

ThreatQuotient



ArcSight Case Management CDF

Version 1.0.1

February 03, 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	3
Support	4
Integration Details.....	5
Introduction	6
Prerequisites	7
Installation.....	8
Configuration	9
ThreatQ Mapping.....	11
ArcSight Case Management (Feed).....	11
Get Case (Supplemental).....	16
Get Events (Supplemental).....	19
Average Feed Run.....	27
ArcSight Case Management Feed.....	27
Known Issues / Limitations	28
Change Log	29

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 © 2025 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.

Support

This integration is designated as **Developer Supported**.

Support Email: support@ke-la.com

Support Web: <https://ke-la.com/contact-us/>

Support Phone: N/A

Integrations designated as **Developer Supported** are supported and maintained by the developer who submitted the integration to the ThreatQ Marketplace. The developer's contact information can be found on the integration's download page within the Marketplace as well as in this guide.

You are responsible for engaging directly with the developer of Developer Supported integrations/apps/add-ons to ensure proper functionality and version compatibility with the applicable ThreatQuotient Software.

If functional or compatibility issues that may arise are not resolved, you may be required to uninstall the app or add-on from their ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply for any issues caused by Developer Supported integrations/apps/add-ons.

ThreatQuotient reserves the right to remove the Developer-Supported designation of third-party apps and add-ons if the developer is not, in ThreatQuotient's determination, fulfilling reasonable obligations for support and maintenance.



Failure by the developer to update compatibility of an app or add-on within 90 days of the release of a new version of applicable ThreatQuotient Software will result in reclassification to Not Actively Supported.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.1
Compatible with ThreatQ Versions	>= 4.35.0
Support Tier	Developer Supported

Introduction

The ArcSight Case Management CDF for ThreatQuotient enables ThreatQ to automatically ingest cases, events, and indicators from ArcSight, ultimately, alerting analysts of any threats within their environment.

The integration provides the following feeds:

- **ArcSight Case Management** - fetches all case IDs within ArcSight.
- **Get Case (Supplemental)** - fetches the (almost) full details of an ArcSight case, by its' ID.
- **Get Events (Supplemental)** - fetches a list of events based on a list of event IDs.

The integration ingests the following system objects:

- Indicators
- Events
- Event Attributes

Prerequisites

You will need the following to run the integration:

- An ArcSight ESM Hostname/IP along with port.
- An ArcSight ESM username and password.

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the 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. 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).



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

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)	Your ArcSight ESM Hostname/IP, along with the port (if applicable).
ArcSight Login	Your ArcSight Login (username) to authenticate with the API.
ArcSight Password	Your ArcSight Login (password) to authenticate with the API.
Ingested Associated Events	Configure whether or not to bring the offending ArcSight Events that make up a Case.
Verify SSL Certificate	Enable or disable SSL certificate verification.

< ArcSight Case Management



☐ Disabled
 ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

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 Login (password) to authenticate with the API

☒ Ingest Associated Events
 Whether or not you want to bring the offending ArcSight Events that make up a Case

☒ Verify SSL Certificate
 Enable or disable SSL certificate verification
 Set indicator status to: Active

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

ArcSight Case Management (Feed)

The ArcSight Case Management feed fetches all case IDs within ArcSight.

! There is no way to fetch a time-fenced list of cases or their IDs. For each case ID returned by the API, the integration will need to fetch the case details using the `Get Case` supplemental feed. Once it has been verified that the case has been updated since its last run, the integration fetch the events using the `Get Events` supplemental feed. From there, the reporting data is built out into events, attributes, and indicators. The below mapping will include all mappings after all supplemental feed data has been fetched.

