ThreatQuotient

ArcSight Exports CDF Guide

Version 1.0.0 rev-a

February 07, 2023

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	1.0.0
Compatible with ThreatQ Versions	>= 4.35.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/arcsight-exports-cdf

Introduction

The ArcSight Exports CDF for ThreatQuotient enables ThreatQ to automatically export suspicious or malicious IOCs to ArcSight Active Lists. Rules can then be created to generate cases based on matches on the threat intelligence.

The integration provides the following feeds:

- **ArcSight MITRE ATT&CK Export (Feed)** - exports MITRE ATT&CK Attack Patterns from ThreatQ to the MITRE ATT&CK Active List within ArcSight. This will ensure that your MITRE ATT&CK information within ArcSight is always up-to-date with the latest MITRE changes.
- **ArcSight Suspicious Addresses Export** - exports IP Addresses from ThreatQ to the Suspicious Addresses Active List within ArcSight.
- **ArcSight Suspicious Domain Export** - exports FQDNs from ThreatQ to the Suspicious Domain Active List within ArcSight.
- **ArcSight Suspicious URL Export** - exports URLs from ThreatQ to the Suspicious URL Active List within ArcSight.
- **ArcSight Suspicious Hash Export** - exports MD5s, SHA-1s, SHA-256s, SHA-512s, and Fuzzy Hashes from ThreatQ to the Suspicious Hash Active List within ArcSight.
- **ArcSight Suspicious Email Export** - exports Email Addresses from ThreatQ to the Suspicious Email Active List within ArcSight.

External data is not ingested into ThreatQ when this feed finishes its run. Instead, a single report will be created, detailing the successfulness of the feed-run. An analyst can use this data to curate their data better, or be alerted when there are issues with the export.

Prerequisites

The ArcSight Exports CDF integration requires that you create the following lists in ArcSight ESM:

- Suspicious Address List
- Suspicious Domain List
- Suspicious Email List
- Suspicious Hash List
- Suspicious URL List

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 feed 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 feed and will require user confirmation before proceeding.
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

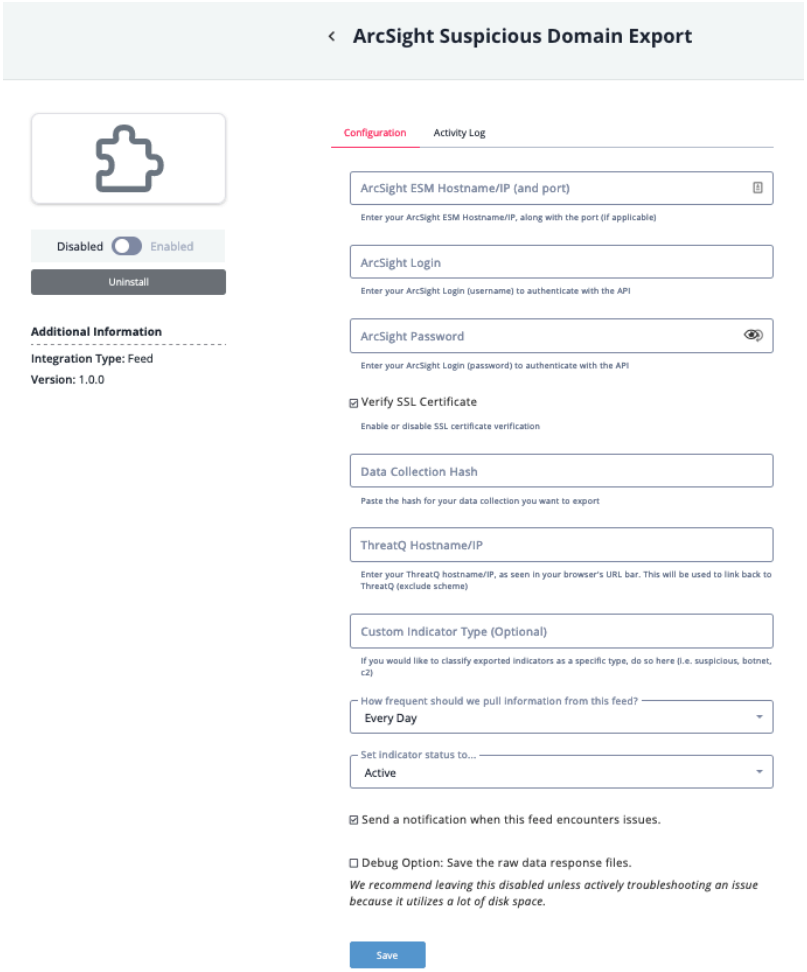
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
ArcSight ESM Hostname/IP (and port)	Enter your ArcSight ESM Hostname/IP, along with the port (if applicable).
ArcSight Login	Enter your ArcSight Login (username) to authenticate with the API.
ArcSight Password	Enter your ArcSight password, associated with the account above, to authenticate with the API.
Verify SSL Certificate	Enable or disable SSL certificate verification.
ThreatQ Hostname/IP	Enter your ThreatQ hostname/IP, as seen in your browser's URL bar. This will be used to link back to ThreatQ (exclude scheme).
Custom Indicator Type (Optional)	Optional - classify exported indicators as a specific type. **Example:** suspicious, botnet, c2

