ArcSight ArcSight Threat Acceleration Program

Software Version: 23.4

ArcSight Threat Acceleration Program Administrator's Guide

Document Release Date: October 2023
Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

The title page of this document home page of this Help contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Contents

Administrator's Guide for ArcSight Threat Acceleration Program 23.4

This guide provides information for ArcSight environment administrators and operators.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the software and its environment..

Additional Documentation

The ArcSight Threat Acceleration Program documentation library includes the following resource:

- *Release Notes for ArcSight Threat Acceleration Program*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight Threat Acceleration Program.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.For specific product issues, contact Micro Focus Customer Care.

For specific product issues, contact Open Text Support for Micro Focus products.

Product Overview

Threat intelligence is no longer considered as a 'nice to have' option and organizations are looking to implement threat detection mechanisms, which can detect the latest and most notorious attacks as early as possible.

ArcSight is an immersive cyberthreat experience that provides actionable and business-centric threat intelligence for security executives. ArcSight enables cyber professionals to quickly gain visibility into the most pressing threats to their business and helps organizations secure their value chains so they can focus on driving business growth.

At a high level, the ArcSight Threat Acceleration Program (ATAP), is comprised of two main components:

• **ArcSight Threat Research Online:** This portal is designed to help CISOs, senior executives, and risk professionals by providing the platform for enhanced visibility to cyber threats. You can analyze cyber threats targeting your organization with practical business insights and guidance. The portal presents customizable dashboards that provides an opportunity for you to prioritize the threats and measure its intensity. You can now understand how threat operates and determine the frequency of attacks. The portal offers a comprehensive threat research and monitors the specific business risks for each individual.

• **ArcSight Threat Acceleration Program (ATAP):** Provides up-to-the-minute threat intelligence (from OSINT -open source- and ArcSight-curated premium intelligence) feed for ArcSight ESM customers.

ArcSight Threat Acceleration Program

At a high level, ATAP comprises of the following two licensing models:

ATAP Basic

- Provides near real-time threat intelligence, by synchronizing an ArcSight ESM Server with ArcSight Threat Intelligence (TI) server in the cloud.
- The threat intelligence received is the Open Source Intelligence (OSINT), filtered on `TLP:WHITE` as provided by the public instance of MISP CIRCL TI feed.
- Does not require an access key.

ATAP Plus

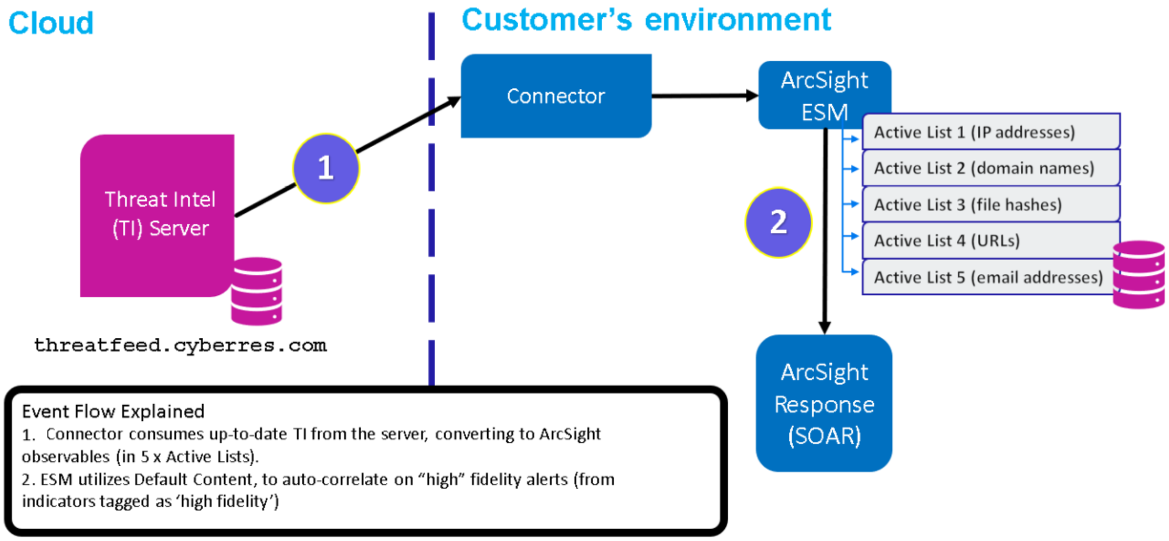
- Commercial, premium offering.
- All of the ATAP Basic features.
- Quicker indicator synchronisation.
- Best suited for triggering automation with the high confidence records.
- Human curation ensures higher fidelity of the records.
- Integration with "ArcSight Threat Research Online".
- Actor attribution.
- Best integrates with default content and high confidence rulesets for automation and resource optimization.

ATAP Solution Overview

As can be seen from the diagram below, ATAP Model Import Connector connects the ArcSight ecosystem to the ArcSight Threat Feed server, synchronizing the data multiple times daily. In the 1.0 release, we support the threat feed only into ArcSight ESM.

ArcSight solution provides an end-to-end experience, by also including the ESM content (detection, correlation rules, etc…) as well as integration into SOAR. This ATAP content is embedded into the ArcSight Default Content, available out-of-the-box, as a turnkey solution for today’s advanced SOC’s.

The ArcSight Threat Acceleration Program Model Import Connector retrieves threat intelligence events and attribute data and uploads it to ESM Active Lists found under **All Active Lists > ArcSight Foundation > Threat Intelligence Platform**. These entries include, IP addresses, domain names, email addresses, hash values, and URLs.

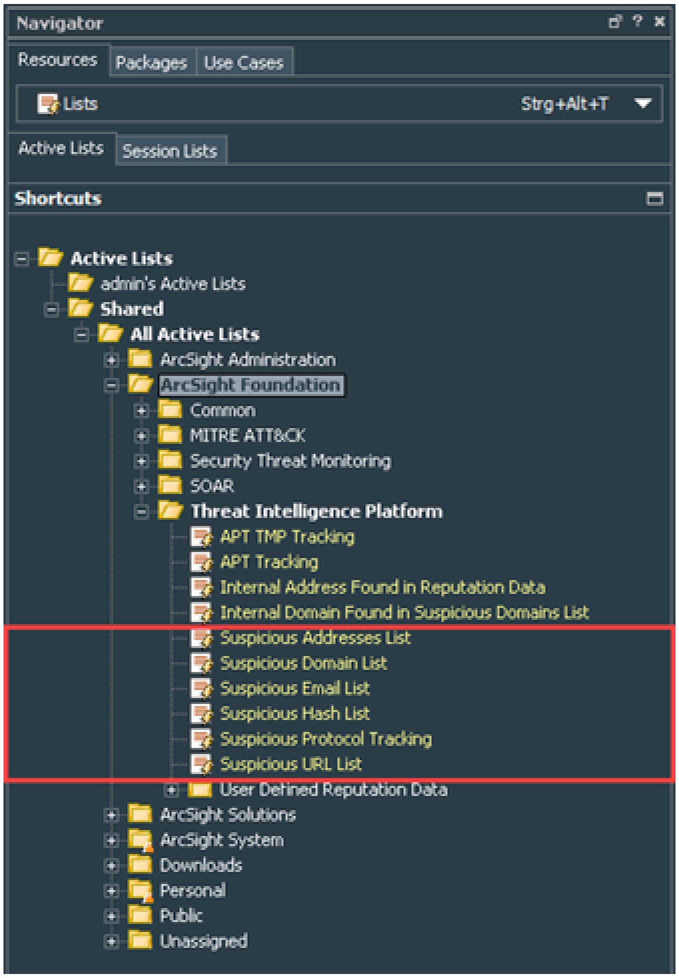


Event Flow Explained
1. Connector consumes up-to-date TI from the server, converting to ArcSight observables (in 5 x Active Lists).
2. ESM utilizes Default Content, to auto-correlate on “high” fidelity alerts (from indicators tagged as ‘high fidelity’)

Event Flow Explained

- ArcSight Model Import Connector consumes up-to-date Threat Intelligence from the server, converting to ArcSight observables (in 5 x Active Lists).
  - Suspicious Addresses List
  - Suspicious Domain List
  - Suspicious Email List
  - Suspicious Hash List

- ○ Suspicious URL List



- ArcSight ESM utilizes Default Content, to auto-correlate on "High confidence" alerts. The `high confidence` tag is added to description field in the 5 Active Lists, and more attack types are added to `indicatorType` field in order to trigger specific rules (for example phishing attack).

ATAP Connector Installation Options

Arcsight Threat Acceleration Program Model Import Connector provides the following three options, as to which threat intelligence feed to synchronize with:

- **ArcSight Threat Acceleration Program Plus:**This option is subscription based and unlocks the premium threat intelligence feed for ArcSight ESM customers. This feed is curated by the ArcSight Threat Intel Research Team and it is hosted on the ATAP server https://threatfeed.cyberres.com. This feed is mostly comprised of "zero false positive, high fidelity indicators of compromise" that correlate with the most critical cyber security threats an organization needs to identify and resolve at the highest urgency level.

This option requires a valid subscription key, to connect to the threat feed server. This subscription key is delivered to all ATAP Plus customers who have purchased 1, 2, or 3-year subscriptions to the ATAP Plus solution. The user is alerted when the ATAP Plus API key expires so that the subscription can be renewed accordingly. ATAP Plus is compatible with the default content update packages that are periodically released.

  - As this option requires a connection to ATAP Threat Feed Server, the following firewall port should be opened one-way, from the ATAP Connector host, to the ATAP Threat Intelligence server as follows:

    Protocol/port: TCP port 443

    from: the host machine hosting/running the ATAP Model Import Connector

    to: https://threatfeed.cyberres.com

  - For more details on required communications initiated by the connector, see Advaned Communication Details.

- **ArcSight Threat Acceleration Program Basic:** All ArcSight ESM customers are entitled to use the ATAP Basic solution free of charge. This option does not require any key. The threat intelligence received is the OSINT (Open Source Intelligence), filtered on `TLP:WHITE` as provided by the public instance of CIRCL MISP TI feed.

  - As this option requires a connection to ATAP Threat Feed Server, the following firewall port must be opened one-way, from the ATAP Model Import Connector host, to the ATAP Threat Intel Server as follows:

    Protocol/port: TCP port 443

    from: the host machine hosting/running the ATAP Model Import Connector

    to: https://threatfeed.cyberres.com

  - For more details on required communications initiated by the connector, see Advaned Communication Details.

- **Custom MISP Instance:** This option can be used if you already use a public or private instance of a MISP server as per the needs of your organization. This option does not require a subscription to ArcSight solution. However, you must have the authorization key - also known as the MISP API key - for the public or private instance of the MISP server you are connecting to.

Note to Existing ArcSight MISP Connector Users: The ArcSight Threat Acceleration Program Model Import Connector is an enhanced version of the previously released ArcSight Model Import Connector for MISP (Open Source Threat Intelligence and Sharing Platform Solution). As upgrading from the Model Import Connector for MISP to ATAP Model Import Connector is not supported, existing users can do a fresh installation of the ATAP Model Import Connector.

Obtaining License Keys

To purchase this pack, contact your account or sales representative.

After you purchase this pack, you can download the package from the Software Licenses and Downloads (SLD) portal.

Log in to the portal using your active service contract ID.

Overview of ATAP Active Lists

The following active lists are being used by ATAP Basic and ATAP Plus:

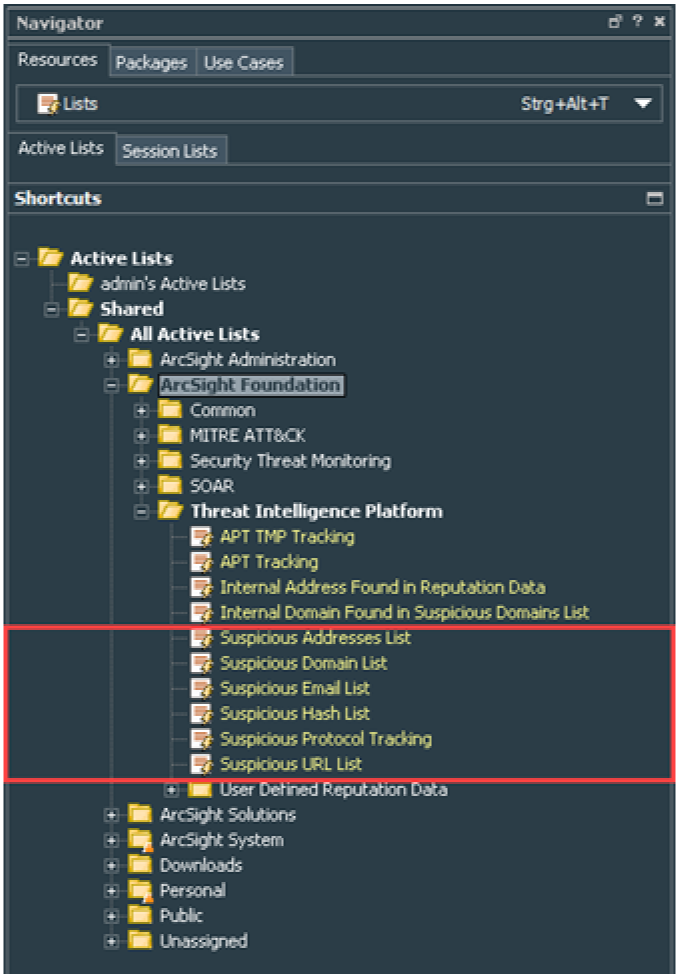
- Suspicious Addresses List
- Suspicious Domain List
- Suspicious Email List
- Suspicious Hash List
- Suspicious URL List

You can adjust the maximum capacity of Active Lists through manager properties, however, it is not required as per the date of this documents writing.

Note, that ATAP Basic and ATAP Plus use the same Active Lists.

Locating ATAP Active Lists

ESM Active Lists are located in **All Active Lists** > **ArcSight Foundation** >**Threat Intelligence Platform** folder.



- Active Lists
  - admin's Active Lists
  - Shared
    - All Active Lists
      - ArcSight Administration
      - ArcSight Foundation
        - Common
        - MITRE ATT&CK
        - Security Threat Monitoring
        - SOAR
        - Threat Intelligence Platform
          - APT TMP Tracking
          - APT Tracking
          - Internal Address Found in Reputation Data
          - Internal Domain Found in Suspicious Domains List
          - Suspicious Addresses List
          - Suspicious Domain List
          - Suspicious Email List
          - Suspicious Hash List
          - Suspicious Protocol Tracking
          - Suspicious URL List
          - User Defined Reputation Data
      - ArcSight Solutions
      - ArcSight System
      - Downloads
      - Personal
      - Public
      - Unassigned

Understanding ATAP Active Lists

Active list entries include, IP addresses, domain names, email addresses, hash values, and URLs.