GET `https://{{host}}/detect-api/rest/cases/allIds`

Sample Response:

```
[
  "7ioxmngBABCbqbxc1EodmA==",
  "7vralVnkBABDl04n55EGTXw=="
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
.name	Attribute	Case Name	N/A	.createdTimestamp	ArcSight Case: Sighting of Trickbot Indicator	This is whatever the analyst makes it
.alias	Attribute	Alias	N/A	.createdTimestamp	N/A	N/A
.creator	Attribute	ArcSight Creator	N/A	.createdTimestamp	N/A	N/A
.ticketType	Attribute	Ticket Type	N/A	.createdTimestamp	INCIDENT	N/A
.stage	Attribute	Stage	N/A	.createdTimestamp	INITIAL	N/A
.frequency	Attribute	Frequency	N/A	.createdTimestamp	NEVER_OR_ONCE	N/A
.operationalImpact	Attribute	Operational Impact	N/A	.createdTimestamp	HIGH_PRIORITY_IMPACT	N/A
.securityClassification	Attribute	Security Classification	N/A	.createdTimestamp	SECRET	N/A
.consequenceSeverity	Attribute	Consequence Severity	N/A	.createdTimestamp	CRITICAL	N/A
.sensitivity	Attribute	Sensitivity	N/A	.createdTimestamp	SECRET	N/A
.associatedImpact	Attribute	Associated Impact	N/A	.createdTimestamp	INTEGRITY	N/A
.action	Attribute	Action	N/A	.createdTimestamp	BLOCK_OR_SHUTDOWN	N/A
.securityClassificationCode	Attribute	Security Classification Code	N/A	.createdTimestamp	IOESIB	N/A
.history	Attribute	History	N/A	.createdTimestamp	KNOWN_OCCURENCE	N/A
.resistance	Attribute	Resistance	N/A	.createdTimestamp	HIGH	N/A
.reportingLevel	Attribute	Reporting Level	N/A	.createdTimestamp	3	N/A
.numberOfOccurrences	Attribute	Number of Occurrences	N/A	.createdTimestamp	0	N/A
.actionsTaken	Attribute	Actions Taken	N/A	.createdTimestamp	N/A	N/A
.plannedActions	Attribute	Planned Actions	N/A	.createdTimestamp	N/A	N/A
.recommendedActions	Attribute	Recommended Actions	N/A	.createdTimestamp	N/A	N/A
.followupContact	Attribute	Follow-up Contact	N/A	.createdTimestamp	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
.conclusions	Attribute	Conclusions	N/A	.createdTimestamp	N/A	N/A
.incidentSource1	Attribute	Incident Source	N/A	.createdTimestamp	N/A	N/A
.incidentSource2	Attribute	Incident Source	N/A	.createdTimestamp	N/A	N/A
.inspectionResults	Attribute	Inspection Results	N/A	.createdTimestamp	N/A	N/A
.vulnerability	Attribute	Vulnerability	N/A	.createdTimestamp	ENVIRONMENT	N/A
.vulnerabilityType1	Attribute	Vulnerability Type	N/A	.createdTimestamp	ACCIDENTAL	N/A
.vulnerabilityType2	Attribute	Vulnerability Type	N/A	.createdTimestamp	EMI_RFI	N/A
.vulnerabilityEvidence	Attribute	Vulnerability Evidence	N/A	.createdTimestamp	N/A	N/A
.vulnerabilitySource	Attribute	Vulnerability Source	N/A	.createdTimestamp	N/A	N/A
.vulnerabilityData	Attribute	Vulnerability Data	N/A	.createdTimestamp	N/A	N/A
.attackMechanism	Attribute	Attack Mechanism	N/A	.createdTimestamp	INFORMATIONAL	N/A
.attackAgent	Attribute	Attack Agent	N/A	.createdTimestamp	OUTSIDER	N/A
.attackTarget	Attribute	Attack Target	N/A	.createdTimestamp	N/A	N/A
.attackService	Attribute	Attack Service	N/A	.createdTimestamp	N/A	N/A
.attackProtocol	Attribute	Attack Protocol	N/A	.createdTimestamp	N/A	N/A
.attackOS	Attribute	Attack OS	N/A	.createdTimestamp	N/A	N/A
.attackProgram	Attribute	Attack Program	N/A	.createdTimestamp	N/A	N/A
.attackImpact	Attribute	Attack Impact	N/A	.createdTimestamp	N/A	N/A
.disabled	Attribute	Is Disabled	Boolean -> String	.createdTimestamp	false	N/A
.inactive	Attribute	Is Inactive	Boolean -> String	.createdTimestamp	false	N/A
.deprecated	Attribute	Is Deprecated	Boolean -> String	.createdTimestamp	false	N/A
.initialized	Attribute	Is Initialized	Boolean -> String	.createdTimestamp	true	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
.detectionTime	Attribute	Detection Time	Dict -> String	.createdTime estamp	N/A	N/A
.estimatedStartTime	Attribute	Estimated Start Time	Dict -> String	.createdTime estamp	N/A	N/A
.estimatedRestoreTime	Attribute	Estimated Restore Time	Dict -> String	.createdTime estamp	N/A	N/A
.attackTime	Attribute	Attack Time	Dict -> String	.createdTime estamp	N/A	N/A
.lastOccurrenceTime	Attribute	Last Occurrence Time	Dict -> String	.createdTime estamp	N/A	N/A
.events[].type	Attribute	Event Type	N/A	.events[].s tartTime	BASE	N/A
.events[].objectType Name	Attribute	Event Object Type	N/A	.events[].s tartTime	SecurityEvent	N/A
.events[].name	Attribute	Event Name	N/A	.events[].s tartTime	TCP_DENIED	N/A
.events[].originator	Attribute	Origination	N/A	.events[].s tartTime	SOURCE	N/A
.events[].assetCriticality	Attribute	Asset Criticality	N/A	.events[].s tartTime	0	N/A
.events[].file.name	Attribute	Active Channel	N/A	.events[].s tartTime	N/A	Only if .events[]. file.type == 'ActiveChannel'
.events[].modelConfidence	Attribute	Model Confidence	N/A	.events[].s tartTime	0	N/A
.events[].priority	Attribute	Priority	N/A	.events[].s tartTime	7	N/A
.events[].relevance	Attribute	Relevance	N/A	.events[].s tartTime	10	N/A
.events[].severity	Attribute	Severity	N/A	.events[].s tartTime	0	N/A
.events[].agentSeverity	Attribute	Agent Severity	N/A	.events[].s tartTime	3	N/A
.events[].agent.name	Attribute	Agent Name	N/A	.events[].s tartTime	N/A	N/A
.events[].agent.type	Attribute	Agent Type	N/A	.events[].s tartTime	squid_file	N/A
.events[].agent. hostName	Attribute	Agent Hostname	N/A	.events[].s tartTime	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
<code>.events[].category.behavior</code>	Attribute	Category Behavior	N/A	<code>.events[].startTime</code>	/Access/Start	N/A
<code>.events[].category.deviceGroup</code>	Attribute	Category Device Group	N/A	<code>.events[].startTime</code>	/Application	N/A
<code>.events[].category.object</code>	Attribute	Category Object	N/A	<code>.events[].startTime</code>	/Host/Resource	N/A
<code>.events[].category.significance</code>	Attribute	Category Significance	N/A	<code>.events[].startTime</code>	/Informational/Warning	N/A
<code>.events[].category.outcome</code>	Attribute	Category Outcome	N/A	<code>.events[].startTime</code>	/Failure	N/A
<code>.events[].category.deviceType</code>	Attribute	Category Device Type	N/A	<code>.events[].startTime</code>	Web Filtering	N/A
<code>.events[].source.address</code>	Value	Indicator (IP Address)	Transformed using ip filter	<code>.events[].startTime</code>	N/A	Private IPs are ignored
<code>.events[].destination.address</code>	Value	Indicator (IP Address)	Transformed using ip filter	<code>.events[].startTime</code>	N/A	Private IPs are ignored
<code>.events[*]</code>	Title	Event (ArcSight Event)	Title built by formatting multiple keys together	<code>.events[].startTime</code>	N/A	N/A
<code>.displayName</code>	Title	Event (ArcSight .typeName ?? Case)	N/A	<code>.createdTimestamp</code>	N/A	N/A
<code>.description</code>	Description	Event	N/A	<code>.createdTimestamp</code>	N/A	N/A

Get Case (Supplemental)

The Get Case supplemental feed will fetch the (almost) full details of an ArcSight case by its ID.

GET `https://{{host}}/detect-api/rest/cases/{{case_id}}`

Sample Response:

