ThreatQuotient

ThreatQ ACE Operation

Version 1.1.2

February 25, 2025

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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.1.2
Compatible with ThreatQ Versions	>= 5.22.0
Support Tier	ThreatQ Supported

Introduction

The ThreatQ ACE operation utilizes the ThreatQ ACE library for parsing unstructured text for contextual intelligence such as IOCs, malware, adversaries, and tags.

The operation provides the following action:

- **Parse** - parses a selected object's unstructured description text for contextualization.

The operation is compatible with the following system objects:

- Adversaries
- Assets
- Campaigns
- Events
- Files
- Incidents
- Malware
- Reports
- Custom Objects
  - Cluster
  - Compromised Account
  - Compromised Asset
  - Compromised Card
  - Hunt Mission
  - IMEI
  - Money Mule
  - Malware Analysis
  - Monitoring
  - Organization
  - Persona
  - RFI
  - Suspected Incident
  - Threat Assessment

> The custom objects listed above are supported but are not required to install and run the operation. See the Installing Custom Objects section for details on how to install a custom object.

Installation

> The ThreatQ Marketplace download for this operation contains the operation .whl file and custom object files. The custom objects are not required to install the operation. To install the operation, extract the .whl file from the downloaded zip file and proceed with the standard operation installation process.

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 zip file.
3. Extract the zip's contents.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the operation .whl file using one of the following methods:
   - Drag and drop the .whl file into the dialog box
   - Select **Click to Browse** to locate the .whl 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. Review any additional settings, make any changes if needed, and click on **Save**.
5. 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
Parse	Parses the given object for context.	Adversary, Campaign, Incident, Event, File, Malware, Report	N/A

Parse

The Parse action parses the selected object's unstructured description text for contextualization.

Parse Parameters

The Parse action provides the following configuration parameters:

PARAMETER	DESCRIPTION
Dry Run	Disable this option to have the operation automatically upload the parsed context to the ThreatQ platform.
Select Parsers	Select which parsers to use in extract data from the current object. Options include: • Indicators (default) • Vulnerabilities • Attributes • Tags • Malware • Adversaries • Attack Patterns
Parsed IOC Types	Select which IOCs types to parse for with the operation. Options include: • MD5 (default) • SHA-1 (default) • SHA-256 (default) • SHA-384 • CIDR Block (default) • URL (default) • FQDN (default) • Email Address • IP Address (default) • Filename • File Path • CVE
Default IOC Status	Select the default status of IOCs that are automatically ingested into the platform. This option only applies when you are have disabled the **Dry Run** option.

Configuration Parameters

- [x] Dry Run

  If disabled, this action will automatically upload the parsed context to ThreatQ.

Select Parsers

Select which parsers to use to extract data from the current object

- [x] Indicators
- [ ] Vulnerabilities
- [ ] Attributes
- [ ] Tags
- [ ] Malware
- [ ] Adversaries
- [ ] Attack Patterns

Parsed IOC Types

Select which IOC types to parse for

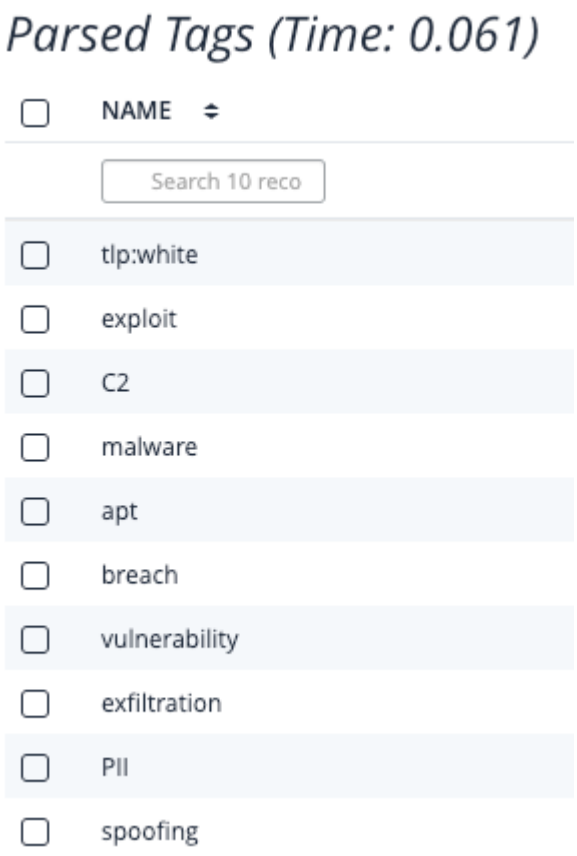
- [x] MD5
- [x] SHA-1
- [x] SHA-256
- [ ] SHA-384
- [x] CIDR Block
- [x] URL
- [x] FQDN
- [ ] Email Address
- [x] IP Address
- [ ] Filename
- [ ] File Path
- [ ] CVE