PARAMETER	DESCRIPTION

> This parameter is not available for the ArcSight MITRE ATT&CK EXport feed



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.

ThreatQ Mapping

Due to the repetitiveness of the feeds within this CDF, the feeds share a lot of the same configurations and mappings. External data is not ingested into ThreatQ when this a run completes. Instead, a single report will be created, detailing the successfulness of the feed-run. An analyst can use this data to curate their data better, or be alerted when there are issues with the export.

All feeds use the same logic to export data out of ThreatQ.

The flow of each feed goes as follows:

1. Fetch data from a ThreatQ data collection
2. Authenticate with ArcSight (Feed: `Get API Token`)
3. If a custom indicator type is specific (in the user fields), create the indicator type in ArcSight (Feeds: `Get List ID by Name`, `Post to Active List`)
4. Get the ArcSight Active List by name (Feed: `Get List ID by Name`)
5. Build the POST payload for the ArcSight API
6. POST the payload to the ArcSight API (Feed: `Post to Active List`)

ThreatQ provides the following default mapping for this feed. Anytime you see `{{active_list}}`, refer to the details of the specific feed.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Value	Report	N/A	N/A	ArcSight `{{active_list}}` Export Report (`{{ run_meta.until or 'First Run' }}`)	N/A
N/A	Attribute	Active List	N/A	N/A	`{{active_list}}` List	This is hard-coded, per-feed
N/A	Attribute	Exported Indicator Type	N/A	N/A	N/A	This is hard-coded, per-feed
`run_vars.export_count`	Attribute	Exported Objects	N/A	N/A	10000	A run-var is used to track the export count
`run_meta.until`	Attribute	Exported Date	N/A	N/A	N/A	Tracks when the export ran

ArcSight MITRE ATT&CK Export (Feed)

The ArcSight Suspicious MITRE ATT&CK Export feed will will export MITRE ATT&CK Attack Patterns from ThreatQ to the MITRE ATT&CK Active List within ArcSight. This will ensure that your MITRE ATT&CK information within ArcSight is always up-to-date with the latest MITRE changes.

The following is an example payload that ArcSight is expecting when adding to the Active List:

```
{
  "fields": [
    "MitreID",
    "Tactic",
    "MitreName"
  ],
  "entries": [
    {
      "fields": [
        "T1001",
        "Command and Control",
        "Data Obfuscation"
      ],
      "fields": [
        "T1001.1001",
        "Command and Control",
        "Junk Data"
      ]
    }
  ]
}
```

ArcSight Suspicious Addresses Export (Feed)

The ArcSight Suspicious Address feed will will export IP Addresses from ThreatQ to the Suspicious Addresses Active List within ArcSight.

The following is an example payload that ArcSight is expecting when adding to the Active List:


```
{
    "fields": [
        "address",
        "indicatorType",
        "firstDetectTime",
        "lastDetectTime",
        "port",
        "sightings",
        "threatLevel",
        "actors",
        "campaign",
        "sector",
        "mitreAttack",
        "description",
        "reference",
        "mitigation",
        "extraInfo"
    ],
    "entries": [
        {
            "fields": [
                "49.234.67.251",
                "malware",
                "7 May 2021 05:54:28 EST",
                "7 May 2021 05:54:28 EST",
                0,
                0,
                7,
                "CozyBear",
                "",
                "",
                "",
                null,
                "https://instance.threatq.online/indicators/<id>/details",
                "",
                ""
            ]
        }
    ]
}
```

ArcSight Suspicious Domain Export (Feed)

The ArcSight Suspicious Domain Export feed exports FQDNs from ThreatQ to the Suspicious Domain Active List within ArcSight.