```
[
  {
    "action": "BLOCK_OR_SHUTDOWN",
    "associatedImpact": "INTEGRITY",
    "attackAgent": "OUTSIDER",
    "attackMechanism": "INFORMATIONAL",
    "attackTime": null,
    "attributeInitializationInProgress": false,
    "consequenceSeverity": "CRITICAL",
    "createdTimestamp": "2021-04-12 14:05:12-00:00",
    "creatorName": "admin",
    "deprecated": false,
    "detectionTime": "2021-4-10 15:23:31 Etc/UTC",
    "disabled": false,
    "displayID": 1,
    "displayName": "ArcSight Case: Sighting of Trickbot Indicator",
    "estimatedRestoreTime": null,
    "estimatedStartTime": "2021-4-10 15:21:53 Etc/UTC",
    "eventIDs": [
      7203010,
      7203080
    ],
    "frequency": "NEVER_OR_ONCE",
    "history": "KNOWN_OCCURENCE",
    "inCache": false,
    "inactive": false,
    "initialized": true,
    "isAdditionalLoaded": false,
    "lastOccurenceTime": null,
    "localID": 30064771073,
    "modificationCount": 8,
    "modifiedTimestamp": "2021-05-10 15:23:31-00:00",
    "modifierName": "admin",
    "name": "ArcSight Case: Sighting of Trickbot Indicator",
    "numberOfOccurences": 0,
    "operationalImpact": "HIGH_PRIORITY_IMPACT",
    "reference": {
      "id": "7ioxmxngBABCbqbxclEodmA==",
      "isModifiable": true,
      "managerID": "92EpNXgBABCAYBuppdOPcA==",
      "referenceName": "Case",
      "referenceString": "<Resource URI=\\\"/All Cases/All Cases/Personal/
admin's Cases/ArcSight Case: Sighting of Trickbot Indicator\\\"
```