List	Type of Information	Works With (Example)
Suspicious Addresses	IP Addresses	Proxies, Firewalls, Flows, DNS, EDR
Suspicious Domains	Domain Names	Proxies, Firewalls, EDR, DNS

List	Type of Information	Works With (Example)
Suspicious Emails	Email Addresses	E-Mail Gateway, Mail Servers
Suspicious Hashes	Hash Values (various algorithms)	EDR, AV
Suspicious URLs	Full URL being requested	Proxies, Firewalls, EDR

Active List Fields

If you subscribe to ATAP Plus, the active lists contain the following fields to ensure that the Plus customers get exclusive premium content to help them quickly identify positive threats:

Sl. No.	Field	Description	Example
1	actors	Actual individuals, groups, or organizations believed to be operating with malicious intent.	GUARDIANS OF PEACE, LOCKBIT GANG, ATMZOW
2	address or domain or email or url or hashValue	The suspicious address, domain, email, URL or hashValue found and shared as harmful indicators.	12.44.11.22, badcorp.tld, badguy@badcorp.tld, HTTPS://VEROFORD.COM/SETUP/BRUME.PHP, 4685811c853ceaebc991c3a8406694bf
3	avSignatureName	One or more virus signatures that were used to detect malware associated with the indicator.	TR/Inject.xbbeicg
4	Campaign	A set of malicious activities or attacks carried out by threat actors using specific techniques for some particular purpose.	FOLLINA, EMOTET, LOG4J
5	confidence	The confidence level of theindicator. The values for confidence level are: very high, high, medium, and low values.	High, Medium, Low
6	creatorOrg (origin)	The organization that created the indicator.	ArcSIght, CERT.SI, ADMIN, CISRT KNF
7	cve	A unique and common identifier for a publicly known security vulnerability that is associated with the indicator. When more than one value exists, they are separated by a comma.	CVE-2022-30190

Sl. No.	Field	Description	Example
8	description	A detailed information about indicators of compromise (IOC).	
9	extraInfo	Additional details about IOC.	
10	firstDetectTime	First time this indicator was detected by the threat research team.	6/19/2022
11	galaxyBulletinId (galaxyOnlineID)	The bulletin identifier that references the bulletin record at https://cyberresgalaxy.com.	e071922AAC
12	galaxysearchterm	The search pattern needed to get the associated threads with reference to the current IOC.	
13	atapPlusCS1	Additional fields specific to ATAP Plus	
14	atapPlusCS2	Additional fields specific to ATAP Plus	
15	atapPlusCS3	Additional fields specific to ATAP Plus	
16	atapPlusCS4	Additional fields specific to ATAP Plus	
17	atapPlusCS5	Additional fields specific to ATAP Plus	
18	indicatorType	One or more publicly known malware types that are associated with this indicator.	suspicious, cobalt strike, benign, adware|c2|cnc server
19	lastDetectTime	Last time this indicator was detected by the threat research team.	6/20/2022
20	malwareName	One or more malware names associated with the indicator.	CONTI, HERMETICWIPER, PEGASUS

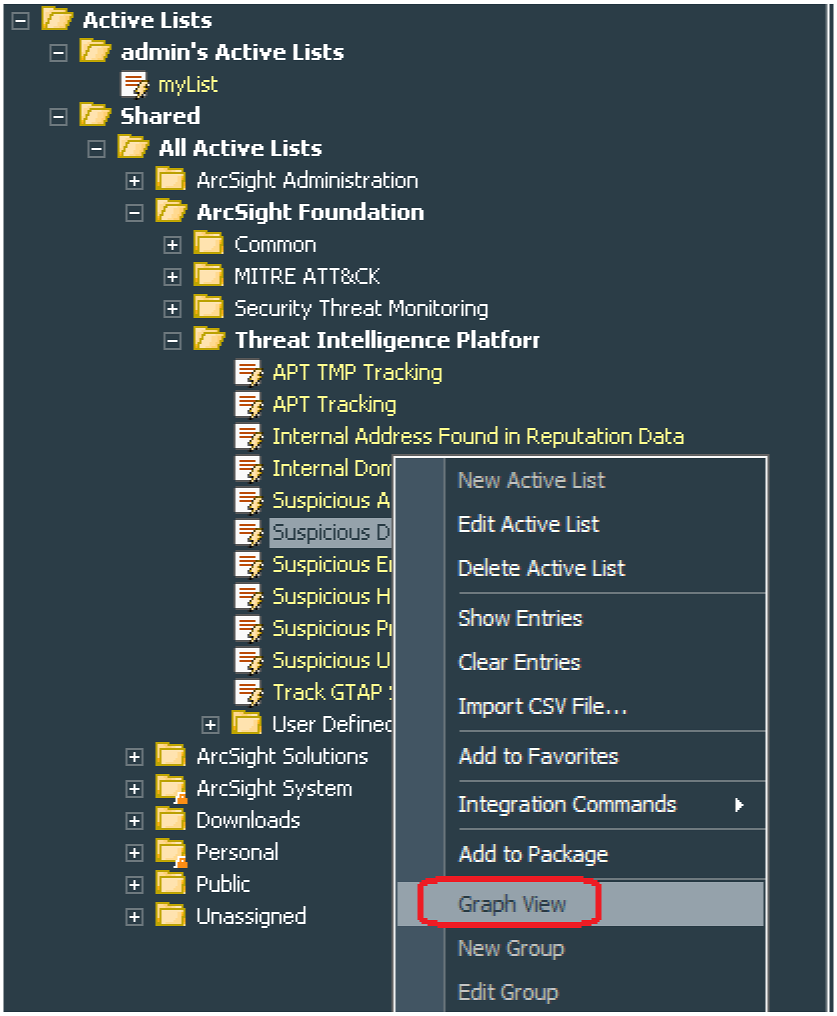
Sl. No.	Field	Description	Example
21	malwareTypes	The malware class determining the type of behavior of the malware.	RANSOMWARE, DATA WIPER, ER, LOADER
22	mitigation	Recommendations, security concepts, technologies that can be used to prevent a technique or sub-technique (used for cyber attacks) from being successfully executed.	
23	mitreAttack	Type of Tactics, Techniques, and Procedures that describe ways that adversaries attempt to compromise targets.	T1060
24	port	Suspicious port number used for the attack	
25	reference	The category, which describes and puts the indicator in a context.	Payload delivery, Network activity
26	sector	Industrial and commercial sectors that the threat belongs to.	Energy, Finance, Chemical, etc.,
27	sightings	The number of times something in the indicator of compromises (such as malware, tool, threat actor, etc.) was seen.	
28	targetLocationRegion	Target regions, we have seen being impacted by this particular indicator.	EUROPE, MIDDLE EAST, AMERICA, AFRICA, OCEANIA
29	targetLocationCountry	Target countries, we have seen being impacted by this particular indicator.	UKRAINE, ISRAEL, INDIA, STATES, BRAZIL, EGYPT, AUSTRALIA
30	toolName	The tool invoked in the indicator activity.	POWERSHELL, RDP, CURL
31	toolTypes	Type of tools used to carry out bad activity.	RCE, BRUTEFORCE, ACCESS, SERVICE

Sl. No.	Field	Description	Example
32	threatActorTypes	The actor group type behind a particular entity.	NATION-STATE, BROKER, CRIMINALS, COMPETITOR, HACKER
33	threatOrigin	The country from where the threat originates or the country sponsoring the threat.	GAMAREDON - RUSSIA
34	threatOperations	The threat itself which is particularly based on the event. The possible values can be threat actors, malware, ransomware or popular vulnerabilities highly exploited in the wild.	FOLLINA, GAMAREDON, LOCKBIT 3.0
35	threatLevel	The severity level of the event, which can be low, medium, or high. **Low:** General mass malware **Medium:** Advanced Persistent Threats (APT) **High:** Sophisticated APTs and 0 day attacks.	Low, Medium, High
36	tiEventID	The global unique identifier of an event across all MISP Servers.	dba88c50-6dd4-447e-9253-c783738eace0
37	virusTotalCount	The number of reliable review committees who consider this indicator harmful.	24

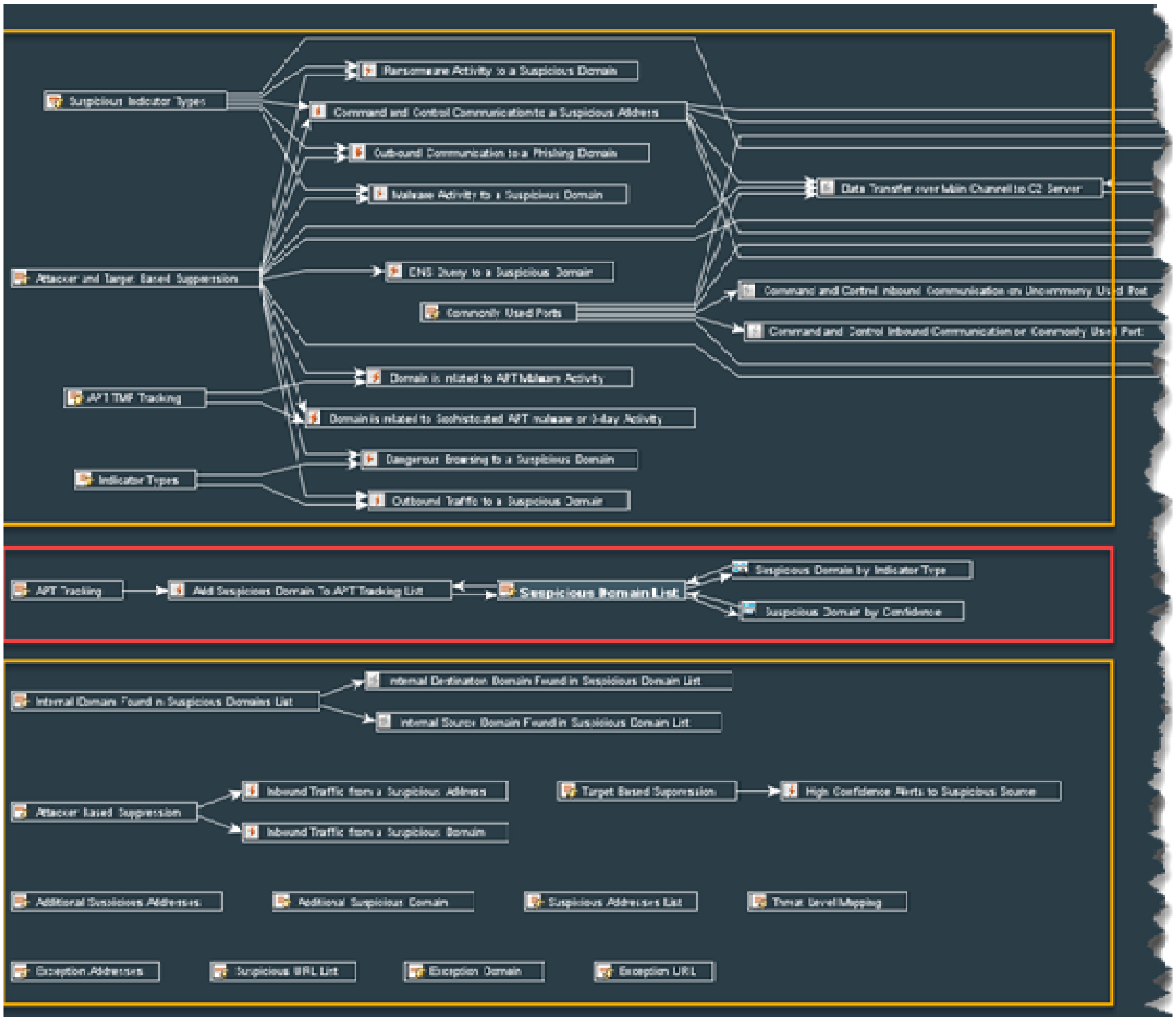
Note: The examples given are not comprehensive dictionaries for the field. Other values could occur.

Understanding How Content Leverages ATAP Active Lists

Various content elements use the lists indirectly. You can generate a graph view of a particular list to understand its indirect usage.



This would look like the following, where YELLOW indicates indirect usage and RED indicates direct usage:


Suspicious Indicator Types
Ransomware Activity to a Suspicious Domain
Command and Control Communication to a Suspicious Address
Outbound Communication to a Phishing Domain
Malware Activity to a Suspicious Domain
Data Transfer over Main Channel to C2 Server
Attacker and Target Based Suppression
DNS Query to a Suspicious Domain
Commonly Used Ports
Command and Control Inbound Communication on Uncommonly Used Port
Command and Control Inbound Communication on Commonly Used Port
Domain is related to APT Malware Activity
APT TMF Tracking
Domain is related to Sophisticated APT malware or 0-day Activity
Dangerous Browsing to a Suspicious Domain
Indicator Types
Outbound Traffic to a Suspicious Domain
APT Tracking
Add Suspicious Domain To APT Tracking List
Suspicious Domain List
Suspicious Domain by Indicator Type
Suspicious Domain by Confidence
Internal Destination Domain Found in Suspicious Domain List
Internal Domain Found in Suspicious Domains List
Internal Source Domain Found in Suspicious Domain List
Inbound Traffic from a Suspicious Address
Attacker Based Suppression
Inbound Traffic from a Suspicious Domain
Target Based Suppression
High Confidence Alerts to Suspicious Source
Additional Suspicious Addresses
Additional Suspicious Domain
Suspicious Addresses List
Threat Level Mapping
Exception Addresses
Suspicious URL List
Exception Domain
Exception URL

Threat Intelligence Platform Dashboards

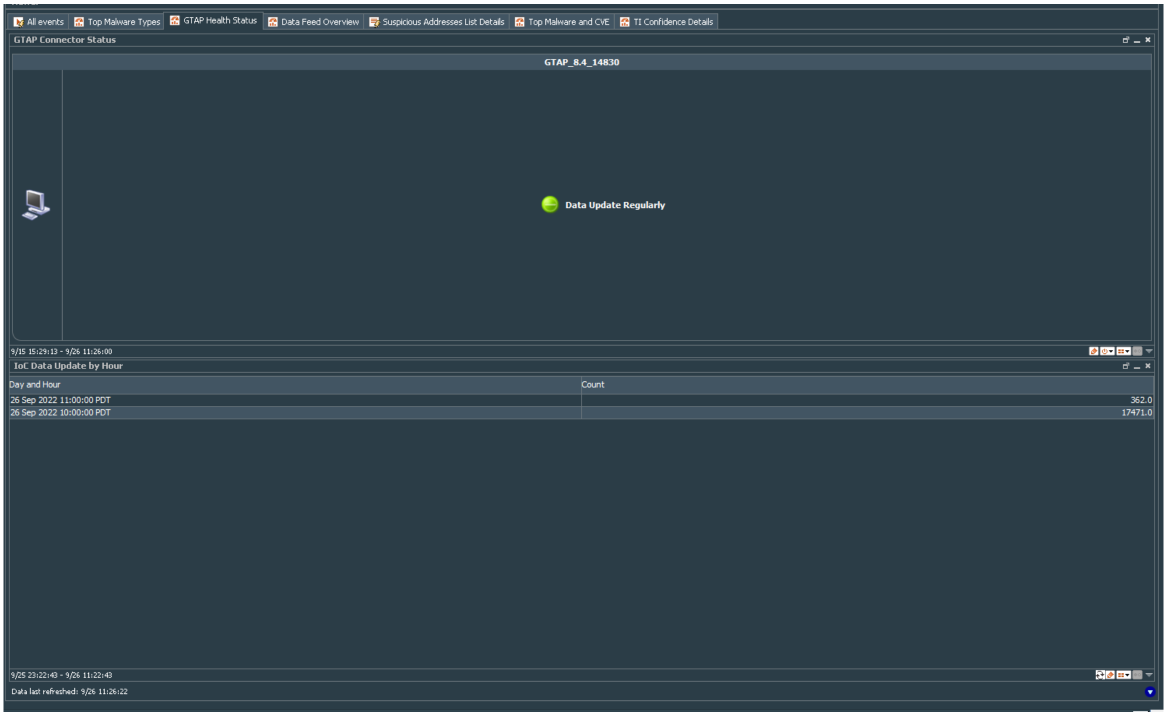
Several dashboards are available to both ATAP Basic and ATAP Plus customers. These dashboards display various charts based on data received from all Active Lists. However, data displayed for ATAP Plus customers is different from data displayed for ATAP Basic customers.

