
Name	create_adversaries
Type	Generic
Description	Create adversaries in ThreatQ

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE
adversary_list	required	A comma-separated or line-separated list of adversary names	string

Output

DATA PATH	TYPE
action_result.parameter.adversary_list	string
action_result.data.*.name	string
action_result.status	string
action_result.message	string
action_result.summary.total	numeric
summary.total_objects	numeric
summary.total_objects_successful	numeric

Create Custom Objects

FIELD	DETAILS
Name	create_custom_objects
Type	Generic
Description	Creates custom objects in ThreatQ

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE
object_list	required	A comma-separated or line-separated list of custom object values	string
object_type	required	The object type of the specified list values	string

Output

DATA PATH	TYPE
action_result.parameter.object_list	string
action_result.parameter.object_type	string
action_result.data.*.value	string
action_result.status	string
action_result.message	string

DATA PATH	TYPE
action_result.summary.total	numeric
summary.total_objects	numeric
summary.total_objects_successful	numeric

Add Attribute

FIELD	DETAILS
Name	add_attribute
Type	Generic
Description	Adds an attribute to a list of custom objects

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE
object_list	required	A comma-separated or line-separated list of object values	string
object_type	required	The object type of the specified list values	string
attribute_name	required	The name of the attribute in ThreatQ	string
attribute_value	required	The value fo the attribute in ThreatQ	string

Output

DATA PATH	TYPE
action_result.parameter.attribute_name	string
action_result.parameter.attribute_value	string
action_result.parameter.object_list	string

DATA PATH	TYPE
action_result.parameter.object_type	string
action_result.data.*.name	string
action_result.data.*.title	string
action_result.data.*.value	string
action_result.status	string
action_result.message	string
action_result.summary.total	numeric
summary.total_objects	numeric
summary.total_objects_successful	numeric

Set Indicator Status

FIELD	DETAILS
Name	set_indicator_status
Type	Generic
Description	Sets the status of an indicator in ThreatQ
Formatting	See the Formatting an Indicator List section.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
indicator_list	required	A comma-separated or line-separated list of indicators and indicator type (optional) name/value pairs (e.g.: IP Address: 1.1.1.1)	string	`domain` `ip` `email` `url` `hash` `sha256` `string` `file name` `file path` `host name` `md5` `process name` `sha1` `user name`
indicator_status	required	The status to give to the list of indicators	string	

Output

DATA PATH	TYPE	CONTAINS
action_result.parameter.indicator_list	string	`domain` `ip` `email` `url` `hash` `sha256` `string` `file name` `file path` `host name` `md5` `process name` `sha1` `user name`

DATA PATH	TYPE	CONTAINS
action_result.parameter.indicator_status	string	
action_result.data.*.value	string	
action_result.status	string	
action_result.message	string	
action_result.summary.total	numeric	
summary.total_objects	numeric	
summary.total_objects_successful	numeric	

Get Related Objects

FIELD	DETAILS
Name	get_related_objects
Type	investigate
Description	Query ThreatQ for an object's relationships

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE
object_list	required	A comma-separated or line-separated list of custom object values	string
object_type	required	The object type of the specified list values	string
related_object_type	required	The object type of the relationships you want to find	string

Output

DATA PATH	TYPE
action_result.parameter.object_list	string
action_result.parameter.object_type	string
action_result.parameter.related_object_type	string
action_result.data.*.attributes	string

DATA PATH	TYPE
action_result.data.*.name	string
action_result.data.*.score	numeric
action_result.data.*.sources.*.name	string
action_result.data.*.status.name	string
action_result.data.*.title	string
action_result.data.*.type.name	string
action_result.data.*.value	string
action_result.status	string
action_result.message	string
action_result.summary.total	numeric
summary.total_objects	numeric
summary.total_objects_successful	numeric

Create Signature

FIELD	DETAILS
Name	create_signature
Type	Generic
Description	Creates a signature within ThreatQ.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE
signature_name	required	The name for the signature uploaded to ThreatQ.	string
signature_value	required	The value for the signature uploaded to ThreatQ.	string
signature_type	required	The type for the signature uploaded to ThreatQ. Options include: Bro, Custom, Cybox, OpenIOC, Regex, Snort, STIX Indicator Pattern, YARA.	string
signature status	required	The status for the signature uploaded to ThreatQ. Options include: Active, Expired, Inactive, Non-malicious, Review, Whitelisted.	String

Output

DATA PATH	TYPE
action_result.parameter.signature_name	string
action_result.parameter.signature_value	string

DATA PATH	TYPE
action_result.parameter.signature_type	string
action_result.parameter.signature_status	string
action_result.data	string
action_result.status	string
action_result.message	string
action_result.summary	string
summary.total_objects	numeric
summary.total_objects_successful	numeric

Add Tag

FIELD	DETAILS
Name	add_tag
Type	Generic
Description	Adds tags to objects in ThreatQ.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE
object_list	required	A comma-separated or line-separated list of object values	string
object_type	required	The object type of the specified list values	string
tag	required	Add a tag to an object.	string