```

ID="\7ioxmxngBABCbqbxclEodmA==\"/>",
    "referenceType": 7,
    "uri": "/All Cases/All Cases/Personal/admin's Cases/ArcSight Case:
Sighting of Trickbot Indicator"
  },
  "reportingLevel": 3,
  "resistance": "HIGH",
  "resourceId": "7ioxmxngBABCbqbxclEodmA==",
  "securityClassification": "SECRET",
  "securityClassificationCode": "I 0   E S I B ",
  "sensitivity": "SECRET",
  "signature": {
    "id": "7ioxmxngBABCbqbxclEodmA==",
    "modificationCount": 8
  },
  "stage": "INITIAL",
  "state": 2,
  "ticketType": "INCIDENT",
  "type": 7,
  "typeName": "Case",
  "uri": "/All Cases/All Cases/Personal/admin's Cases/ArcSight Case:
Sighting of Trickbot Indicator",
  "vulnerability": "ENVIRONMENT",
  "vulnerabilityType1": "ACCIDENTAL",
  "vulnerabilityType2": "EMI_RFI"
},
{
  "action": "BLOCK_OR_SHUTDOWN",
  "alias": "Sighting of Malware",
  "associatedImpact": "AVAILABILITY",
  "attackAgent": "INSIDER",
  "attackMechanism": "PHYSICAL",
  "attackTime": null,
  "attributeInitializationInProgress": false,
  "consequenceSeverity": "MARGINAL",
  "createdTimestamp": "2021-05-10 14:22:52-00:00",
  "creatorName": "admin",
  "deprecated": false,
  "description": "This is a mlicious event sighting. Write that down.",
  "detectionTime": null,
  "disabled": false,
  "displayID": 2,
  "displayName": "Sighting of Malware",
  "estimatedRestoreTime": "2021-4-10 14:20:20 Etc/UTC",
  "estimatedStartTime": null,
  "events": [],
  "frequency": "NEVER_OR_ONCE",
  "history": "KNOWN_OCCURENCE",
  "inCache": true,
  "inactive": false,
  "initialized": true,

```