To use dashboards, you must install the ESM default content packages from Marketplace.

The following dashboards are part of Threat Intelligence Platform in the ESM Console:

- ATAP SmartConnector Status
- TI Confidence Details
- Data Feed Overview
- Top Malware and CVE
- TI Confidence Comparison - Open Source vs ArcSight-curated
- Threat Intelligence Security Incidents Overview

ATAP Connector Status



GTAP Connector Status

GTAP_8.4_14830

● Data Update Regularly

9/15 15:29:13 - 9/26 11:26:00

IoC Data Update by Hour

Day and Hour	Count
26 Sep 2022 11:00:00 PDT	362.0
26 Sep 2022 10:00:00 PDT	17471.0

9/25 23:22:43 - 9/26 11:22:43

Data last refreshed: 9/26 11:26:22

- **ATAP Connector Status:** This dashboard gives you an indicator of whether your organization and the results coming from the SIEM system are of higher accuracy or not. If feeds are not coming in, you might consider alerts slightly different, when triggered by Threat Intelligence information.

  Another way of using it is to pay closer attention to alerts after an issue was resolved, as you might see a higher intake of indicators, and thus, a slight alert peak after an issue is resolved.

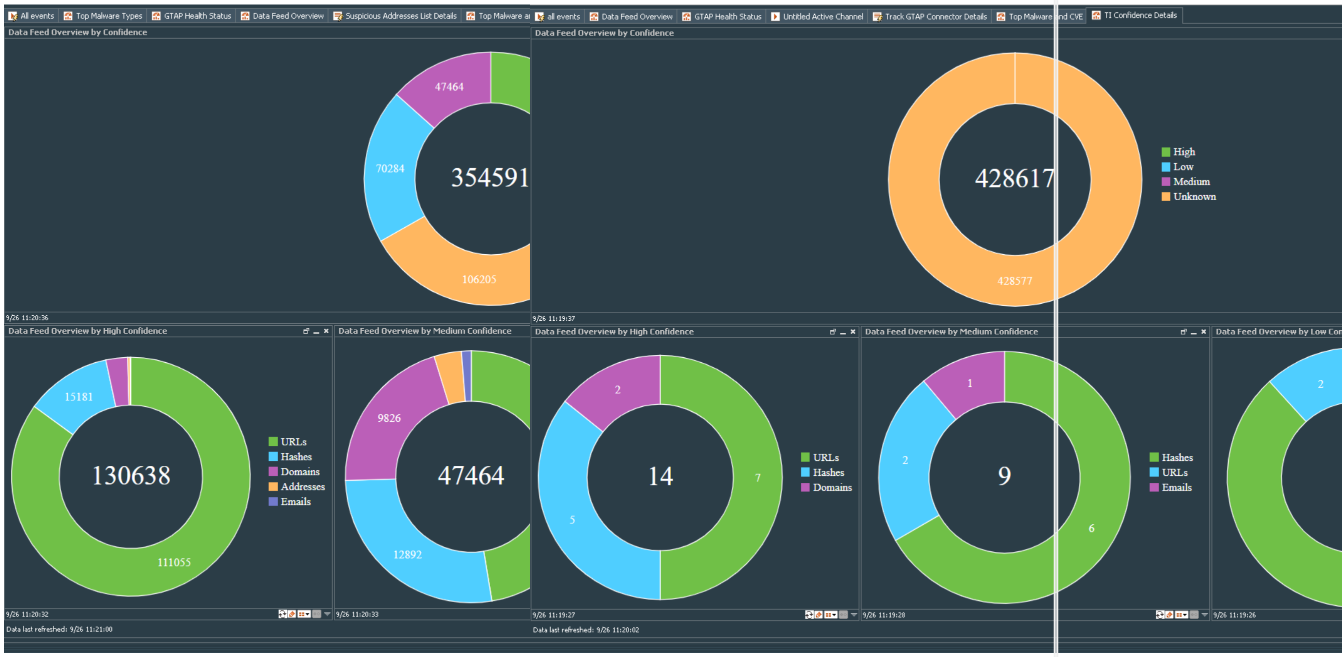
  The most obvious way is to troubleshoot at the connector and network level to investigate why updates/indicator downloads create issues.

  Green indicates that data is getting updated regularly and the connector is up
- **IoC Data Update by Hour:** Updates per hour received by the feed gives an indication of how lively the feeds are. The records are not generated and forgotten. Research can unveil changing perspectives over time which we try to get into the feed as timely as possible.

TI Confidence Details

The TI Confidence dashboard indicates our confidence based on our research if an attribute is malicious or not. High indicates that we are highly confident that the attribute is malicious and can be a candidate for auto-block.

To access the TI Confidence Details dashboard, go to **All Dashboards** > **ArcSight Foundation** > **Threat Intelligence Platform** > **TI Confidence Details**.



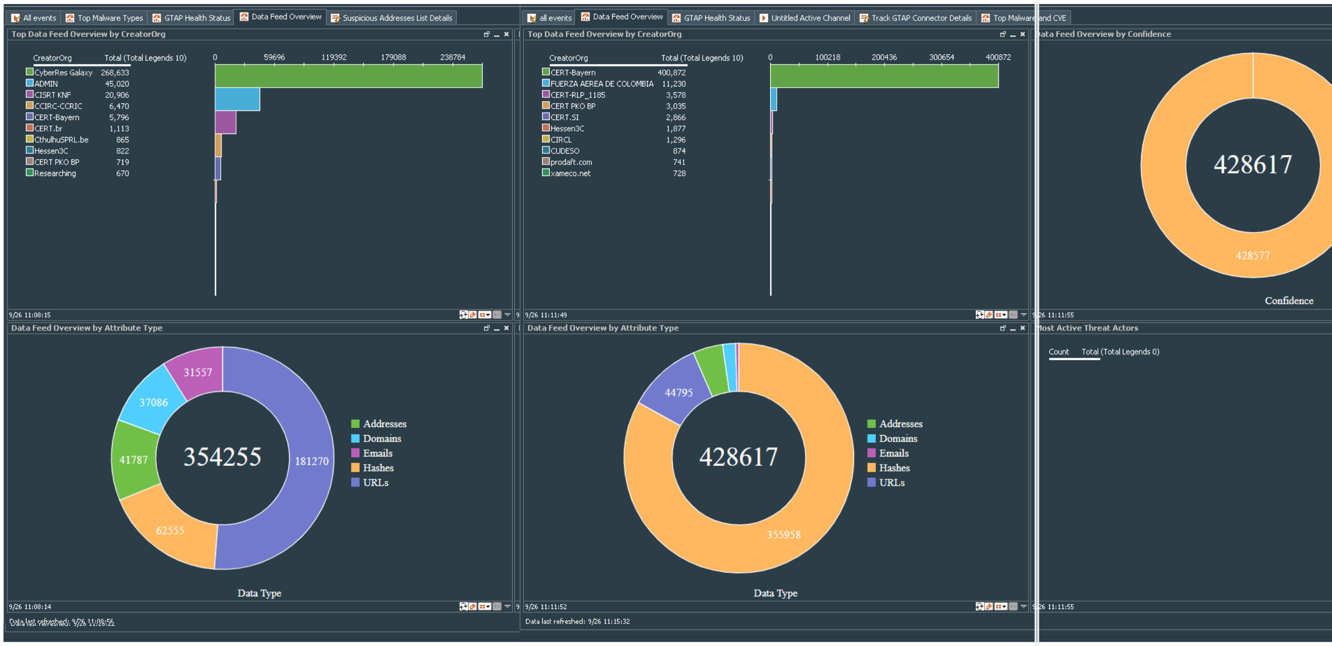
TI Confidence Details Dashboard for ATAP Plus	TI Confidence Details Dashboard for ATAP Basic

This dashboard has the following charts:

- **Data Feed Overview by Confidence:** This dashboard displays the level of confidence, and thus the potential for automation and resource savings in your security operations practice. This high level of confidence is a direct indicator for potential false positive rates (wasted resources) and potential for automation (resource savings).
- **Data Feed Overview by High Confidence:** This chart shows total count with high confidence in each TI data feed, which are stored in five active lists (address, domain, hash, email, and URL).
- **Data Feed Overview by Medium Confidence:** This chart shows total count with medium confidence in each TI data feed, which are stored in five active lists (address, domain, hash, email, and URL).
- **Data Feed Overview by Low Confidence:** This chart shows total count with low confidence in each TI data feed, which are stored in five active lists (address, domain, hash, email, and URL).

Data Feed Overview

To access the Data Feed Overview dashboard, go to **All Dashboards** > **ArcSight Foundation** > **Threat Intelligence Platform** >**Data Feed Overview**.



CreatorOrg	Total (Total Legends 10)
CyberRes Galaxy	268,633
ADMIN	45,020
CISRT KNF	20,906
CCIRC-CCRIC	6,470
CERT-Bayern	5,796
CERT.br	1,113
CthulhuSPRL.be	865
Hessen3C	822
CERT PKO BP	719
Researching	670

CreatorOrg	Total (Total Legends 10)
CERT-Bayern	400,872
FUERZA AEREA DE COLOMBIA	11,230
CERT-RLP_1185	3,578
CERT PKO BP	3,035
CERT.SI	2,866
Hessen3C	1,877
CIRCL	1,296
CUDESO	874
prodaft.com	741
xameco.net	728

Data Feed Overview Dashboard for ATAP Plus	**Data Feed Overview Dashboard for ATAP Basic**

This dashboard contains the following charts:

- **Data Feed Overview by Attribute Type:** The amount of indicators that are deliver by indicator type. This gives your Security Operations personal a good insight into what are most prevalent types of indicators found in our research activities. A higher count will also increase the number of highly confident indicators usable for automation.

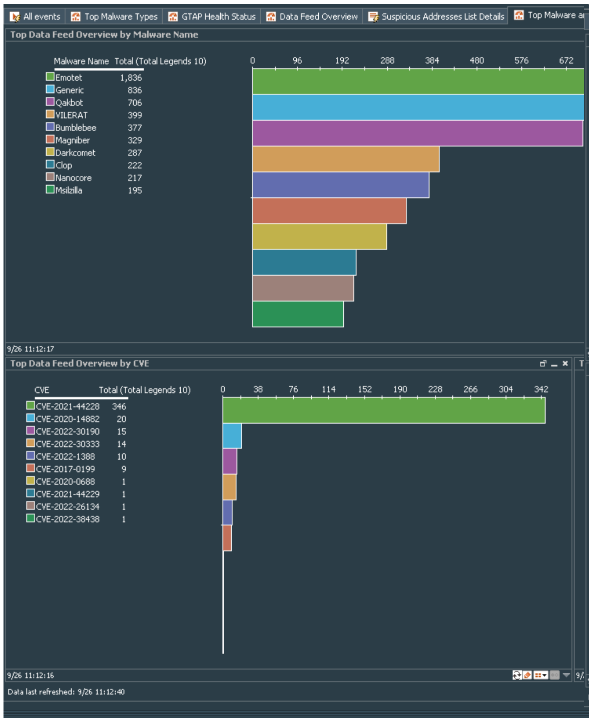
  From the relation between indicator types you can see where the "low hanging fruits" might be, when it comes to automated mitigation with certain types of backend ACL systems.

- **Most Active Threat Actors:** If your Threat Intelligence program collected intelligence about an actor, relevant for your industry in your region, this chart gives you a piece of context on how active that actor is in general. High level of activity of an actor relevant for you, kind of increases your overall threat condition. It could be used as a booster to your evaluation of risk in SIEM.
- **Data Feed overview by CreatorOrg:** You directly see the additional value you get through the subscription into ATAP Plus. Everything published by "Creator Organization" ArcSight would be missing without ATAP Plus.
- **Data Feed Overview by Confidence:** It displays the level of confidence, and thus the potential for automation and resource savings in your security operations practice are much better in the curated only feed (middle donut is for ArcSight Curated TI Feed/ATAP Plus Only). This high level of confidence is a direct indicator for potential

false positive rates (wasted resources) and potential for automation (resource savings).

Top Malware and CVE

To access the Top Malware and CVE dashboard, go to **All Dashboards** > **ArcSight Foundation** > **Threat Intelligence Platform** > **Top Malware and CVE**.