Default IOC Status

Review

Select the default status for IOCs automatically ingested into ThreatQ (when dry run is disabled)

Example - Parsed Tags



Example - Parsed Attributes

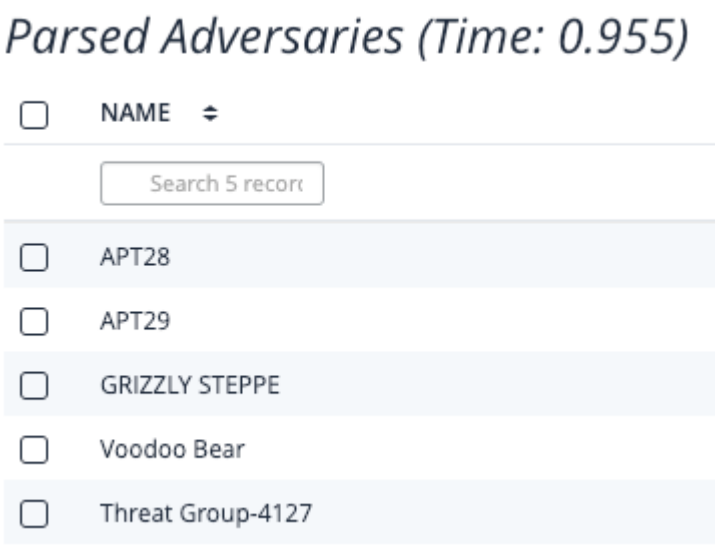
Parsed Attributes (Time: 0.239)

NAME	VALUE
Search 40 reco	Search 40 reco
Affected Operating System	Windows
Affected Operating System	Linux
Detection	Trojan.PHP.Shell.JB
Detection	Trojan.Script.Crypt.dsonvo
Detection	Trojan.PHP.Crypt
Detection	Trojan.PHP.Shell.LV
Detection	Trojan.Win32.Malware
Detection	W32/Trojan3.XZP
Detection	Trojan.Generic.20173242
Detection	Trojan.Cozer.B
Detection	Win.Trojan.OnionDuke-5486244-0
Detection	Trojan.Win32.MiniDuke.ekecow
Detection	W32/Trojan3.XZO
Detection	Trojan.Generic.20173160
Detection	Win.Trojan.OnionDuke-5486245-0
Detection	Trojan.Win32.AD.ekdqnf
Detection	Trojan.Win32.Agent
Detection	W32/Dridex.HX
Detection	Win.Trojan.Agent-5486255-0
Detection	Trojan.Rtf.Stealer.efqzyl
Detection	Trojan.Win32.Zlader
Detection	Trojan.Win32.Crypt5.AYWX
Detection	Trojan.Fareit.Win32.14782
Detection	Win.Trojan.Agent-5486256-0
Detection	Trojan/Win32.Fareit