```

        "isAdditionalLoaded": false,
        "lastOccurrenceTime": null,
        "localID": 30064771074,
        "modificationCount": 0,
        "modifiedTimestamp": "2021-05-10 14:22:52-00:00",
        "modifierName": "admin",
        "name": "ArcSight Malicious Event Sighting",
        "numberOfOccurrences": 0,
        "operationalImpact": "HIGH_PRIORITY_IMPACT",
        "reference": {
            "id": "7vralVnkBABDl04n55EGTXw==",
            "isModifiable": true,
            "managerID": "92EpNXgBABCAYBuppdOPcA==",
            "referenceName": "Case",
            "referenceString": "<Resource URI=\\\"/All Cases/All Cases/Personal/
admin's Cases/Sighting of Malware\\\" ID=\\\"7vralVnkBABDl04n55EGTXw==\\\"/>",
            "referenceType": 7,
            "uri": "/All Cases/All Cases/Personal/admin's Cases/Sighting of
Malware"
        },
        "reportingLevel": 2,
        "resistance": "HIGH",
        "resourceId": "7vralVnkBABDl04n55EGTXw==",
        "securityClassification": "CONFIDENTIAL",
        "securityClassificationCode": "P I    D U A B ",
        "sensitivity": "UNCLASSIFIED",
        "signature": {
            "id": "7vralVnkBABDl04n55EGTXw==",
            "modificationCount": 0
        },
        "stage": "INITIAL",
        "state": 2,
        "ticketType": "INCIDENT",
        "type": 7,
        "typeName": "Case",
        "uri": "/All Cases/All Cases/Personal/admin's Cases/Sighting of
Malware",
        "vulnerability": "DESIGN",
        "vulnerabilityType1": "ACCIDENTAL",
        "vulnerabilityType2": "EMI_RFI"
    }
]

```

Get Events (Supplemental)

The Get Events supplemental feed will fetch a list of events based on a list of event IDs.

POST <https://{{host}}/detect-api/rest/events/retrieve>

Sample Response:

```
[
  {
    "agent": {
      "address": 168624229,
      "addressAsBytes": "Cg0AZQ==",
      "assetId": "43GEpNXgBABCAXca3khNRMw==",
      "assetLocalId": 17179869185,
      "assetName": "10.13.0.101",
      "hostName": "10.13.0.101",
      "id": "3IWIpNXgBABCAPa1BlSONA==",
      "macAddress": -9223372036854776000,
      "mutable": true,
      "name": "Manager Internal Agent",
      "translatedAddress": -9223372036854776000,
      "type": "arcsight_security_manager",
      "version": "7.4.0.2675.0",
      "zone": {
        "id": "ML8022AABABCDTFpYAT3UdQ==",
        "isModifiable": true,
        "managerID": "92EpNXgBABCAYBuppdOPcA==",
        "referenceID": 2083,
        "referenceName": "Zone",
        "referenceString": "<Resource URI=\\\"/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255\\\" ID=\\\"ML8022AABABCDTFpYAT3UdQ=\\\"/>",
        "referenceType": 29,
        "uri": "/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255"
      }
    },
    "agentReceiptTime": -9223372036854776000,
    "agentSeverity": 1,
    "aggregatedEventCount": 1,
    "assetCriticality": 0,
    "baseEventCount": 1,
    "bytesIn": -2147483648,
    "bytesOut": -2147483648,
    "category": {
      "behavior": "/Execute/Query",
      "deviceGroup": "/Application",
      "mutable": true,
      "object": "/Host/Application",
      "outcome": "/Success",

```

```

    "significance": "/Normal"
  },
  "concentratorAgents": [
    {
      "address": 168624229,
      "addressAsBytes": "Cg0AZQ==",
      "assetId": "43GEpNXgBABCAXca3khNRMw==",
      "assetLocalId": 17179869185,
      "assetName": "10.13.0.101",
      "hostName": "10.13.0.101",
      "id": "3IWIpNXgBABCAZpa1BlSONA==",
      "macAddress": -9223372036854776000,
      "mutable": true,
      "name": "Manager Internal Agent",
      "translatedAddress": -9223372036854776000,
      "type": "arcsight_security_manager",
      "version": "7.4.0.2675.0",
      "zone": {
        "id": "ML8022AABABCDTFpYAT3UdQ==",
        "isModifiable": true,
        "managerID": "92EpNXgBABCAYBuppdOPcA==",
        "referenceID": 2083,
        "referenceName": "Zone",
        "referenceString": "<Resource URI=\\\"/All Zones/ArcSight
System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255\\\"
ID=\\\"ML8022AABABCDTFpYAT3UdQ=\\\"/>",
        "referenceType": 29,
        "uri": "/All Zones/ArcSight System/Private Address Space
Zones/RFC1918: 10.0.0.0-10.255.255.255"
      }
    }
  ],
  "concentratorDevices": [
    {
      "address": 168624229,
      "addressAsBytes": "Cg0AZQ==",
      "assetId": "43GEpNXgBABCAXca3khNRMw==",
      "assetLocalId": 17179869185,
      "assetName": "10.13.0.101",
      "hostName": "tie-dev-arcsight",
      "macAddress": -9223372036854776000,
      "mutable": true,
      "product": "ArcSight",
      "translatedAddress": -9223372036854776000,
      "vendor": "ArcSight",
      "version": "7.4.0.2675.0",
      "zone": {
        "id": "ML8022AABABCDTFpYAT3UdQ==",
        "isModifiable": true,
        "managerID": "92EpNXgBABCAYBuppdOPcA==",

```