Top Data Feed Overview by Malware Name

Malware Name	Total (Total Legends 10)
🟩 Emotet	1,836
🟦 Generic	836
🟪 Qakbot	706
🟧 VILERAT	399
🟦 Bumblebee	377
🟥 Magniber	329
🟨 Darkcomet	287
🟦 Clop	222
🟫 Nanocore	217
🟩 Msilzilla	195

9/26 11:12:17

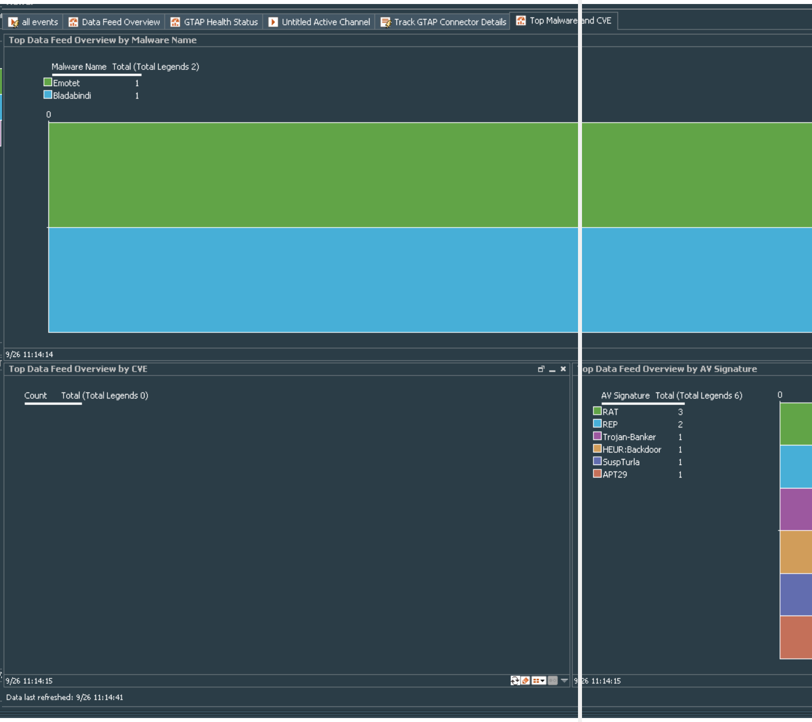
Top Data Feed Overview by CVE

CVE	Total (Total Legends 10)
🟩 CVE-2021-44228	346
🟦 CVE-2020-14882	20
🟪 CVE-2022-30190	15
🟧 CVE-2022-30333	14
🟦 CVE-2022-1388	10
🟥 CVE-2017-0199	9
🟨 CVE-2020-0688	1
🟦 CVE-2021-44229	1
🟫 CVE-2022-26134	1
🟩 CVE-2022-38438	1

9/26 11:12:16

Data last refreshed: 9/26 11:12:40

Top Malware and CVE Overview dashboard for ATAP Plus



Top Data Feed Overview by Malware Name

Malware Name	Total (Total Legends 2)
🟩 Emotet	1
🟦 Bladabindi	1

9/26 11:14:14

Top Data Feed Overview by CVE

Count	Total (Total Legends 0)

9/26 11:14:15

op Data Feed Overview by AV Signature

AV Signature	Total (Total Legends 6)
🟩 RAT	3
🟦 REP	2
🟪 Trojan-Banker	1
🟧 HEUR:Backdoor	1
🟦 SuspTurla	1
🟥 APT29	1

9/26 11:14:15

Data last refreshed: 9/26 11:14:41

Top Malware and CVE Overview dashboard for ATAP Basic

This dashboard has the following charts:

Top Data Feed Overview by Malware Name: The indicators evaluate particular malware names as very active. What it means is that if you are missing these malwares in your AV protection layer, that is a high risk for your environment. Malware names with a high degree of activity is more likely to hit you and must be taken care of specifically.

Combining that information with AV Update information gives you a risk indicator of "Exposedness" which can trigger priorities in particular host activity monitoring or AV mitigation activity.

Top Data Feed Overview by AV Signature:

Similar to the above, AV signature can be used as an indicator of how critical particular a missing AV updates are or findings of a particular type can be. Combine that information with AV status information to drive "Risk Conditions" and TLP status on your SOC screen.

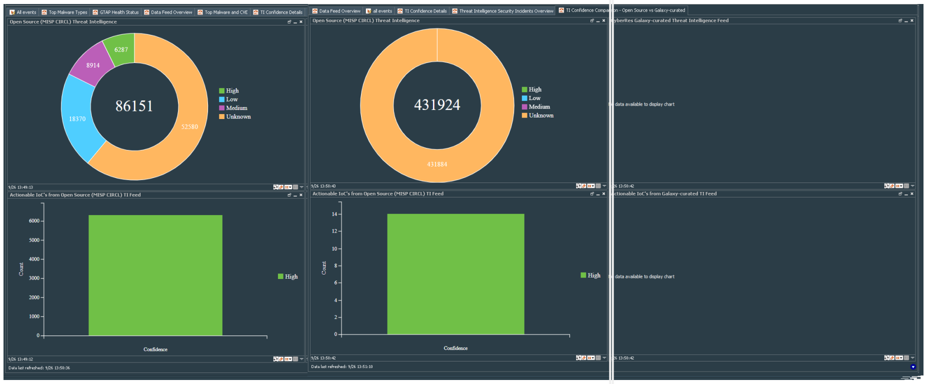
Top Data Feed Overview by CVE:

Activity in these feeds by using particular CVEs gives you prioritization for your vulnerability management teams. The findings of any particular very highly active CVEs are more likely to hit you then CVEs with lower number of origins (according to the threat feed).

TI Confidence Comparison - Open Source vs ArcSight-curated

This chart displays the level of confidence, and thus the potential for automation and resource savings in your security operations practice are much better in the curated only feed (middle donut - ArcSight Curated TI Feed/ATAP Plus Only). This high level of confidence is a direct indicator for potential false positive rates (wasted resources) and potential for automation (resource savings). Open source feeds, due to their nature and how they are created and delivered, have a much higher level of ambiguity and higher level of manual rework in security operations teams.

To access the TI Confidence Comparison - Open Source vs ArcSight-curated dashboard, go to **All Dashboards** > **ArcSight Foundation** > **Threat Intelligence Platform** > **TI Confidence Comparison - Open Source vs ArcSight-curated**.

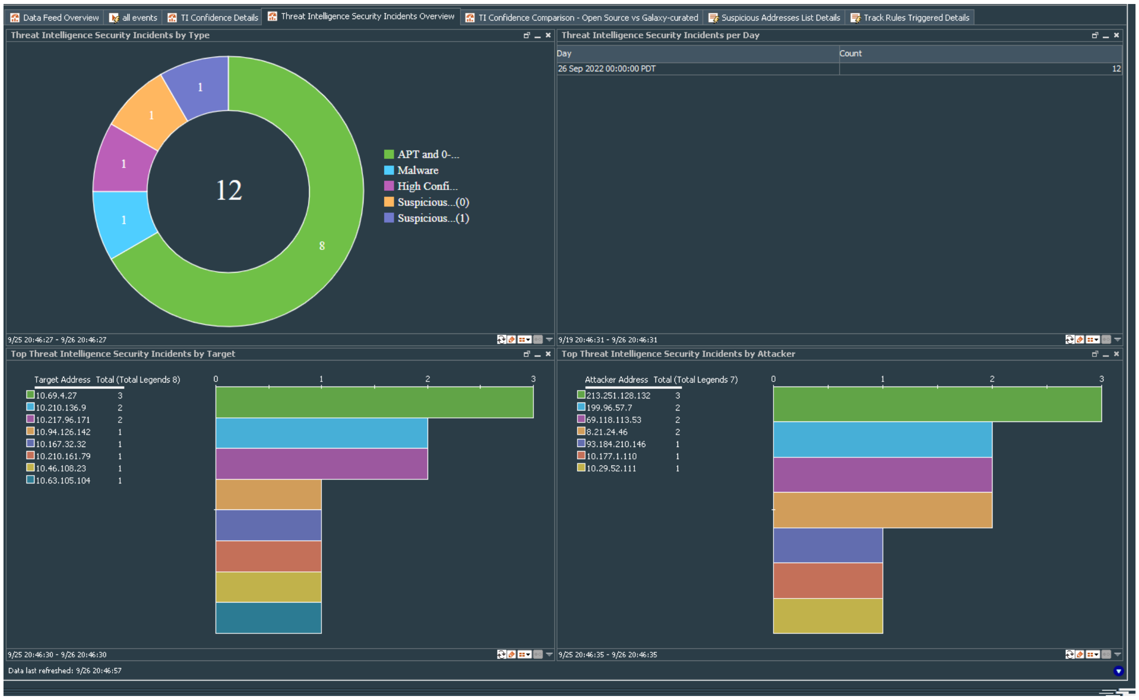

All events
Top Malware Types
GTAP Health Status
Data Feed Overview
Top Malware and CVE
TI Confidence Details
Open Source (MISP CIRCL) Threat Intelligence
6287
8914
18370
52580
86151
High
Low
Medium
Unknown
9/26 13:49:13
Actionable IoC's from Open Source (MISP CIRCL) TI Feed
6000
5000
4000
3000
2000
1000
0
Count
Confidence
High
9/26 13:49:12
Data last refreshed: 9/26 13:50:36
Data Feed Overview
all events
TI Confidence Details
Threat Intelligence Security Incidents Overview
TI Confidence Comparison - Open Source vs Galaxy-curated
Open Source (MISP CIRCL) Threat Intelligence
431924
431884
High
Low
Medium
Unknown
9/26 13:50:43
Actionable IoC's from Open Source (MISP CIRCL) TI Feed
14
12
10
8
6
4
2
0
Count
Confidence
High
9/26 13:50:42
Data last refreshed: 9/26 13:51:10
CyberRes Galaxy-curated Threat Intelligence Feed
No data available to display chart
9/26 13:50:42
Actionable IoC's from Galaxy-curated TI Feed
No data available to display chart
9/26 13:50:42

Comparison for ATAP Plus	**Comparison for ATAP Basic**

Threat Intelligence Security Incidents Overview

This dashboard provides charts, which display an overview of threat intelligence alerts by type, alerts per day, alerts by target and alerts by attacker.

To access the Threat Intelligence Overview dashboard, go to **All Dashboards** > **ArcSight Foundation** > **Threat Intelligence Platform** > **Threat Intelligence Security Incidents Overview**.


Data Feed Overview
all events
TI Confidence Details
Threat Intelligence Security Incidents Overview
TI Confidence Comparison - Open Source vs Galaxy-curated
Suspicious Addresses List Details
Track Rules Triggered Details
12
8
1
1
1
1
APT and 0-...
Malware
High Confi...
Suspicious...(0)
Suspicious...(1)
0
1
2
3

Threat Intelligence Security Incidents by Type

9/25 20:46:27 - 9/26 20:46:27

Threat Intelligence Security Incidents per Day

Day	Count
26 Sep 2022 00:00:00 PDT	12

9/19 20:46:31 - 9/26 20:46:31

Top Threat Intelligence Security Incidents by Target

Target Address	Total (Total Legends 8)
🟩10.69.4.27	3
🟦10.210.136.9	2
🟪10.217.96.171	2
🟧10.94.126.142	1
🟦10.167.32.32	1
🟥10.210.161.79	1
🟨10.46.108.23	1
🟦10.63.105.104	1

9/25 20:46:30 - 9/26 20:46:30

Top Threat Intelligence Security Incidents by Attacker

Attacker Address	Total (Total Legends 7)
🟩213.251.128.132	3
🟦199.96.57.7	2
🟪69.118.113.53	2
🟧8.21.24.46	2
🟦93.184.210.146	1
🟥10.177.1.110	1
🟨10.29.52.111	1

9/25 20:46:35 - 9/26 20:46:35

Data last refreshed: 9/26 20:46:57

This dashboard contains the following charts:

- **Threat Intelligence Alerts by Type:** Threat Intelligence security alerts counts grouped by attack type, such as Malware, Phishing, High Confidence etc.
- **Threat Intelligence Alerts per Day:** This view provides an indication of how intense ATAP's monitoring techniques trigger based on TI information. If filtered on high confident TI records only, this can give a very good indicator of whether the customer is under attack if the number of hits is extraordinarily high. Ideally, if you see a low and constant number in here, it is nevertheless a good enough reason to investigate the triggers.
- **Threat Intelligence Alerts by Target:** Hosts, which are particularly exposed by alerts enriched by our feeds. In a ATAP Plus only environment, this is a very strong indicator

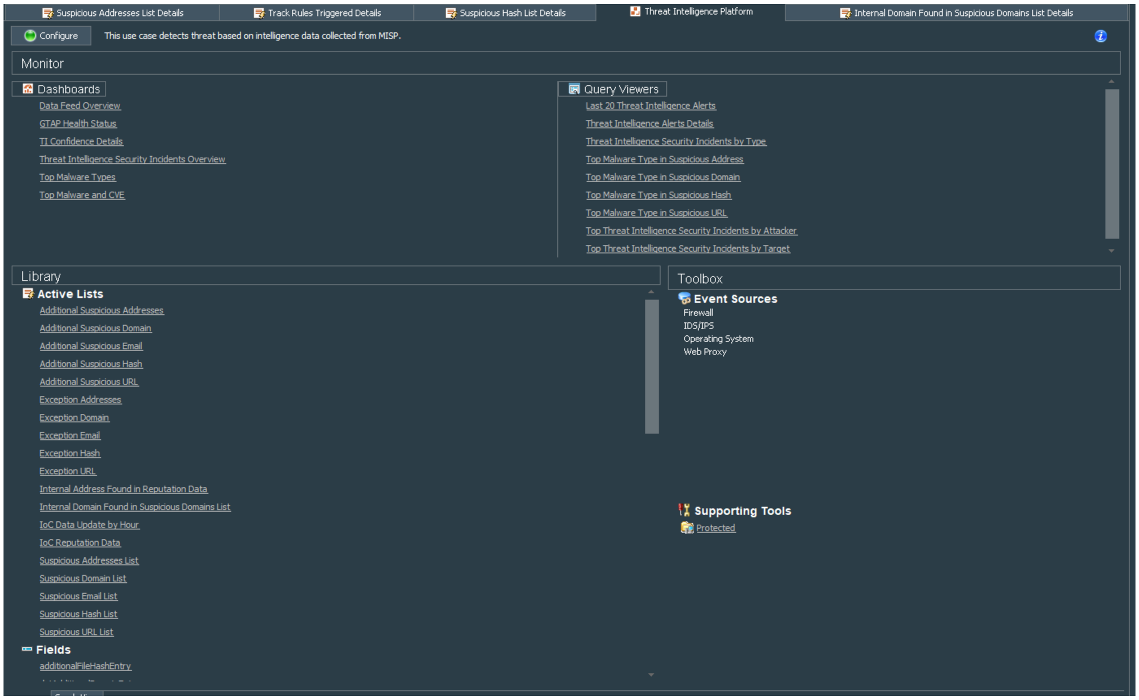
for "deeper monitoring of hosts" and might trigger forensic analytics for the top hosts in that list.