The following is an example payload that ArcSight is expecting when adding to the Active List:


```
{
    "fields": [
        "domain",
        "indicatorType",
        "firstDetectTime",
        "lastDetectTime",
        "port",
        "sightings",
        "threatLevel",
        "actors",
        "campaign",
        "sector",
        "mitreAttack",
        "description",
        "reference",
        "mitigation",
        "extraInfo"
    ],
    "entries": [
        {
            "fields": [
                "somebaddomain.com",
                "malware",
                "7 May 2021 05:54:28 EST",
                "7 May 2021 05:54:28 EST",
                0,
                0,
                7,
                "CozyBear",
                "",
                "",
                "",
                null,
                "https://instance.threatq.online/indicators/<id>/details",
                "",
                ""
            ]
        }
    ]
}
```

ArcSight Suspicious URL Export (Feed)

The ArcSight Suspicious URL Export feed will will export URLs from ThreatQ to the Suspicious URL Active List within ArcSight.

The following is an example payload that ArcSight is expecting when adding to the Active List:

```
{
    "fields": [
        "url",
        "indicatorType",
        "firstDetectTime",
        "lastDetectTime",
        "port",
        "sightings",
        "threatLevel",
        "actors",
        "campaign",
        "sector",
        "mitreAttack",
        "description",
        "reference",
        "mitigation",
        "extraInfo"
    ],
    "entries": [
        {
            "fields": [
                "http://leakforums.sx/attachments/payload.exe",
                "malware",
                "7 May 2021 05:54:28 EST",
                "7 May 2021 05:54:28 EST",
                0,
                0,
                7,
                "CozyBear",
                "",
                "",
                "",
                null,
                "https://instance.threatq.online/indicators/<id>/details",
                "",
                ""
            ]
        }
    ]
}
```

ArcSight Suspicious Hash Export (Feed)

The ArcSight Suspicious Hash Export feed will will export MD5s, SHA-1s, SHA-256s, SHA-512s, and Fuzzy Hashes from ThreatQ to the Suspicious Hash Active List within ArcSight.

The following is an example payload that ArcSight is expecting when adding to the Active List:


```
{
    "fields": [
        "hash",
        "indicatorType",
        "firstDetectTime",
        "lastDetectTime",
        "port",
        "sightings",
        "threatLevel",
        "actors",
        "campaign",
        "sector",
        "mitreAttack",
        "description",
        "reference",
        "mitigation",
        "extraInfo"
    ],
    "entries": [
        {
            "fields": [
                "0024c971e6c4947c6e0e7522a3203baf79610d452e4028ca8cb35de7bf17777a",
                "malware",
                "7 May 2021 05:54:28 EST",
                "7 May 2021 05:54:28 EST",
                0,
                0,
                7,
                "CozyBear",
                "",
                "",
                "",
                null,
                "https://instance.threatq.online/indicators/<id>/details",
                "",
                ""
            ]
        }
    ]
}
```

ArcSight Suspicious Email Export (Feed)

The ArcSight Suspicious Email Export feed will will export Email Addresses from ThreatQ to the Suspicious Email Active List within ArcSight.

The following is an example payload that ArcSight is expecting when adding to the Active List:

```
{
    "fields": [
        "email",
        "indicatorType",
        "firstDetectTime",
        "lastDetectTime",
        "port",
        "sightings",
        "threatLevel",
        "actors",
        "campaign",
        "sector",
        "mitreAttack",
        "description",
        "reference",
        "mitigation",
        "extraInfo"
    ],
    "entries": [
        {
            "fields": [
                "steve.jobs@timapple.com",
                "malware",
                "7 May 2021 05:54:28 EST",
                "7 May 2021 05:54:28 EST",
                0,
                0,
                7,
                "CozyBear",
                "",
                "",
                "",
                null,
                "https://instance.threatq.online/indicators/<id>/details",
                "",
                ""
            ]
        }
    ]
}
```