```

        "referenceID": 2083,
        "referenceName": "Zone",
        "referenceString": "<Resource URI=\\\"/All Zones/ArcSight
System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255\\\"
ID=\\\"ML8022AABABCDTFpYAT3UdQ==\\\"/>",
        "referenceType": 29,
        "uri": "/All Zones/ArcSight System/Private Address Space
Zones/RFC1918: 10.0.0.0-10.255.255.255"
    }
},
],
"correlatedEventCount": 0,
"destination": {
    "address": 168624229,
    "addressAsBytes": "Cg0AZQ==",
    "assetId": "43GEpNXgBABCAXca3khNRMw==",
    "assetLocalId": 17179869185,
    "assetName": "10.13.0.101",
    "geo": {
        "latitude": 0,
        "latitudeLong": 0,
        "longitude": 0,
        "longitudeLong": 0,
        "mutable": true
    },
    "hostName": "10.13.0.101",
    "macAddress": -9223372036854776000,
    "mutable": true,
    "port": 8443,
    "processId": -2147483648,
    "translatedAddress": -9223372036854776000,
    "translatedPort": -2147483648,
    "userId": "1oDcnNXgBABCA26-LEyzrew==",
    "userName": "admin",
    "zone": {
        "id": "ML8022AABABCDTFpYAT3UdQ==",
        "isModifiable": true,
        "managerID": "92EpNXgBABCAYBuppdOPcA==",
        "referenceID": 2083,
        "referenceName": "Zone",
        "referenceString": "<Resource URI=\\\"/All Zones/ArcSight System/
Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255\\\"
ID=\\\"ML8022AABABCDTFpYAT3UdQ==\\\"/>",
        "referenceType": 29,
        "uri": "/All Zones/ArcSight System/Private Address Space Zones/
RFC1918: 10.0.0.0-10.255.255.255"
    }
},
"device": {
    "address": 168624229,

```

```

    "addressAsBytes": "Cg0AZQ==",
    "assetId": "43GEpNXgBABCAXca3khNRMw==",
    "assetLocalId": 17179869185,
    "assetName": "10.13.0.101",
    "hostName": "tie-dev-arcsight",
    "macAddress": -9223372036854776000,
    "mutable": true,
    "product": "ArcSight",
    "translatedAddress": -9223372036854776000,
    "vendor": "ArcSight",
    "version": "7.4.0.2675.0",
    "zone": {
      "id": "ML8022AABABCDTFpYAT3UdQ==",
      "isModifiable": true,
      "managerID": "92EpNXgBABCAYBuppdOPcA==",
      "referenceID": 2083,
      "referenceName": "Zone",
      "referenceString": "<Resource URI=\\\"/All Zones/ArcSight System/
Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255\\\"
ID=\\\"ML8022AABABCDTFpYAT3UdQ=\\\"/>",
      "referenceType": 29,
      "uri": "/All Zones/ArcSight System/Private Address Space Zones/
RFC1918: 10.0.0.0-10.255.255.255"
    },
  },
  "deviceCustom": {
    "mutable": true,
    "string2Label": "Configuration Resource"
  },
  "deviceCustomDate1": -9223372036854776000,
  "deviceCustomDate2": -9223372036854776000,
  "deviceCustomFloatingPoint1": 5e-324,
  "deviceCustomFloatingPoint2": 5e-324,
  "deviceCustomFloatingPoint3": 5e-324,
  "deviceCustomFloatingPoint4": 5e-324,
  "deviceCustomNumber1": -9223372036854776000,
  "deviceCustomNumber2": -9223372036854776000,
  "deviceCustomNumber3": -9223372036854776000,
  "deviceCustomString2": "<Resource URI=\\\"/All Active Channels/ArcSight
Administration/ESM/System Health/Events/System Events Last Hour\\\"
ID=\\\"QjZvvPPsAABCAEcWZ6-B1EQ=\\\"/>",
  "deviceDirection": -2147483648,
  "deviceEventCategory": "/Active Channel/Attached",
  "deviceEventClassId": "channel:001",
  "deviceProcessId": -2147483648,
  "deviceReceiptTime": 1620660113611,
  "deviceSeverity": "Warning",
  "domainDate1": -9223372036854776000,
  "domainDate2": -9223372036854776000,
  "domainDate3": -9223372036854776000,

```