Notifications to host owners and service owners for which this hosts contribute, are good practices with those systems being effected.

- **Threat Intelligence Alerts by Attacker:** Threat Intelligence security alerts counts grouped by attacker addresses.

Use Cases

Use cases provide most important resource in one place. You can also access the dashboard by clicking the **Use Cases** tab.


Suspicious Addresses List Details
Track Rules Triggered Details
Suspicious Hash List Details
Threat Intelligence Platform
Internal Domain Found in Suspicious Domains List Details
Configure

This use case detects threat based on intelligence data collected from MISP.

Monitor

Dashboards

- Data Feed Overview
- GTAP Health Status
- TI Confidence Details
- Threat Intelligence Security Incidents Overview
- Top Malware Types
- Top Malware and CVE

Query Viewers

- Last 20 Threat Intelligence Alerts
- Threat Intelligence Alerts Details
- Threat Intelligence Security Incidents by Type
- Top Malware Type in Suspicious Address
- Top Malware Type in Suspicious Domain
- Top Malware Type in Suspicious Hash
- Top Malware Type in Suspicious URL
- Top Threat Intelligence Security Incidents by Attacker
- Top Threat Intelligence Security Incidents by Target

Library

Active Lists

- Additional Suspicious Addresses
- Additional Suspicious Domain
- Additional Suspicious Email
- Additional Suspicious Hash
- Additional Suspicious URL
- Exception Addresses
- Exception Domain
- Exception Email
- Exception Hash
- Exception URL
- Internal Address Found in Reputation Data
- Internal Domain Found in Suspicious Domains List
- IoC Data Update by Hour
- IoC Reputation Data
- Suspicious Addresses List
- Suspicious Domain List
- Suspicious Email List
- Suspicious Hash List
- Suspicious URL List

Fields

- additionalFileHashEntry

Toolbox

Event Sources

- Firewall
- IDS/IPS
- Operating System
- Web Proxy

Supporting Tools

- Protected

Installing ESM Default Content

To use dashboards and active lists, you must install Threat Intelligence Platform 4.2, which is an ESM out of the box content package. This package contains default content to monitor the ATAP connector.

For a fresh installation of Content Package 4.2, see Installing Default Content Package.

If you already have 3.x version of default content, you cannot directly upgrade the package to 4.x. For more information, see Upgrading Default Content Package From Version 3.x to Version 4.x.

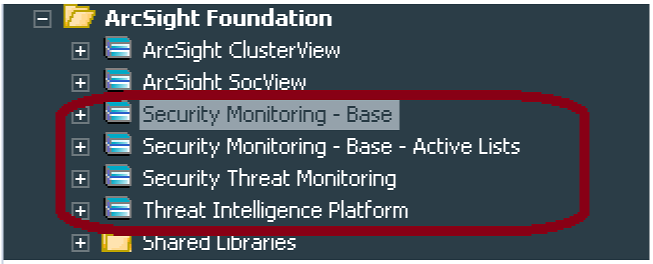
Prerequisites

- ArcSight ESM 7.2 or later.
- Download ESM default content package from Marketplace.

Upgrading Default Content Package From Version 3.x to Version 4.x

To upgrade Default Content Package From Version 3.x to Version 4.x:

1. Log in to the ESM Console.
2. Uninstall and delete the **Threat Intelligence Platform** package:

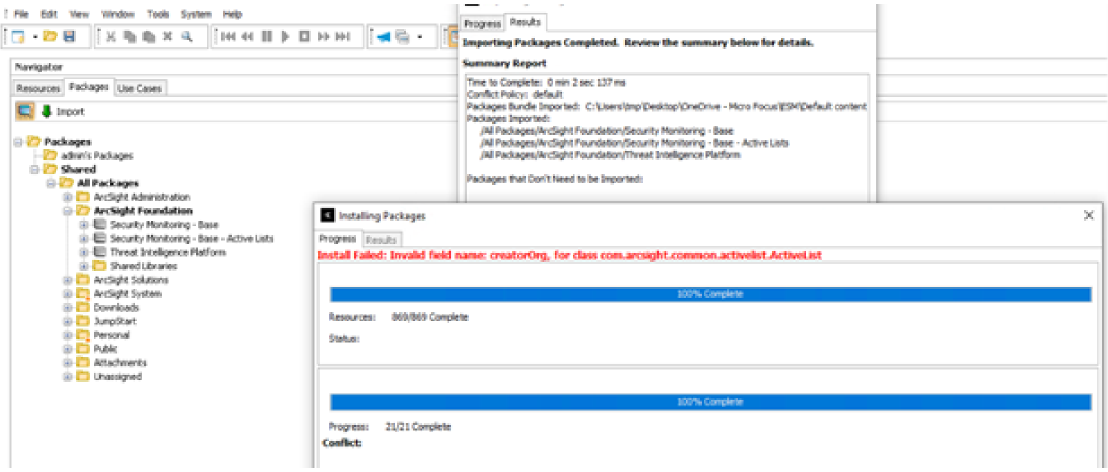
   
   ArcSight Foundation
   ArcSight ClusterView
   ArcSight SocView
   Security Monitoring - Base
   Security Monitoring - Base - Active Lists
   Security Threat Monitoring
   Threat Intelligence Platform
   Shared Libraries

   Note: It is not mandatory to delete the other three packages.
3. Make sure that all resources in **ArSight Foundation** > **Threat Intelligence Platform** folder, including the Active Lists are deleted.
4. Restart the ESM manager:

```
/opt/arcsight/services/init.d/arcsight_services stop manager
```

```
/opt/arcsight/services/init.d/arcsight_services start manager
```

Note: If you do not restart the manager, the following error message will be displayed during installation:



Importing Packages Completed. Review the summary below for details.

Summary Report

```
Time to Complete: 0 min 2 sec 137 ms
Conflict Policy: default
Packages Bundle Imported: C:\Users\tmp\Desktop\OneDrive - Micro Focus\ESM\Default content
Packages Imported:
    /All Packages/ArcSight Foundation/Security Monitoring - Base
    /All Packages/ArcSight Foundation/Security Monitoring - Base - Active Lists
    /All Packages/ArcSight Foundation/Threat Intelligence Platform

Packages that Don't Need to be Imported:
```

```
Install Failed: Invalid field name: creatorOrg, for class com.arcsight.common.activelist.ActiveList

100% Complete
Resources:    869/869 Complete
Status:

100% Complete
Progress:    21/21 Complete
Conflict:
```

5. Complete the steps in the Installing the Default Content Package section.

Installing the Default Content Package

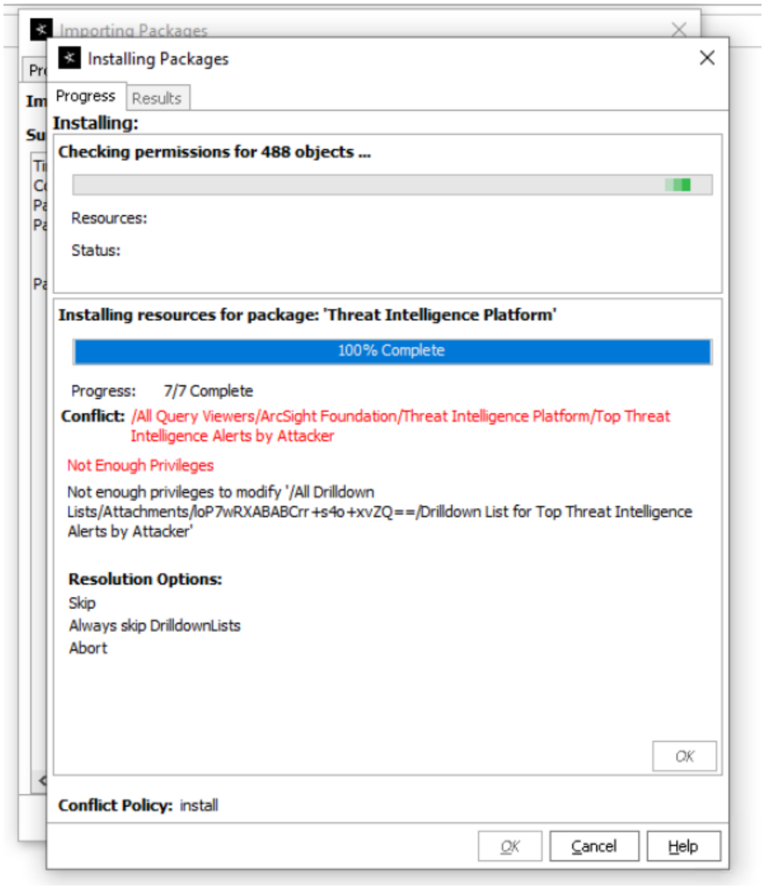
To install the package, complete the following steps:

1. Go to the ArcSight Console.
2. Click **Packages**.
3. Click **Import**.
4. Select the package *.arb* file from the *.zip* file.

   The .zip file contains one Security Threat Monitoring package, and one Threat Intelligence Platform package.
5. Follow the prompts to import and install the packages.

   If you were upgrading from a previous version of content package and did not delete the three packages that were not mandatory to be deleted, the Threat Intelligence Platform package will update two Base packages only. Right-click **Threat Intelligence Platform** to finish the installation.

   If you get the following error message during installation, Click **Always skip DrilldownLists**, to continue with the installation.



Installing:

Checking permissions for 488 objects ...

Resources:

Status:

Installing resources for package: 'Threat Intelligence Platform'

100% Complete

Progress: 7/7 Complete

Conflict: /All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Top Threat Intelligence Alerts by Attacker

Not Enough Privileges

Not enough privileges to modify '/All Drilldown Lists/Attachments/loP7wRXABABCrr+s4o+xvZQ==/Drilldown List for Top Threat Intelligence Alerts by Attacker'

Resolution Options:

Skip
Always skip DrilldownLists
Abort

Conflict Policy: install

Note: If you clicked **Always Skip DrilldownLists** during installation, some drilldown functions might not work properly.

Installing and Configuring the Connector

The following sections provide the steps to install and configure the Connector. It is recommended not to install the Connector on the same machine as ESM.

If you have ArcSight subscription, then select either **ArcSight Threat Acceleration Program Plus** or **ArcSight Threat Acceleration Program Basic**. However,

ATAP Plus is a subscription based license. Before you proceed with this option, make sure that you have purchased the license and have the API key details.

If you have already have an MISP license and want to continue with that, then use the **Custom MISP Instance** option.

Note: Use a non-root account to install the Connector.

Preparing to Install the Connector

Before installing the connector, verify that **ESM** and **Console** have already been installed correctly.

For complete product information, refer to the Administrator's Guide to ArcSight Platform guide, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the ArcSight Management Center Administrator's Guide for instructions.

Note: If you are an existing user who have been using the **ArcSight Threat Acceleration Basic** version, and want to upgrade to the **ArcSight Threat Acceleration Plus** version, then you must purchase the license, get the valid API Key, and reinstall the connector using the Configuring parameters for ArcSight Threat Acceleration Plus option.

Important: It is recommended to clear the data in the Active List.

Before installing the Connector, ensure that you have the following:

- Local access to the machine where you want to install the Connector.
- Additional 2GB memory if the connector is running in a standalone mode.
- Local administrator access to the machine on which the connector will be installed.
- Refer to the Technical Requirements Guide for supported platforms.

- The machine, on which the connector will be installed, has external access over the Internet to any system over port 443 and connectivity to the ESM machine over port 8443 (default) or the configured port if the default was not used.
- ESM IP address, port, administrator user name, and password.
- Make sure that the ESM default content package is installed and is available in **All Packages > ArcSight Foundation > Threat Intelligence Platform**. For more information, see Installing ESM Default Content.
- If you had installed the ArcSight Model Import Connector for MISP on the machine before, then clear the Active Lists before proceeding to install the ArcSight Threat Acceleration Program Connector.

Downloading the Certificates

Perform the following steps to download the Threatfeed Cyberres certificate, if you are planning to install the connector in FIPS mode in either **ArcSight Threat Acceleration Program Plus** or **ArcSight Threat Acceleration Program Basic**:

1. Open a browser and enter the Threatfeed Cyberres URL.
2. Click the **Lock** symbol in the browser next to where you have entered the URL.
3. Click **Connection secure**.
4. Click **More information**.
5. Click **View Certificate** under the **Security** tab. This will redirect you to a new tab in the browser.
6. In the **threatfeed.cyberres.com** > **Miscellaneous** section, click **PEM (cert)** to download the certificate.

Preparing the Communication Requirements

You must ensure a communication between the ATAP Connector and the internet, and between the ATAP Connector and a single ArcSight ESM instance, before using ATAP Threat feeds.

For Internet Connection:

- Ensure that your connector can communicate to API endpoint at Threatfeed Cyberres at standard HTTPS port 443.
- Ensure that your connector can also communicate to all addresses that can be resolved for AWS CloudFront DNS. These addresses are listed under List Cloudfront-IP and must be allowed from your connector.

- If your organization have communication policies based on DNS names, then ensure that your connector can communicate to the current CloudFront DNS. Since this address is dynamic, so you must verify the current address by accessing Threatfeed Cyberres in a browser and check the address to which your request is forwarded.

For Backend Connection:

Ensure your connector can connect to single ESM instance where the TI information is sent on port <ESM-Address>:8443

If you configure your connector for ATAP Basic, then you must have all the Internet communication settings as described. If you have configured the ATAP connector for Plus, you would need only Threatfeed Cyberres.

> **Note:** Since the ATAP Plus feed includes the ATAP Basic feed at current state, so you also need the ATAP Basic firewall communication set up correctly, in order to make the ATAP Plus feed work.

Installing and Configuring ATAP Plus

This is a subscription based service. Before you proceed with this option, make sure that you have purchased the license and have the API key details.

Follow the instructions in the wizard to install the core software.

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. (Conditional) If you are planning to install the connector in a FIPS-enabled environment, then perform the following actions:
    a. Exit the installation wizard after the installation of core software completes.

    b. Import the exported certificate into the connector framework FIPS keystore, using a command similar to the following from the current directory:

    ```
     ./jre/bin/keytool -importcert -file /opt/certificate.cer -keystore
    $ARCSIGHT_HOME/current/user/agent/fips/bcfips_ks -storepass
    changeit -storetype BCFKS -providername BCFIPS -providerclass
    org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -
    providerpath $ARCSIGHT_HOME/current/lib/agent/fips/bc-fips-
    1.0.2.jar -J-Djava.security.egd=file:/dev/urandom -alias
    mispInstance
    ```

    Specify the path to the folder where you have downloaded the certificate file by using the Downloading the Certificates procedure.

   c. Use the runagentsetup file in the *./current/bin/* to proceed with the connector installation.