Get API Token (Supplemental)

The Get API Token endpoint will authenticate with ArcSight, returning a token to use in subsequent requests.

```
POST https://{{host}}/www/core-service/rest/LoginService/login
```

Sample Response:

```
{
  "log.loginResponse": {
    "log.return": "MjGWac8irk9n4WEc_qX112q7z-tgsPCol3ulagI57UY."
  }
}
```

Get List ID by Name (Supplemental)

The Get List ID by Name endpoint return an Active List ID, given the friendly name

`GET https://{{host}}/detect-api/rest/v1/activelists/findAll/{{list_name}}`

Sample Response:


```
[
  {
    "resourceId": "HSmvsV2sBABC7uprfdqI7yA==",
    "name": "Suspicious Domain List",
    "description": "This active list contains suspicious domains collected from MISP Circl.",
    "reference": {
      "id": "HSmvsV2sBABC7uprfdqI7yA==",
      "uri": "/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain List",
      "referenceString": "<Resource URI=\"/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Suspicious Domain List\" ID=\"HSmvsV2sBABC7uprfdqI7yA==\"/>",
      "managerID": "92EpNXgBABCAYBuppdOPcA==",
      "referenceType": 24,
      "isModifiable": true,
      "referenceName": "ActiveList"
    },
    "type": 24,
    "typeName": "ActiveList",
    "isAdditionalLoaded": false,
    "modificationCount": 1,
    "createdTimestamp": 1615799482035,
    "modifiedTimestamp": 1615799519710,
    "versionID": "AAAADpFCfjFrckkZ",
    "contentVersionID": "AAAADpFCda1rckka",
    "disabled": false,
    "inactive": false,
    "deprecated": false,
    "localID": 103079215175,
    "state": 2,
    "creatorName": "admin",
    "modifierName": "admin",
    "optimizeData": false,
    "capacity": 500000,
    "entryTimeToLive": 2592000000,
    "multiMap": false,
    "partialCache": false,
    "timePartitioned": false,
    "activeListType": "FIELD_BASED",
    "caseSensitiveType": "CASE_SENSITIVE",
    "initialized": true,
    "uri": "/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain List",
    "inCache": true,
    "attributeInitializationInProgress": false,
    "signature": {
      "id": "HSmvsV2sBABC7uprfdqI7yA==",
      "modificationCount": 1
    },
    "displayName": "Suspicious Domain List",
    "fields": [
```

```
{
  "name": "domain",
  "type": "String",
  "key": true
},
{
  "name": "indicatorType",
  "type": "String",
  "key": false
},
{
  "name": "firstDetectTime",
  "type": "Date",
  "key": false
},
{
  "name": "lastDetectTime",
  "type": "Date",
  "key": false
},
{
  "name": "port",
  "type": "Integer",
  "key": false
},
{
  "name": "sightings",
  "type": "Integer",
  "key": false
},
{
  "name": "threatLevel",
  "type": "String",
  "key": false
},
{
  "name": "actors",
  "type": "String",
  "key": false
},
{
  "name": "campaign",
  "type": "String",
  "key": false
},
{
  "name": "sector",
  "type": "String",
  "key": false
},
{
  "name": "mitreAttack",
  "type": "String",
  "key": false
},
{
  "name": "description",
  "type": "String",
  "key": false
},
{
```

```
      "name": "reference",
      "type": "String",
      "key": false
    },
    {
      "name": "mitigation",
      "type": "String",
      "key": false
    },
    {
      "name": "extraInfo",
      "type": "String",
      "key": false
    }
  ]
 }
]
```

Post to Active List (Supplemental)

The Post to Active List endpoint will bulk-add indicators to a given Active List

```
POST https://{{host}}/detect-api/rest/v1/activelists/{{active_list_id}}/entries
```

Sample Response:

```
Status Code: 201
```

Average Feed Run

> Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

External data is not ingested into ThreatQ when this feed finishes its run. Instead, a single report will be created, detailing the successfulness of the feed-run.

METRIC	RESULT
Run Time	1 minute
Report	1
Report Attributes	4

Change Log

- **Version 1.0.0 rev-a**
  - Guide Update - Added new Prerequisites chapter
- **Version 1.0.0**
  - Initial release