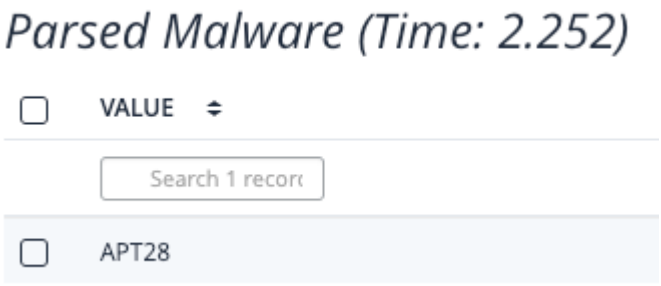
‹ 1 2 › | Rows per page 25

Add Selected Attributes

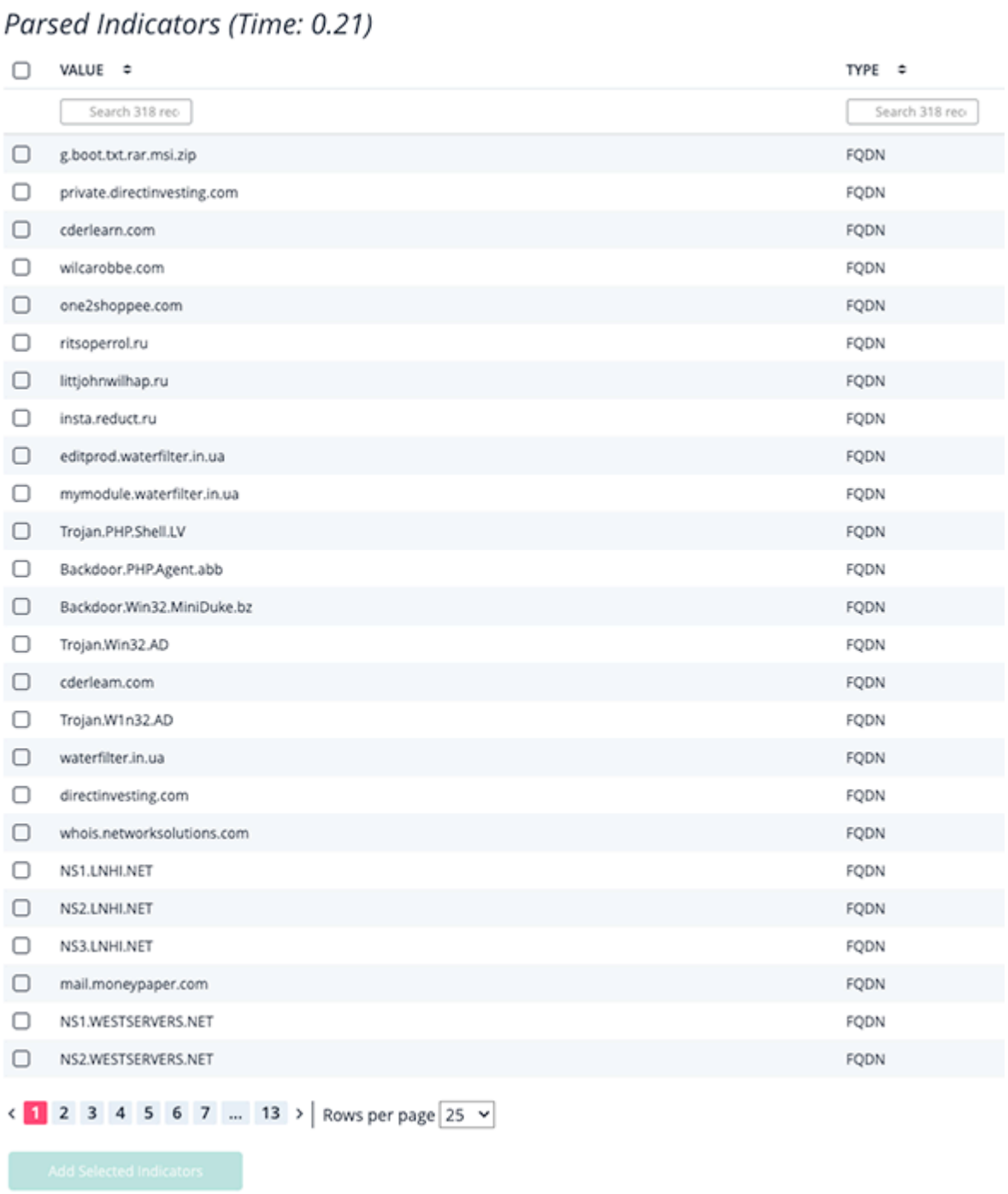
Example - Parsed Adversaries



Example - Parsed Malware

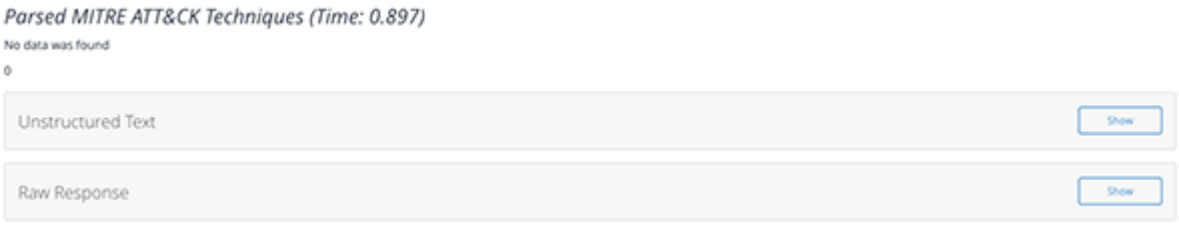


Example - Parsed Indicators



Example - Parsed Vulnerabilities

Example - Parsed MITRE ATT&CK Techniques



Installing Optional Custom Objects

The ThreatQ ACE operation does not require the installation of any custom objects in order be installed on your ThreatQ instance. The operation does support the following optional custom objects:

- Cluster
- Compromised Account
- Compromised Asset
- Compromised Card
- Hunt Mission
- IMEI
- Money Mule
- Malware Analysis
- Monitoring
- Organization
- Persona
- RFI
- Suspected Incident
- Threat Assessment

The custom objects listed above are included in the integration zip file downloaded from the ThreatQ Marketplace. Use the following steps to install one of the above optional custom objects:

> When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

ThreatQ V6 Steps

Use the following steps to install the custom object in ThreatQ v6:

1. Download the integration bundle from the ThreatQ Marketplace.
2. Unzip the bundle and locate the custom object files.

   > The custom object files will typically consist of a JSON definition file, install.sh script, and a images folder containing the svg icons.

3. SSH into your ThreatQ instance.
4. Navigate to the following location:

   ```
   cd /var/lib/threatq/misc/
   ```

5. Upload the custom object files, including the images folder.

   The directory structure should be as the following:

   - misc
     - install.sh
     - <custom_object_name>.json
     - images (directory)
       - <custom_object_name>.svg
6. Run the following command:

```
kubectl exec -it deployment/api-schedule-run -n threatq -- sh /var/
lib/threatq/misc/install.sh /var/lib/threatq/misc
```

> The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

7. Delete the install.sh, definition json file, and images directory from the `misc` directory after the object has been installed as these files are no longer needed.