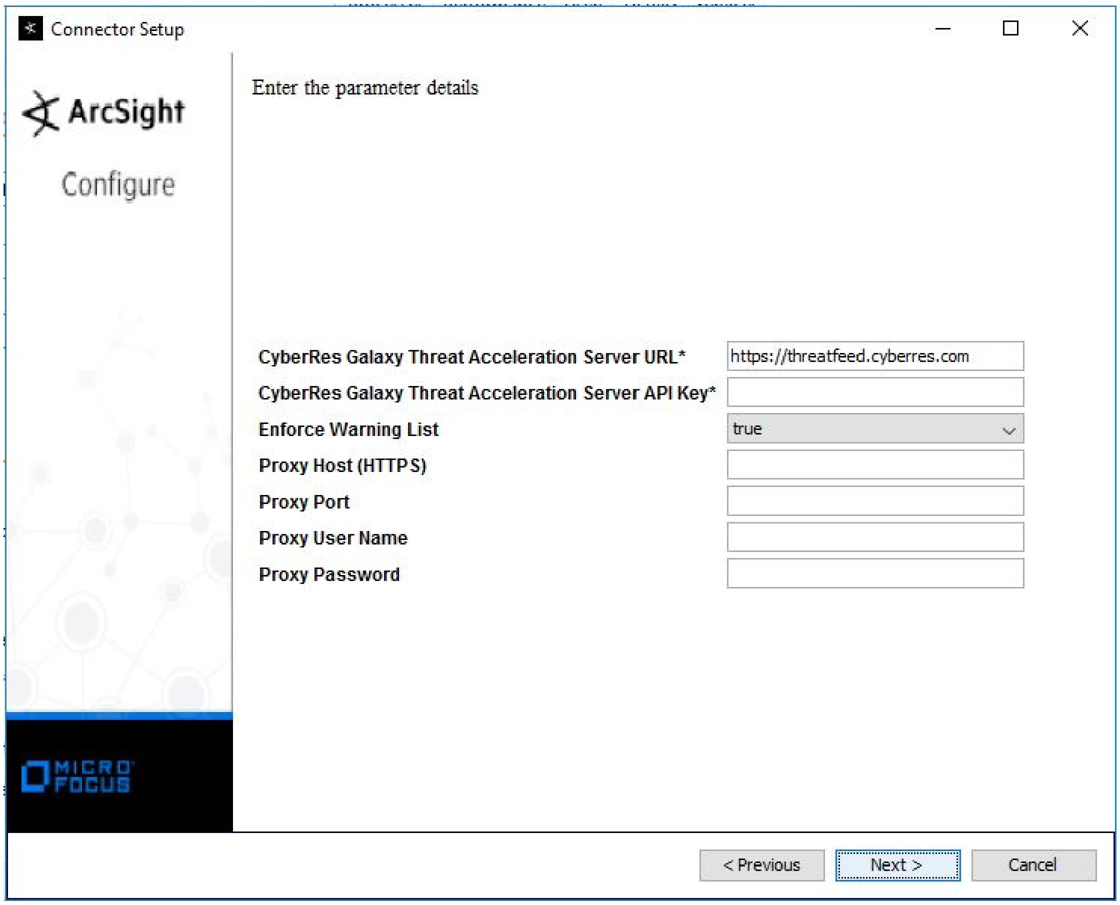
4. Specify the relevant Global Parameters, when prompted. To install the connector in a FIPS-enabled environment, select Enabled for FIPS Mode.

   > **Note:** Make sure that the FIPS Mode configuration matches with the FIPS mode configuration in the ESM application. For example, if the FIPS mode is enable in ESM, then FIPS mode must be enable in Connectors as well.

5. Select **ArcSight Acceleration Program Model ImportConnector** and click **Next**.

6. Select the **ArcSight Threat Acceleration Program Plus** option.

7. Specify the following details:



Enter the parameter details

CyberRes Galaxy Threat Acceleration Server URL*	https://threatfeed.cyberres.com
CyberRes Galaxy Threat Acceleration Server API Key*	
Enforce Warning List	true
Proxy Host (HTTPS)	
Proxy Port	
Proxy User Name	
Proxy Password	

Parameter Name	Description
ArcSight Threat Acceleration Server URL	Specify threatfeed.cyberres.com as the URL for the ArcSight Threat Acceleration server instance.
ArcSight Threat Acceleration Server API Key	Specify the API Key that you received after purchasing the license.
Enforce Warning List	Select **True**. **Note:** misp-warninglists are lists of well-known indicators that can be associated with potential false positives, errors, or mistakes. The enforceWarninglist parameter of MISP restSearch can be used to exclude attributes that have a warninglist hit.
Proxy Host (HTTPS)	Specify a URL of the proxy host without https://. For example: web-proxy.am.example.net.
Proxy Port	Enter the port number for the proxy.
Proxy User Name	Enter the name of the proxy user.
Proxy Password	Enter the password of the proxy user. This value is populated when the proxy requires an authentication and if you have specified a proxy user name.

8. Click **Next**, then proceed to complete the installation.

> **Note**: If you get the error message "The parameters are invalid, Do you want to Continue", click **No**. Make sure that you have entered the correct Access Key. If you do not have a valid access key, then purchase the license and get a valid Access Key before proceeding to ArcSight Threat Acceleration Plus.

Installing and Configuring ATAP Basic

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. (Conditional) If you are planning to install the connector in a FIPS-enabled environment, then perform the following actions:

   a. Exit the installation wizard after the installation of core software completes.

   b. Import the exported certificate into the connector framework FIPS keystore, using a command similar to the following from the current directory:

      ```
      ./jre/bin/keytool -importcert -file /opt/certificate.cer -keystore
      $ARCSIGHT_HOME/current/user/agent/fips/bcfips_ks -storepass
      changeit -storetype BCFKS -providername BCFIPS -providerclass
      org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -
      providerpath $ARCSIGHT_HOME/current/lib/agent/fips/bc-fips-
      1.0.2.jar -J-Djava.security.egd=file:/dev/urandom -alias
      mispInstance
      ```

      Specify the path to the folder where you have downloaded the certificate file by using the Downloading the Certificates procedure.

   c. Use the runagentsetup file in the *./current/bin/* to proceed with the connector installation.

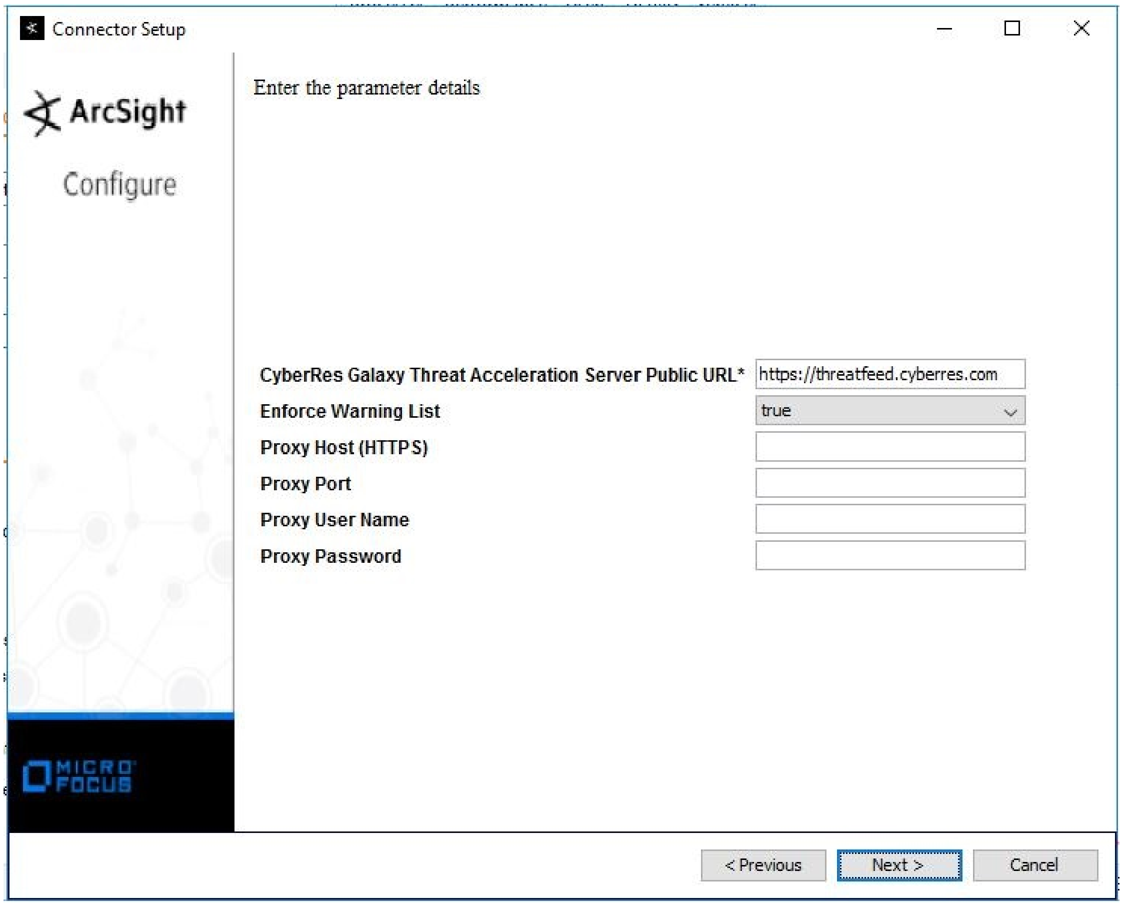
4. Specify the relevant Global Parameters, when prompted. To install the connector in a FIPS-enabled environment, select Enabled for FIPS Mode.

   > **Note:** Make sure that the FIPS Mode configuration matches with the FIPS mode configuration in the ESM application. For example, if the FIPS mode is enable in ESM, then FIPS mode must be enable in Connectors as well.

5. Select **ArcSight Acceleration Program SmartConnector** and click **Next**.

6. Select the **ArcSight Threat Acceleration Program Basic** option.

7. Specify the following details:



Enter the parameter details

CyberRes Galaxy Threat Acceleration Server Public URL* https://threatfeed.cyberres.com
Enforce Warning List true
Proxy Host (HTTPS)
Proxy Port
Proxy User Name
Proxy Password

Parameter Name	Description
ArcSight Threat Server Public URL	Specify threatfeed.cyberres.com as the URL for the ArcSight Threat Acceleration Server instance.

8. Click **Next**, then proceed to complete the installation.

Installing and Configuring ATAP Custom

You can configure only one destination per installation.

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. (Conditional) If you are planning to install the connector in a FIPS-enabled environment, then perform the following actions:
   a. Exit the installation wizard.
   b. Download the MISP instance certificate:

> **Note:** You must export the MISP instance certificate from the browser as a DER encoded binary x.509 (.CER) file.

i. Open a browser and enter the URL of the MISP server instance.

ii. **Specify** the email and password.

iii. Click the **Lock** symbol in the browser next to where you have entered the URL.

iv. Click **Connection secure**.

v. Click **Certificate is valid** to download and **Save** the certificate.

> **Note**: It displays the date and validity of the certificate, which is for one year.

vi. Navigate to **Details**, then click **Copy to file** by clicking the option to save it in your local.

vii. Click **Next**, in the certificate export wizard.

viii. The **x.CER** format is automatically selected. Click **Next**.

ix. Add the **File Name** and the **Path** where you want to download the certificate.

x. Click **Save**.

xi. Click **Finish**.

xii. Click **OK** to successfully export the certificate.

c. Import the exported certificate into the connector framework FIPS keystore, using a command similar to the following from the current directory:

```
./jre/bin/keytool -importcert -file /opt/certificate.cer -keystore
$ARCSIGHT_HOME/current/user/agent/fips/bcfips_ks -storepass
changeit -storetype BCFKS -providername BCFIPS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -
providerpath $ARCSIGHT_HOME/current/lib/agent/fips/bc-fips-
1.0.2.jar -J-Djava.security.egd=file:/dev/urandom -alias
mispInstance
```

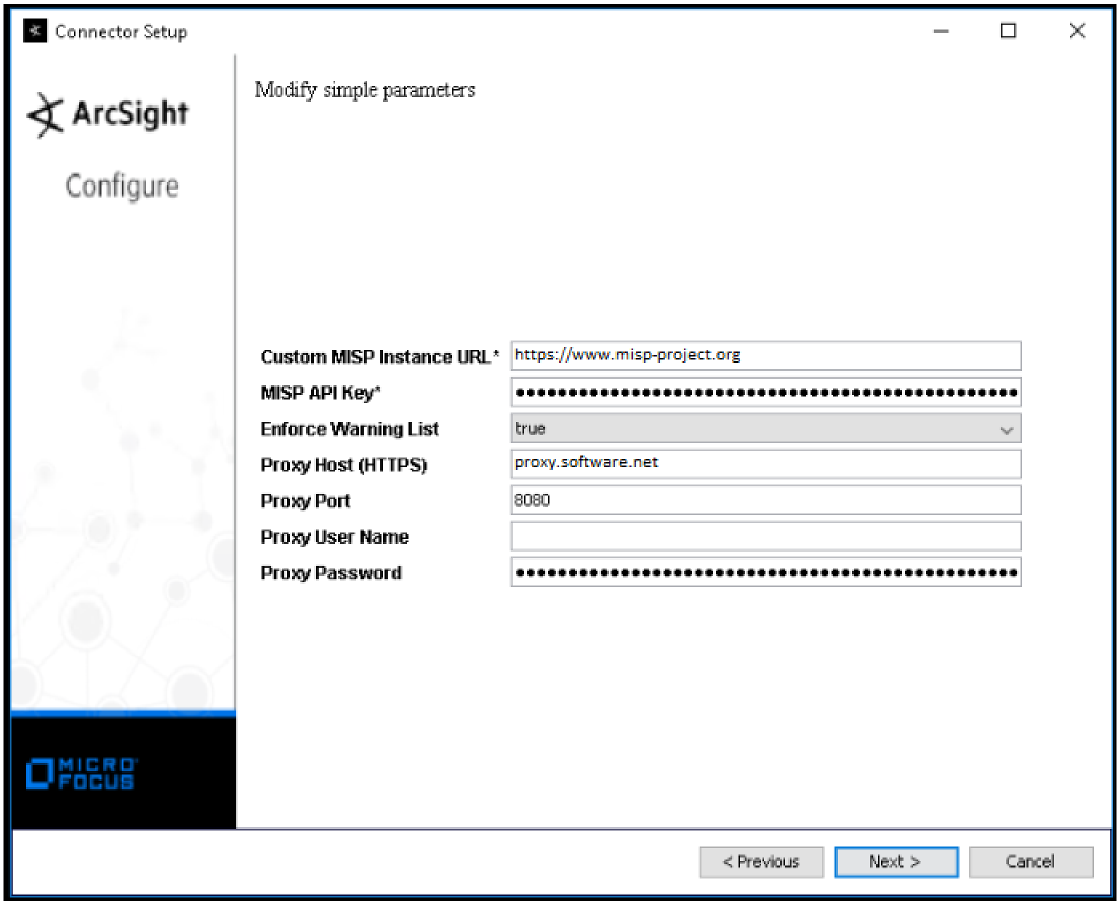
Specify the path to the folder where you have downloaded the certificate file in Step a.

d. Use the runagentsetup file in the *./current/bin/* to proceed with the connector installation.

