ThreatQuotient

Palo Alto AutoFocus Operation Guide

Version 1.0.0

January 03, 2022

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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.

Versioning

- Current integration version: `1.0.0`
- Compatible with ThreatQ versions >= `4.40.0`

Introduction

The Palo Alto AutoFocus operation enriches ThreatQ indicators with Palo Alto AutoFocus data in the form of attributes and related indicators.

The operation provides the following action:

- **Enrich Indicator** - adds data from Palo Alto AutoFocus as attributes or related indicators to the indicator.

See the Actions chapter for more details on the action listed above.

The operation is compatible with the following indicator sub-types:

- Email Address
- File Name
- FQDN
- IP Address
- IPv6 Address
- SHA-256
- 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 feed 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.
6. 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).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Token	Your Palo Alto AutoFocus API Token.
Response Size	The number of results the user wishes to see. The default setting is 50. **The query can return thousands of results. In order to save time and space, ThreatQuotient recommends limiting the number of results using this parameter.**
Time Range	An optional time range so as to only see query results that were created between the set range. Options include: ◦ Today ◦ Yesterday ◦ Last week ◦ Last 6 months

PARAMETER	DESCRIPTION
	The bigger the time range is, the longer it may take to load the results. If none is selected, it will search during a time range of the last year.

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the operation.

Actions

The Palo Alto AutoFocus operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Enrich Indicator	Add data from AutoFocus as attributes or related indicators to the indicator	Indicators	IP Address, IPv6 Address, FQDN, SHA-256, URL, Email Address, Filename

Enrich Indicator

The Enrich Indicator action adds data from Palo Alto AutoFocus as attributes or related indicators to the indicator.

`POST https://autofocus.paloaltonetworks.com/api/v1.0/samples/results/<af_cookie>`