ThreatQ v5 Steps

1. Download the integration zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

   ```
   cd /tmp/
   ```

4. Create a new directory:

   ```
   mkdir ace_op
   ```

5. Upload the **<object_file_name>.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the ace_op directory.

   ```
   mkdir images
   ```

7. Upload the <object_file_name>.svg.
8. Navigate to the **/tmp/ace_op**.

   The directory should resemble the following:

   - tmp
     - **ace_op**
       - **<object_file_name>.json**
       - **install.sh**
       - **images**
         - **<object_file_name>.svg**

9. Run the following command to ensure that you have the proper permissions to install the custom object:

```
chmod +x install.sh
```

10. Run the following command:

```
sudo ./install.sh
```

> You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
rm -rf ace_op
```

Known Issues / Limitations

- The ThreatQ ACE Operation may encounter issues when parsing data from PDFs due to formatting included in these files. For instance, a file path may be truncated due to PDF wrapping which splits the path into two lines.

Change Log

- **Version 1.1.2**
  - Added the ability to parse CVEs as either indicators or vulnerabilities.
  - Added a new option to the **Parsed IOC Types** parse action parameter: `CVE`.
- **Version 1.1.1**
  - Updated the operation to access the updated ACE libraries in ThreatQ version 5.22.0.
  - The operation will now ingest multiple descriptions for an object (if applicable).
  - Updated the operation for improved parsing of hashes from files.
  - Updated minimum ThreatQ version to 5.22.0.
- **Version 1.1.0**
  - Added support for the Asset object type and the following custom objects: IMEI, Organization, Compromised Account, Compromised Card, Money Mule, Cluster, Compromised Asset, Hunt Mission, Malware Analysis, Monitoring, Persona, RFI, Suspected Incident, Threat Assessment.
- **Version 1.0.1**
  - The ACE library dependency is now embedded with the operation and no requires manual installation.
  - Updated the minimum ThreatQ version to 5.15.0
- **Version 1.0.0**
  - Initial release