4. Specify the relevant Global Parameters, when prompted. To install the connector in a FIPS-enabled environment, select Enabled for FIPS Mode.

> **Note:** Make sure that the FIPS Mode configuration matches with the FIPS mode configuration in the ESM application. For example, if the FIPS mode is enable in ESM, then FIPS mode must be enable in Connectors as well.

5. Select **ArcSight Acceleration Program SmartConnector** and click **Next**.
6. Select the **Arcsight Threat Acceleration Custom** option.
7. Specify the following details:



Modify simple parameters

Custom MISP Instance URL* https://www.misp-project.org
MISP API Key* ••
Enforce Warning List true
Proxy Host (HTTPS) proxy.software.net
Proxy Port 8080
Proxy User Name
Proxy Password ••

Parameter Name	Description
Custom MISP Instance URL	Specify the URL for your MISP instance.
MISP API Key	Specify the API Key for your MISP instance.

8. Click **Next**, then proceed to complete the installation.

Completing Installation

1. Select **ArcSight Manager (Encrypted)**, then click **Next**.
2. Specify the following destination parameters:

Parameter Name	Description
Manager Hostname	Enter the hostname for Manager.
Manager Port	Enter **8443**.
User	Enter the user name
Password	Enter the password for the user.

3. Click **Next** and enter a **Name** for the connector and a description.
4. Click **Next.**
5. Review the **Add connector Summary** and click **Next**.
6. Select either **Install as a service or Leave as a standalone application as the mode to run the connector** and click **Next**.
7. Increase the Java Heap size.
8. Set up the user in ESM.
9. Start the data import.
10. (Optional) If you have installed the connector in the standalone mode, then run the connector manually.

Advanced Communication Details

ATAP connector configuration for ATAP Plus requires the access to the ArcSight ESM instance and https://threatfeed.cyberresgalaxy.com only.

ATAP connector for ATAP Basic, must have access to the ArcSight ESM instance and internet for using ATAP threat feeds.

To have a seamless internet connectivity, ensure:

- The connector can communicate with the API endpoint at https://threatfeed.cyberres.com, on standard https port 443.
- The connector must allow and communicate to all addresses that can be resolved for AWS CloudFront DNS. The list of the addresses are available at https://d7uri8nf7uskq.cloudfront.net/tools/list-cloudfront-ips.
- If the AWS CloudFront infrastructure changes for AWS operational reasons, see the AWS documentation to verify current CloudFront IP addresses.
- The connector can communicate to the current CloudFront DNS, if your organization follows DNS names based communication policies. As this address is dynamic, you must verify the current address by opening https://threatfeed.cyberres.com/feed/manifest.json in a browser and check the address to which your request gets forwarded.

To have a seamless backend connectivity, ensure:

- The connector can connect to the ESM instance that it sends TI information to, on the port <ESM-Address>:8443---

> Note: As the ATAP Plus feed also includes the ATAP Basic feed at current state, the ATAP Basic firewall communication is also required for ATAP Plus feed.

Increasing the Java Heap Size

You can increase the java heap memory for the connector by doing the following:

- If you are running the connector as a **Windows service or Linux daemon**, open the *~../current/user/agent/agent.wrapper.conf* file and set the heap size as follows:

  ```
  #Initial Java Heap Size (in MB)
  ```

  ```
  wrapper.java.initmemory=1024
  ```

  ```
  #Maximum Java Heap Size (in MB)
  ```

  ```
  wrapper.java.maxmemory=4096
  ```

- If you are running the connector in a **Standalone mode**:
  - **Linux:** Create an executable shell script *~/ARCSIGHT_HOME/current/user/agent/setmem.sh*, with the following content:

    ```
    ARCSIGHT_MEMORY_OPTIONS=" -Xms1024m -Xmx4096m"
    ```

  - **Windows:** Create the batch file *$ARCSIGHT_HOME\current\user\agent\setmem.bat* with the following content:

    ```
    SET ARCSIGHT_MEMORY_OPTIONS=" -Xms1024m -Xmx4096m"
    ```

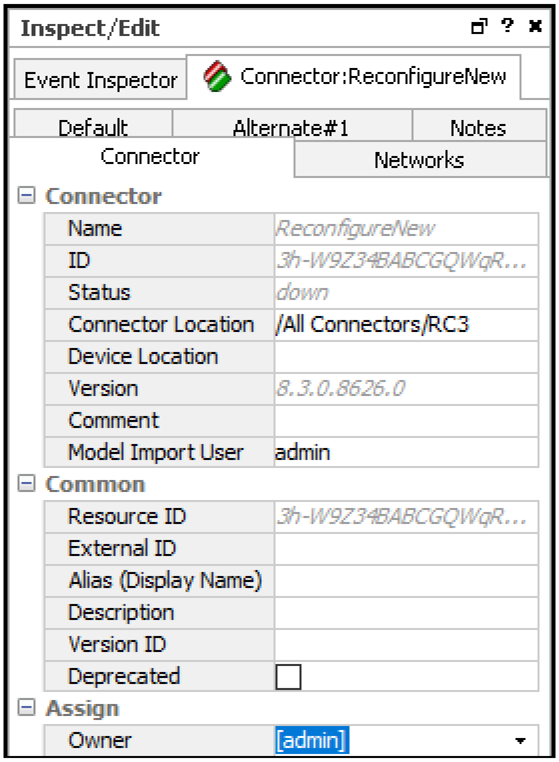
To verify if the connectors are running, select the ArcSight **Console Navigator** in the **Resources** tab, under **Connectors**. If the connector is running, you will see <connector_name> (running) listed. For more information, see Running Connectors.

Setting Up the User in ESM

After installing, configuring, and starting the connector, you must set the user for the connector from the ArcSight Console. Setting the user links the user to the resources, and that user is then treated as the **Creator** of resources. The connector is then run on that user’s behalf.

> **Note**: The user must have console administrative privileges. Else, the import fails.

1. From the ArcSight Console, go to the **Navigator** > **Resources** tab.
2. From **All Connectors**, navigate to your **ArcSight Threat Acceleration Program Connector**.
3. Right-click on the connector and select **Configure**.
4. On the **Inspect/Edit** panel, select the **Connector** tab.
5. Enter **Model Import User** as **Admin** and **Owner** as **Admin**.



Connector

Name	ReconfigureNew
ID	3h-W9Z34BABCGQWqR...
Status	down
Connector Location	/All Connectors/RC3
Device Location	
Version	8.3.0.8626.0
Comment	
Model Import User	admin

Common

Resource ID	3h-W9Z34BABCGQWqR...
External ID	
Alias (Display Name)	
Description	
Version ID	
Deprecated	□

Assign

Owner	[admin]

6. Click **Apply/ OK**.

Starting and Stopping Data Import

By default the connector’s data import capability is not started. You must start the import manually in the ArcSight Console.

> **Note:** Data import needs to be started only once from the ArcSight Console. Unless it is stopped from the ArcSight Console, there is no need to restart the data import.

To start and stop import data for the ATAP Connector:

1. Select the ATAP connector and right-click.
2. Specify the following commands:
    - **To Start:** Select **Send Command > Model Import Connector > Start Import**
    - **To Stop:** Select **Send Command > Model Import Connector > Stop Import**

Configuring the Start Date

When the ATAP Model Import Connector is installed in **ArcSight Threat Acceleration Program Plus** and **ArcSightThreat Acceleration Program Custom** options, it starts retrieving data from a month prior to the date of installation. However, you can configure the connector to retrieve older data as well.

To set data retrieval to a different date, modify the agent.properties as **agent (0).start.date**, then restart the connector.

For **ArcSight Threat Acceleration Program Basic** option, after the connector is installed all the events will be downloaded.

Optimizing Data Transfer by Using a Timer

The time interval between archives sent by the connector to ESM can be controlled by the `buildmodeldelay` property. The default value is 1 minute.

To increase or decrease this time interval, you can add the `buildmodeldelay` property to the file `agent.properties` (located at `$ARCSIGHT_HOME\current\user\agent`). The property `buildmodeldelay` is expressed in milliseconds.

For example, the following property sets the time interval to 10 seconds:

```
agent.component[35].buildmodeldelay=10000
```

Running the Connectors

The Connector can be run in stand-alone mode or as a service, depending on the mode selected during installation.

> **Note:** Before you start the Connector, make sure that ArcSight ESM is up and running.

To verify that a connector is running, you can check the **ArcSight Console Navigator** in the **Resources** tab, under **Connectors**. If the connector is running, you will see <connector_ name> (running) listed.

Running in Standalone Mode

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted.

- To run all Connectors installed in stand-alone mode on a particular host, open a command window, go to the **$ARCSIGHT_HOME\current\bin** directory and run the following command:

```
arcsight connectors
```

- To view the Connector log, read the following file:

```
$ARCSIGHT_HOME/current/logs/agent.log
```

- To stop all Connectors, enter **Ctrl+C** in the command window.

Running as a Windows Service

- To start or stop Connectors installed as services on Windows platforms:
  a. Right-click **My Computer**, then select **Manage** from the **Context** menu.
  b. Expand the **Services and Applications** folder and select **Services**.
  c. Right-click the Connector service name and select **Start** to run the Connector or **Stop** to stop the service.
- To verify that a Connector service has started, view the following file:

```
$ARCSIGHT_HOME/logs/agent.out.wrapper.log
```

- To reconfigure a Connector as a service, open a command window on $ARCSIGHT_ HOME/current/bin and run the following command to start the Connector **Configuration Wizard**:

```
runagentsetup
```

Running Connectors as a UNIX Daemon

> **Note:** When installing the connector as a Linux daemon, run the following command as root and ensure the -u parameter is a non-root user:
>
> ```
> $ARCSIGHT_HOME/current/bin/arcsight agentsvc -i -u user -sn <service_name>
> ```

Connectors installed as a daemon can be started and stopped manually by using platform-specific procedures.

On UNIX systems, when you configure a Connector to run automatically, ArcSight creates a control script in the /etc/init.d directory.

- To start or stop a particular Connector, find the control script and run it with either a start or stop command parameter.

  For example:

  ```
  /etc/init.d/arc_serviceName {start|stop}
  ```

- To verify that a Connector service has started, view the file:

  ```
  $ARCSIGHT_HOME/logs/agent.out.wrapper.log
  ```

- To reconfigure the Connectors as a daemon, run the Connector **Configuration Wizard** again. Open a command window on *$ARCSIGHT_HOME/current/bin* and enter:

  ```
  runagentsetup
  ```

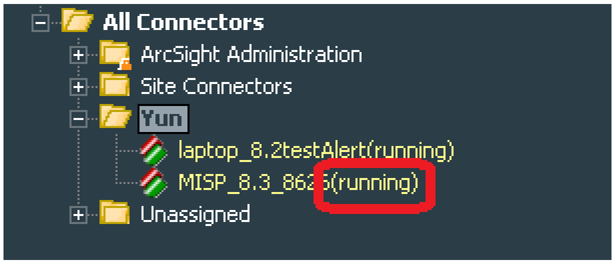
> **Note:** By default, the connector collects events starting from a month prior to the installation day. To start retrieving older events, modify the `start.date` parameter in the `../current/user/agent/agent.properties` file. The format of the field is `YYYY-MM-DD`. The connector can only collect data up to 12 months from the date of installation. If the `start.date` set, is a period longer than 12 months, the default time of one month will be used. The MISP Instance timezone is defined in the PHP.ini file on the MISP Instance host.

Verifying the Connector Functionality

After you have installed and configured the connector, you must verify the connector functionality.

Verification Using ESM:

1. Log in to the ESM Console.
2. Go to **All Connectors** > ***<installation_folder*** > ***<connector_name>***, then verify that the status is displayed as *running*.



3. Go to **All Active Lists** > **Threat Intelligence Platform**, then right-click the following active lists and select **Show Entries** to verify if data is populated in the active lists:

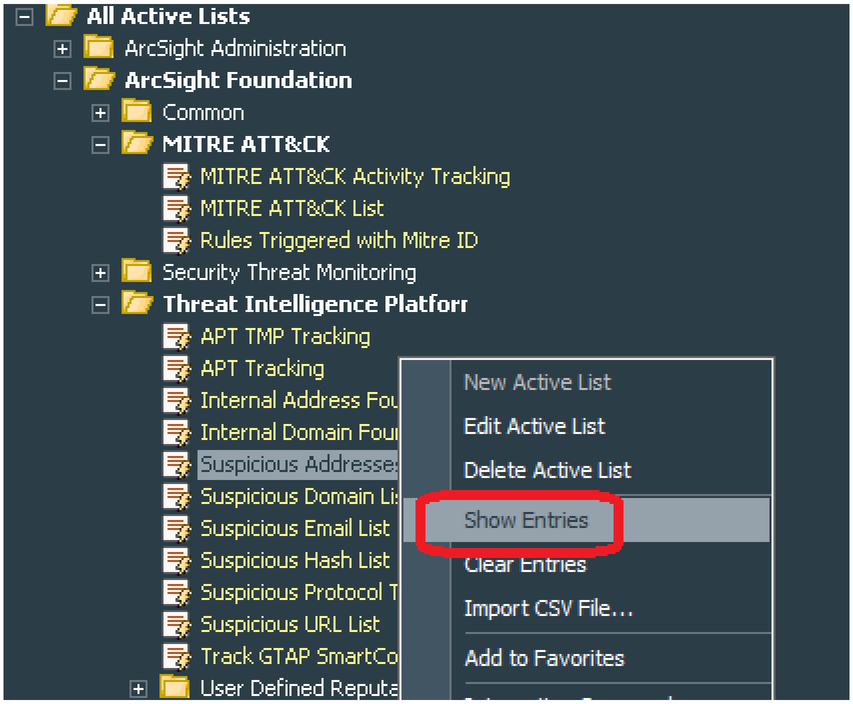
   /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Addresses List

   /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain List

   /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email List

   /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash List

   /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious URL List

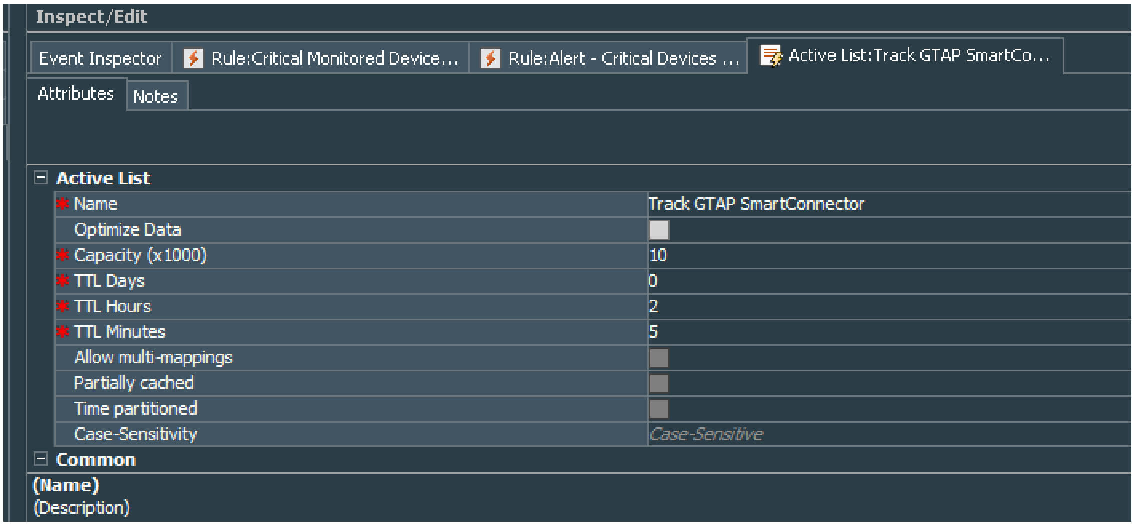


> The Connector requires approximately 5-15 minutes to sync data into active lists for the first time after installation.