See below a sample response for a URL.


```
{
  'af_complete_percentage': 100,
  'tags': {
    'unit42.android_sudo': {
      'tag_name': 'AndroidSudo',
      'up_votes': 2,
      'lasthit': 1620041071000,
      'tag_definition_id': 39972,
      'source': 'Unit 42',
      'tag_groups': [
        {
          'tag_group_name': 'MobileMalware',
          'description': 'Mobile malware is malicious software that targets mobile phones by causing loss or leakage
of confidential information. This generic group will encompass all mobile malware, such as Android malware. '
        }
      ],
      'tag_definition_scope_id': 4,
      'description': 'The tag indicates when an Android sample try to execute the "su" command to get root privilege,
commonly used to root the phone or otherwise execute code at with root privileges.',
      'customer_industry': 'High Tech',
      'public_tag_name': 'Unit42.AndroidSudo',
      'tag_definition_status_id': 1,
      'support_id': 1,
      'count': 15571072,
      'customer_name': 'Palo Alto Networks Unit42',
      'tag_class_id': 5
    }
  },
  'af_in_progress': False,
  'af_message': 'success',
  'tag_groups': {
    'mobile_malware': {
      'tag_group_name': 'MobileMalware',
      'description': 'Mobile malware is malicious software that targets mobile phones by causing loss or leakage of
confidential information. This generic group will encompass all mobile malware, such as Android malware. '
    }
  },
  'af_indices': 0,
  'bucket_info': {
    'daily_points': 5000,
    'minute_points': 200,
    'minute_points_remaining': 199,
    'daily_points_remaining': 4743,
    'daily_bucket_start': '2021-12-27 14:25:34',
    'minute_bucket_start': '2021-12-27 17:24:41'
  },
  'af_first_result_af_took': 0,
```

```
 'took': 0,
 'total': 453,
 'af_cookie': 'b2684f3b-6739-11ec-8469-b9c443efd47e',
 'hits': [
   {
     'sort': [],
     '_id': 'ccaa59639974ab56041e45a3a0f86276775a0ef930f938a0b2e93197e7555f8c',
     'visible': True,
     '_source': {
       'tag': ['Unit42.AndroidSudo'],
       'tags': ['35794', '39712', '47735', '66523', '39972', '66328'],
       'create_date': '2021-12-27T09:06:17',
       'source': 11,
       'sha1': 'a527a584f53a15b311c30a381ab26266fc3431df',
       'size': 36705924,
       'malware': 0,
       'sha256': 'ccaa59639974ab56041e45a3a0f86276775a0ef930f938a0b2e93197e7555f8c',
       'filetype': 'Android APK',
       'tag_groups': ['MobileMalware'],
       'filename': 'ccaa59639974ab56041e45a3a0f86276775a0ef930f938a0b2e93197e7555f8c',
       'finish_date': '2021-12-27T09:11:11',
       'app_name': 'CNN',
       'mid': 1205589785551,
       'ispublic': 1,
       'ssdeep': '786432:ice+bvCoUGE5V1fyqPgjZvCEJMYaOPz7JK:J9vaGE1fM3rhK',
       'region': 'us',
       'md5': '26409cc05edecf7b45a5373929062f06',
       'app_packagename': 'com.cnn.mobile.android.phone'
     }
   },
   {
     'sort': [],
     '_id': '329d3d8334b2092ee1dfee4b177c0aa101696331fac9094bc9516e8e499f564c',
     'visible': True,
     '_source': {
       'tag': ['Unit42.AndroidSudo'],
       'tags': ['34418', '84206', '66523', '39972', '1477', '66328'],
       'create_date': '2021-12-27T01:39:15',
       'source': 11,
       'sha1': 'bc870243b7eb469f324b84db63b6163038c2079e',
       'size': 72163782,
       'malware': 0,
       'sha256': '329d3d8334b2092ee1dfee4b177c0aa101696331fac9094bc9516e8e499f564c',
       'filetype': 'Android APK',
       'tag_groups': ['MobileMalware'],
       'filename': '329d3d8334b2092ee1dfee4b177c0aa101696331fac9094bc9516e8e499f564c',
       'finish_date': '2021-12-27T01:43:26',
       'app_name': 'Samsung Internet',
       'mid': 5005614916861,
       'ispublic': 1,
       'ssdeep': '786432:1t7CttFD1JA+EAjmgO9pcroBmapP/S4+xdHt5U:1JkXWTOgY/U',
       'region': 'us',
       'md5': '9db590162b8a52d9d4c74217a73bc0b8',
       'app_packagename': 'com.sec.android.app.sbrowser'
     }
   },
   ...
 ]
}
```

ThreatQ provides the following default mapping for this Action:

SOURCE	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
response.hits[]._source.tag[]	Attribute	Tag	Unit42.AndroidSudo
response.hits[]._source.create_date	Attribute	Create Date	2021-12-27T09:06:17
response.hits[]._source.sha1	Indicator	SHA-1	a527a584f53a15b311c30a381ab26266fc3431df
response.hits[]._source.size	Attribute	File Size	36705924
response.hits[]._source.malware	Attribute	Malware	0
response.hits[]._source.sha256	Indicator	SHA-256	ccaa59639974ab56041e45a3a0f86276775a0ef930f938a0b2e93197e7555f8c
response.hits[]._source.filetype	Attribute	File Type	Android APK
response.hits[]._source.tag_groups	Attribute	Tag Groups	MobileMalware
response.hits[]._source.finish_date	Attribute	Finish Date	2021-12-27T09:11:11
response.hits[]._source.app_name	Attribute	App Name	CNN
response.hits[]._source.mid	Attribute	MID	1205589785551
response.hits[]._source.ispublic	Attribute	isPublic	1
response.hits[]._source.ssdeep	Attribute	ssdeep	786432:ice+bvCoUGE5V1fyqPgjZvCEJMYaOPz7JK:J9vaGE1fM3rhK
response.hits[]._source.region	Attribute	Region	US
response.hits[]._source.md5	Indicator	MD5	26409cc05edecf7b45a5373929062f06
response.hits[]._source.app_packagename	Attribute	App Packagename	com.cnn.mobile.android.phone

Change Log

- **Version 1.0.0**
  - Initial Release