```

"domainDate4": -9223372036854776000,
"domainDate5": -9223372036854776000,
"domainDate6": -9223372036854776000,
"domainFp1": 5e-324,
"domainFp2": 5e-324,
"domainFp3": 5e-324,
"domainFp4": 5e-324,
"domainFp5": 5e-324,
"domainFp6": 5e-324,
"domainFp7": 5e-324,
"domainFp8": 5e-324,
"domainIpv4addr1": -9223372036854776000,
"domainIpv4addr2": -9223372036854776000,
"domainIpv4addr3": -9223372036854776000,
"domainIpv4addr4": -9223372036854776000,
"domainNumber1": -9223372036854776000,
"domainNumber10": -9223372036854776000,
"domainNumber11": -9223372036854776000,
"domainNumber12": -9223372036854776000,
"domainNumber13": -9223372036854776000,
"domainNumber2": -9223372036854776000,
"domainNumber3": -9223372036854776000,
"domainNumber4": -9223372036854776000,
"domainNumber5": -9223372036854776000,
"domainNumber6": -9223372036854776000,
"domainNumber7": -9223372036854776000,
"domainNumber8": -9223372036854776000,
"domainNumber9": -9223372036854776000,
"dummyField": "dummyField",
"endTime": 1620660113611,
"eventAnnotation": {
  "auditTrail":
"1,1620660216190,,,8,,\n1,1615800140091,root,Queued,,,\\n",
  "endTime": 1620660216190,
  "eventId": 7203010,
  "flags": 8,
  "managerReceiptTime": 1620660113611,
  "modificationTime": 1620660216190,
  "stage": {
    "id": "R9MHiNfoAABCASsxbPIxG0g==",
    "isModifiable": false,
    "managerID": "92EpNXgBABCAyBuppdOPcA==",
    "referenceID": 2207,
    "referenceName": "Stage",
    "referenceString": "<Resource URI=\\\"/All Stages/Queued\\\"
ID=\\\"R9MHiNfoAABCASsxbPIxG0g=\\\"/>",
    "referenceType": 34,
    "uri": "/All Stages/Queued\"
  },
  "stageUpdateTime": 1620660216190,

```