4. To verify if the Connector works properly, go to **All Dashboards** > **ArcSight Foundation** > **Threat Intelligence Platform**, then check if the ATAP Connector status is green.

   If the status is red, it might indicate one of the following:

   - ESM has received an error message from the connector.
   - Active lists have not been updated during the time specified in the **All Active Lists** > **ArcSight Foundation** > **Threat Intelligence Platform** > **Track ATAP SmartConnector** > **TTL Hours** field. By default, this value is set to 2 hours.


Inspect/Edit
Event Inspector
Rule:Critical Monitored Device...
Rule:Alert - Critical Devices ...
Active List:Track GTAP SmartCo...
Attributes
Notes

Active List

* Name	Track GTAP SmartConnector
Optimize Data	□
* Capacity (x1000)	10
* TTL Days	0
* TTL Hours	2
* TTL Minutes	5
Allow multi-mappings	□
Partially cached	□
Time partitioned	□
Case-Sensitivity	*Case-Sensitive*

Common

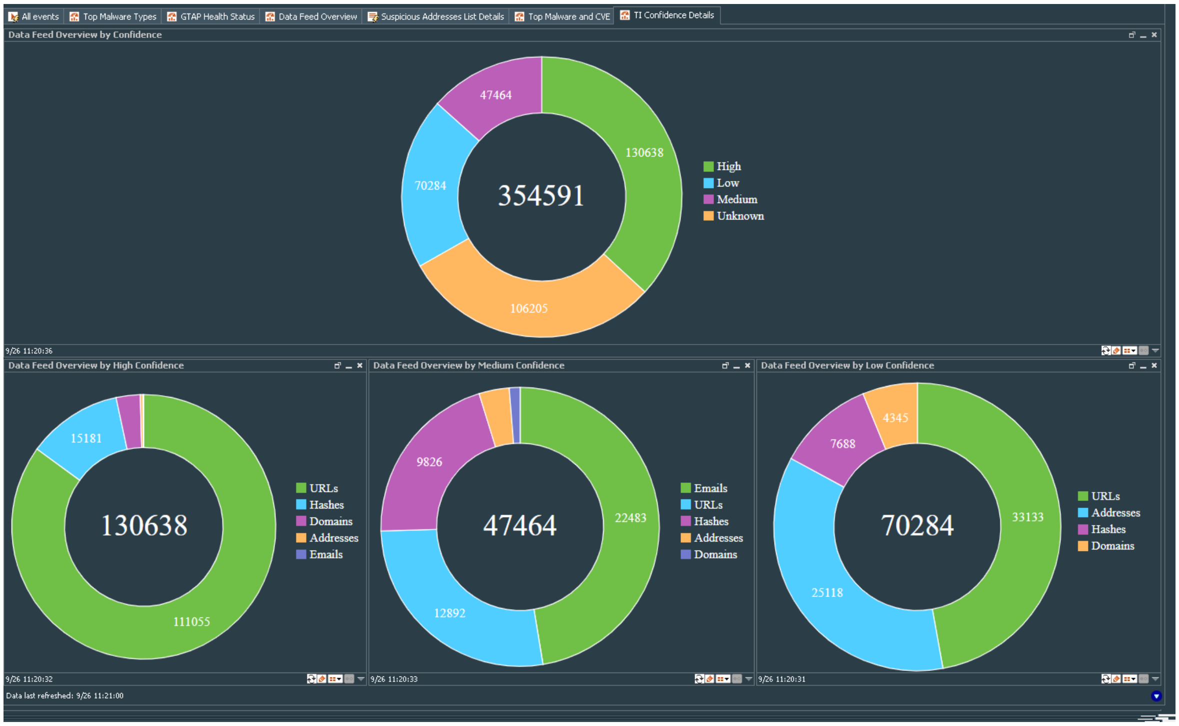
(Name)
(Description)

Identifying Basic and Plus Content When ATAP Plus Connector is Installed

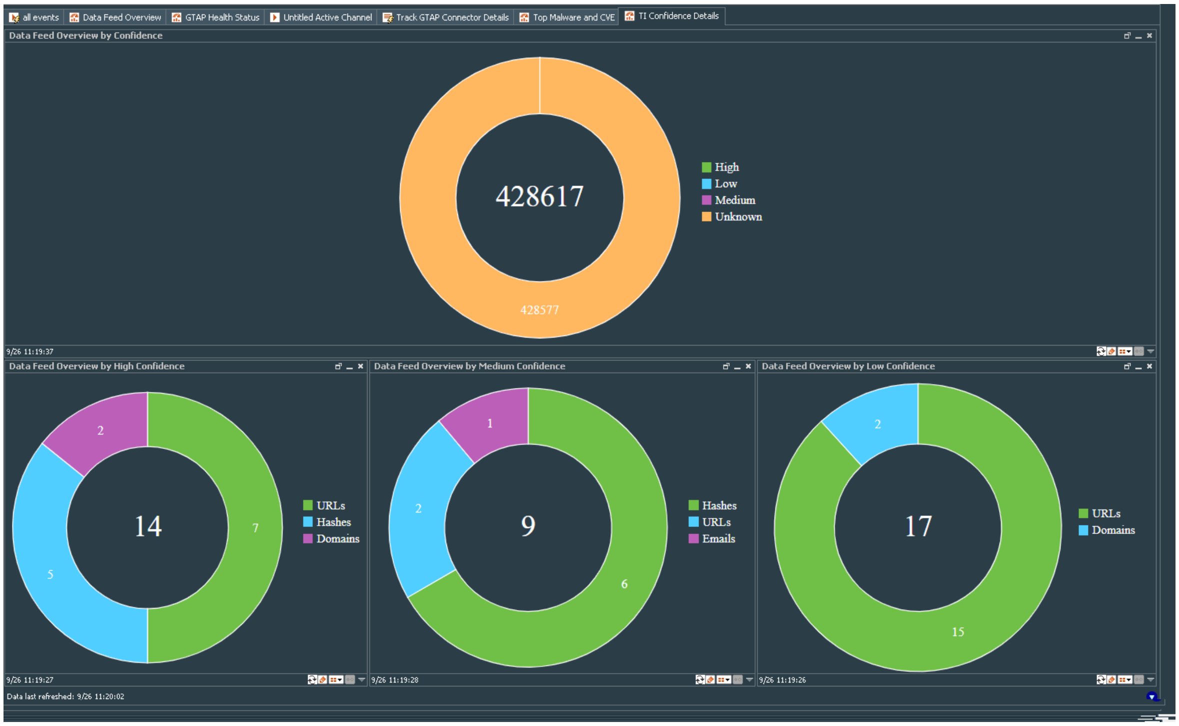
ATAP Basic Connector displays the confidence of threat intelligence feed as "Unknown" whereas the ATAP Plus Connector displays *High/Medium/Low* confidence data for threat intelligence feed so that organizations can identify and resolve threat at the highest urgency level.

To view the threat intelligence confidence details, go to **All Dashboards** > **ArcSight Foundation** > **Threat Intelligence Platform** > **TI Confidence Details**

The Dashboard for ATAP Plus Connector displays *High/Medium/Low* confidence as shown in the following image:



The dashboard for ATAP Basic Connector displays *Unknown* confidence, as shown in the following image:



Upgrading ATAP Connectors

If you have an older version of ATAP connector installed, complete the following procedure to upgrade the connector:

1. Stop the connector.
2. Run the ATAP Connector installer.
3. Select the location of the connector that you want to upgrade.
4. The installation wizard detects that a previous installation exists and prompts the user to upgrade.
5. Click **OK** to continue with the upgrade.
6. Click **Next**, then **Next** again to proceed with the configuration upgrade.

   The upgraded connector is installed in the `$ARCSIGHT_HOME\current folder`.

   During the upgrade, the original installation folder is backed up and saved as a .zip file, while the upgraded connector installation files are saved in the current folder.
7. Specify your ESM account credentials, when prompted.

   The connector upgrade completes successfully.

Troubleshooting

This section has the following troubleshooting topics:

Common Causes of Error

Following are some of the typical issues that might be present:

- **Communication requirements between the connector and the service address are not met**

  Check for network connectivity and verify if the ATAP Model Import Connector is able to reach the ATAP Server or if the ATAP Model Import Connector is able to connect to the ESM server.

- **Model import user is not properly set on ESM**

  For more information, see Setting the Model Import user on ESM.

- **Data import did not start.**

  For more information, see Starting and Stopping Data Import.

- **Content pack for "Threat Intelligence Platform" is not installed on ESM**.

  For more information about installing the Threat Intelligence Platform content pack, see ArcSight Marketplace.

- **Lower number or no records are downloaded**

  This behavior is expected due to the default sync time span of one month. Wait until data import has been completed, which might take up to an hour. Check if you have set the `time period` through `agent.properties` file to a custom, very short time frame.

- **Issues with the API key**

  Ensure that you pass the API key of an API-enabled user along in the Authorization header.

Errors Specific to ATAP Plus, Basic and Custom MISP versions

Some of the errors that might appear for ATAP Basic, Plus, and Custom MISP instance are:

ATAP Plus and Custom MISP

License Key Entered Is Invalid

The following error messages indicate that the license key entered is invalid:

In *$ARCSIGHT_HOME/current/logs/agent.log:*

```
[ERROR] [verifyParameters] Unable to connect to ArcSight Threat
Acceleration Server instance. <Additional data>
```

In *$ARCSIGHT_HOME/current/logs/agentsetup.log*:

```
Unable to connect to ArcSight Threat Acceleration Server instance. Please
provide valid information and try again.
```

Workaround: Verify that the license key that you have entered is valid.

Unable to Retrieve Events

The following error messages might be displayed for both Plus or Custom MISP instances of Model Import Connector in the *agent.log* file in the *$ARCSIGHT_HOME/current/logs* folder:

```
[ERROR] [retrieveEvents] Unable to retrieve response due to <cause>
```

```
[ERROR] [retrieveEvents] <with additional information>
```

Workaround: Check the network connectivity or look for authentication issues. If the Connector is unable to reach the ATAP server, try restarting the server.

ATAP Basic

Following error message might be displayed for the ATAP Model Import Connector in the *agent.log* file in the *$ARCSIGHT_HOME/current/logs* folder.

```
[ERROR] [processATAPEvents] <with additional information>
```

Workaround: Check the network connectivity or look for authentication issues. If the Connector is unable to reach the ATAP server, try restarting the server.

In the ESM Console

In ESM Console, look for the connector events "Data received" and "Data processed" Count=<count>" in Message field.

For ATAP Basic version, you must see this event every 60 minutes and for ATAP Plus and Custom MISP, you must see this every 15 minutes. If you do not see this event, then it indicates that the Connector is not working properly.

Workaround: Check the network connectivity or look for authentication issues. If the Connector is unable to reach the ATAP server, try restarting the server.

Connector is unable to receive any events if the /user/ agent/agentdata folder contains cache

If you had installed MISP Model Import Connector, and installed ArcSight Threat Model Import Connector on the same machine with the **ArcSight Threat Acceleration Plus** option, the connector is unable to receive any after the installation completes.

Workaround: Clear cache from the `user/agent/agentdata` folder, then restart the connector. The connector will now be able to receive events and send events to destination.

Invalid Parameters Error During ATAP Plus Installation

You might get the error message "`The parameters are invalid. Do you want to Continue`, while installing the ATAP Plus version.

Workaround: Click **No** to exit installation. Verify that the API key you have entered is correct. If you do not have a valid API key, then purchase the license and get a valid API Key before proceeding to install ArcSight Threat Acceleration Plus.

Resetting Data Import

If you are unable to see updated data in active lists or if you suspect that the data is not loading properly, you can stop the connector, delete all the existing files and then restart the connector. The connector will then load all data from the start date set in the agent.properties file.

To reload the Connector:

1. Stop the connector, if active.
2. Remove all files:
   - **Linux:** `~/ARCSIGHT_HOME/current/user/agent/agentdata`
   - **Windows:** `$\ARCSIGHT_HOME\current\user\agent\agentdata`
3. In the ArcSight Console, clear all entries in the **Suspicious Domain List**, **Suspicious Email List**, **Suspicious Hash List** and **Suspicious URL List**. For each Active List:
   a. Under **Threat Intelligence Platform**, select the, **Suspicious Domain List**, **Suspicious Addresses List**, **Suspicious Email List**, **Suspicious Hash List** and/ or the **Suspicious URL List** and right-click.
   b. Select **Clear Entries**.
4. Restart the connector.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on ArcSight Threat Acceleration Program Administrator's Guide (ArcSight Threat Acceleration Program 23.4)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!