Output

DATA PATH	TYPE
action_result.parameter.tag	string
action_result.parameter.object_list	string
action_result.parameter.object_type	string
action_result.data.*.name	string
action_result.data.*.title	string
action_result.data.*.value	string
action_result.status	string
action_result.message	string
action_result.summary.total	numeric
summary.total_objects	numeric

DATA PATH	TYPE
summary.total_objects_successful	numeric

Add Comment

FIELD	DETAILS
Name	add_comment
Type	Generic
Description	Adds a comment to objects in ThreatQ.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE
object_list	required	A comma-separated or line-separated list of object values.	string
object_type	required	The object type of the specified list values.	string
comment	required	The comment to add to the objects.	string

Output

DATA PATH	TYPE
action_result.parameter.comment	string
action_result.parameter.object_list	string

DATA PATH	TYPE
action_result.parameter.object_type	string
action_result.data.*.name	string
action_result.data.*.title	string
action_result.data.*.value	string
action_result.status	string
action_result.message	string
action_result.summary.total	numeric
summary.total_objects	numeric
summary.total_objects_successful	numeric

Additional App Instructions

The following section contains information on formatting indicator lists and upgrading app versions.

Formatting an Indicator List

You can pass a list of indicators to an action using several different methods. While the methods for parsing may differ slightly, the outcomes will be similar.

Method 1

If only values are specified, the integration will attempt to "detect" the indicator types and upload the known values (i.e. `1.1.1.1, badurl.com`). The following indicator types are supported by this method:

- MD5
- SHA-1
- SHA-256
- SHA-384
- SHA-512
- CIDR Block
- URL
- FQDN
- Email Address
- IP Address
- CVE
- Filename
- File Path

Method 2

You can specify indicator types by separating the type and value by a `:` or `=` character (i.e. `IP Address: 1.1.1.1, FQDN: badurl.com`).

The entries are not case sensitive. You must use the same string type and spacing used by ThreatQ. **Example**: ThreatQ uses the following spacing **IP Address,** so using **IPAddress** in your entry will not work.

Method 3

You can pass the function a list of dictionaries. Each entry requires the following:

- **type**

- **value**
- one of following:
  - **object_name**
  - **object_type**
  - **object_code**
  - **collection**
  - **api_name**

List Example

```
[
    {
        "type": "IP Address",
        "value": "1.1.1.1",
        "object_type": "indicators"
    },
    {
        "type": "FQDN",
        "value": "badurl.com",
        "object_type": "indicators"
    }
]
```

The entries are not case sensitive. You must use the same string type and spacing used by ThreatQ. **Example**: ThreatQ uses the following spacing **IP Address,** so using **IPAddress** in your entry will not work.

Upgrading from 1x to 2.x

While many of the actions in v2.x of the Splunk SOAR App look very similar to the v1.x App, they operate very differently. It is recommended that you recreate and reconfigure all of the ThreatQ App actions. Review the App Actions chapter for configuration information.

Known Issues / Limitations

- Upgrading Versions - While many of the actions in v2.x of the Splunk SOAR App look very similar to the v1.x App, they operate very differently. It is recommended that you recreate and reconfigure all of the ThreatQ App actions. Review the App Actions chapter for configuration information.

Change Log

- **Version 2.3.2**
  - Added improved parsing for when indicators are sent on multiple lines using separators between the type and the value.
- **Version 2.3.1**
  - Added improved parsing and support for other input formats for `object_list` parameters.
  - The `object_list` parameter can now take ThreatQ IDs (line-separated, comma-separated, JSON List, or JSON Dict).
  - The `object_list` parameter now provides better support of Event object types.
  - Added improved IOC parser.
  - Fixed an issue that occurred when adding Attributes to Events.
  - Added new **Add Tag** action.
  - Added new **Add Comment** action.
  - Updated supported SOAR version.
- **Version 2.2.0**
  - Added new action: **Create Signature**.
  - Updated the Apps chapter.
    - Updated the name of **Create Spearphish** action to **Upload Spearphish**.
- **Version 2.1.0**
  - Fixed an issue where FQDN indicators were created when parsing a URL that did not have a URL pathway.
- **Version 2.0.3**
  - The app has been renamed to Splunk SOAR App for ThreatQ (previously known as Phantom App).
  - Performed backend code updates to provide better input support, error handling, and overall app stability.
  - Replaced all "reputation" actions with an all-in-one query action.
  - Added actions to interact with custom objects.
  - All response views now share the same template, including tables for attributes and related objects (including custom objects).
  - Response data is now better formatted to be used within Phantom playbooks to make better decisions.
  - Querying an indicator will query *all* information about that indicator, including attributes, score, status, and relationships. That information is then made accessible within the conditions block in order to make a decision.
- **Version 1.3.0**
  - Indicator lookup now does an "approximate" lookup so we can find "similar" results instead of exact matches

    

    This allows subdomains and full URLs to be returns when searching for just the host domain.

  - Added action to start an investigation from a Phantom Playbook
  - Added action to create a task from a Phantom Playbook
  - Added action to upload a spearphish email from a Phantom Playbook
  - All new actions will create relationships in ThreatQ
  - Fixed a bug where indicator score would be > 0
  - Fixed a bug where related indicators would not be shown
- **Version 1.2.0**
  - Various bug fixes.
- **Version 1.0.0**
  - Initial release