```

    "version": 2
  },
  "eventId": 7203010,
  "file": {
    "createTime": -9223372036854776000,
    "modificationTime": -9223372036854776000,
    "name": "System Events Last Hour",
    "path": "/All Active Channels/ArcSight Administration/ESM/System
Health/Events/System Events Last Hour",
    "size": -9223372036854776000,
    "type": "ActiveChannel"
  },
  "finalDevice": {
    "address": 168624229,
    "addressAsBytes": "Cg0AZQ==",
    "assetId": "43GEpNXgBABCAXca3khNRMw==",
    "assetLocalId": 17179869185,
    "assetName": "10.13.0.101",
    "hostName": "tie-dev-arcsight",
    "macAddress": -9223372036854776000,
    "mutable": true,
    "product": "ArcSight",
    "translatedAddress": -9223372036854776000,
    "vendor": "ArcSight",
    "version": "7.4.0.2675.0",
    "zone": {
      "id": "ML8022AABABCDTFpYAT3UdQ==",
      "isModifiable": true,
      "managerID": "92EpNXgBABCAYBuppdOPcA==",
      "referenceID": 2083,
      "referenceName": "Zone",
      "referenceString": "<Resource URI=\\\"/All Zones/ArcSight System/
Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255\\\"
ID=\\\"ML8022AABABCDTFpYAT3UdQ=\\\"/>",
      "referenceType": 29,
      "uri": "/All Zones/ArcSight System/Private Address Space Zones/
RFC1918: 10.0.0.0-10.255.255.255"
    }
  },
  "flexDate1": -9223372036854776000,
  "flexNumber1": -9223372036854776000,
  "flexNumber2": -9223372036854776000,
  "locality": 0,
  "managerId": -128,
  "managerReceiptTime": 1620660113611,
  "modelConfidence": 4,
  "name": "Channel [System Events Last Hour] got attached",
  "objectTypeName": "SecurityEvent",
  "originalAgent": {
    "address": 168624229,

```

```

    "addressAsBytes": "Cg0AZQ==",
    "assetId": "43GEpNXgBABCAXca3khNRMw==",
    "assetLocalId": 17179869185,
    "assetName": "10.13.0.101",
    "hostName": "10.13.0.101",
    "id": "3IWIpNXgBABCaZpa1BlSONA==",
    "macAddress": -9223372036854776000,
    "mutable": true,
    "name": "Manager Internal Agent",
    "translatedAddress": -9223372036854776000,
    "type": "arcsight_security_manager",
    "version": "7.4.0.2675.0",
    "zone": {
      "id": "ML8022AABABCDTFpYAT3UdQ==",
      "isModifiable": true,
      "managerID": "92EpNXgBABCAYBuppdOPcA==",
      "referenceID": 2083,
      "referenceName": "Zone",
      "referenceString": "<Resource URI=\\\"/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255\\\"ID=\\\"ML8022AABABCDTFpYAT3UdQ=\\\"/>",
      "referenceType": 29,
      "uri": "/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255"
    },
    },
    "originator": "SOURCE",
    "persistence": -2147483648,
    "priority": 3,
    "relevance": 10,
    "sessionId": -9223372036854776000,
    "severity": 0,
    "source": {
      "address": 168624188,
      "addressAsBytes": "Cg0APA==",
      "assetId": "46ByWg3gBABCbJmdfYAV+lw==",
      "assetLocalId": 17179869188,
      "assetName": "10.13.0.60",
      "geo": {
        "latitude": 0,
        "latitudeLong": 0,
        "longitude": 0,
        "longitudeLong": 0,
        "mutable": true
      },
      "hostName": "10.13.0.60",
      "macAddress": -9223372036854776000,
      "mutable": true,
      "port": -2147483648,
      "processId": -2147483648,

```

```

    "serviceName": "/XmlRpc",
    "translatedAddress": -9223372036854776000,
    "translatedPort": -2147483648,
    "zone": {
      "id": "ML8022AABABCDTFpYAT3UdQ==",
      "isModifiable": false,
      "managerID": "92EpNXgBABCAYBuppdOPcA==",
      "referenceID": 2083,
      "referenceName": "Zone",
      "referenceString": "<Resource URI=\\\"/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255\\\" ID=\\\"ML8022AABABCDTFpYAT3UdQ=\\\"/>",
      "referenceType": 29,
      "uri": "/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255"
    },
    "startTime": 1620660113611,
    "ttl": 10,
    "type": "BASE"
  }
]

```

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.

ArcSight Case Management Feed

METRIC	RESULT
Run Time	1 minute
Indicators	3
Events	7
Event Attributes	143

Known Issues / Limitations

- There is currently no way to time fence queries to the API when fetching cases. Due to this limitation, the integration will fetch all cases using their IDs and drop the ones that haven't been updated.

Change Log

- **Version 1.0.1**
 - Resolved an issue where the feed would respond with an `Error Applying Filter` error if the **Get Events supplemental** feed returned an empty list from ArcSight.
- **Version 1.0.0 rev-a**
 - Updated installation steps as users are no longer required to install the IP filter manually.
- **Version 1.0.0**
 - Initial release