opentext™

ArcSight ESM

Software Version: 4.2

ESM Default Content 4.2 Release Notes

Document Release Date: September 2023
Software Release Date: September 2023

Legal Notices

Open Text Corporation

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

Copyright Notice

Trademark Notices

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

What's New

ESM Default Content 4.2 rebrands Galaxy Threat Acceleration Program to ArcSight Threat Acceleration Program (GTAP to ATAP) and exchanges all CyberRes references for ArcSight. Additionally, 4.2 adds new content to the Security Threat Monitoring and Threat Intelligence Platform packages to help you monitor command obfuscation, exfiltration to text storage sites, Suspicious API activity, and communication to malvertising publishing domains/IPs.

- Security Threat Monitoring
- Threat Intelligence Platform

Security Threat Monitoring

4.2 includes three new rules to help you detect attacks in your environment using PowerShell, GuardDuty, and more.

Rule Name	Tactic/Technique	Description	Location	Log Source	Events Monitored
Command Obfuscation Using PowerShell	Defense Evasion T1027.010	Detects command obfuscation using Powershell.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Command Obfuscation Using PowerShell	PowerShell	Microsoft-Windows-PowerShell:4104 PowerShell:800
Possible Exfiltration to Text Storage Sites	Exfiltration T1567.003	Creates correlation events for possible exfiltration to text storage sites. This rule includes an Active List with the entries of the URLs of text storage sites. Users can add their own URLs to the existing active list as entries.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Possible Exfiltration to Text Storage Sites	Firewall Events, Proxy Events, and IIS events	Firewall Events, Proxy Events, and IIS events

Rule Name	Tactic/Technique	Description	Location	Log Source	Events Monitored
Suspicious AWS Cloud API Activity Detected	Execution T1059.009	Detects suspicious usage of cloud API. This rule is disabled by default.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Cloud Monitoring/Suspicious AWS Cloud API Activity Detected	GuardDuty	GuardDuty

Threat Intelligence Platform

4.2 releases two new rules that monitor outbound communication.

Resource Type	Rule Name	Description	Platform	Location	Data Source
Rule	Outbound Communication to a Malvertising Publishing Domain	Resource Development T1583.008	Detects malvertising communication to publishing domains.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Dangerous Browsing /Outbound Communication to a Malvertising Publishing Domain	Proxy Events
Rule	Outbound Communication to Malvertising Publishing Address	Resource Development T1583.008	Detects malvertising communication to publishing addresses.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Dangerous Browsing/Outbound Communication to Malvertising Publishing Address	Proxy Events

Updated Content

ESM Default Content 4.2 includes updated content for Security Threat Monitoring and Threat Intelligence Platform.

- Security Threat Monitoring
- Threat Intelligence Platform

Security Threat Monitoring

The following rules have been updated for Security Threat Monitoring 4.2.

Tactic/Technique	Rule Name	What Changed
Persistence|Privilege Escalation T1547.006-Kernel Modules and Extensions	Linux Auditd Kernel Module Loaded in Critical Server	Updated description.
Discovery T1049-System Network Connections Discovery	System Network Connections Discovery	Updated description.

Threat Intelligence Platform

The following resources have been updated for Threat Intelligence Platform 4.2.

Resource Type	Name	What Changed
Rule	ATAP Plus Very High Confidence Alerts with Suspicious File Hash	Name change.
Rule	ATAP Plus Very High Confidence Alerts to Suspicious Source	Name change.
Rule	No Update from ATAP Connector	Name change.
Rule	ATAP Plus High Confidence Alerts to Suspicious Source	Name change.
Rule	Track ATAP Connector Type	Name change.
Rule	ATAP Plus High Confidence Alerts with Suspicious File Hash	Name change.
Rule	Error in ATAP Connector Service Message	Name change.
Rule	Track ATAP Connector Service Message	Name change.
Rule	Track ATAP Connector Update Count	Name change.

Resource Type	Name	What Changed
Data Monitor	ATAP Connector Status	Name change.
Dashboard	ATAP Health Status	Name change.
Dashboard	TI Confidence Comparison- Open Source vs ArcSight-curated	Name change.
Active List	Track ATAP Connector Type	Name change.
Active List	Track ATAP Connector Type	Name change.
Query	High Confidence ArcSight-curated Threat Intelligence Feed	Name change.
Query Viewer	Actionable IoC's from ArcSight-curated TI Feed	Name change.
Query Viewer	ArcSight-curated Threat Intelligence Feed	Name change.
Filter	Update events from ATAP Connector	Name change.

ESM Requirements

Requires ArcSight ESM 7.2 or later.

Log Source Requirements

Security Threat Monitoring and Threat Intelligence Platform require the use of ArcSight SmartConnectors.

ArcSight Threat Acceleration Program Connector

Arcsight Threat Acceleration Program Connector is essential for the Threat Intelligence Platform's capabilities.

Other Log Source Requirements

Log Source	Requirement
Amazon Web Services	SmartConnector for Amazon Web Services CloudTrail
Linux Audit	ArcSight Linux Audit File SmartConnector
Microsoft IIS File	SmartConnector for Microsoft IIS File
Microsoft Office 365	ArcSight Microsoft 365 Defender SmartConnector
Microsoft Windows	ArcSight Microsoft Windows Connector SmartConnector

Security Threat Monitoring and Threat Intelligence Platform have rules and other resources that require SmartConnectors to catch and provide information about events. Information about the log sources associated with each rule are listed in the rule's documentation. You can find the relevant SmartConnector in the SmartConnector Grand List (A-Z).

Note: For log sources like IDS, Proxy, and Firewall, there are a range of SmartConnectors available. You can choose the connectors that best suite your environment from the SmartConnector Grand List.

Deployment

ArcSight Marketplace has two .zip files for the ESM 4.2 Default Content release:

- Security_Threat_Monitoring4.2.zip
  - Security_Threat_Monitoring4.2.arb
  - ESM4.2DefaultContentReleaseNotes.pdf
  - Security_ThreatMonitoring4.2.arb.sig
- Threat_Intelligence_Platform4.2.zip
  - Threat_Intelligence_Platform4.2.arb
  - ESM4.2DefaultContentReleaseNotes.pdf
  - Threat_Intelligence_Platform4.2.arb.sig

Verifying the Downloaded Installation Software

Open Text provides a digital public key to enable you to verify that the signed software you received is indeed from Open Text and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

https://support.microfocus.com/kb/doc.php?id=7025140

Updating or Installing Security Threat Monitoring 4.2

1. Download Security_Threat_Monitoring4.2.zip.
2. Extract the zipped files.
3. Go to the ArcSight Console.
4. Click **Packages**.
5. Click **Import**.
6. Select the corresponding .arb.
7. Follow the prompts to install or update this package.

Installing Threat Intelligence Platform 4.2

1. Download Threat_Intelligence_Platform4.2.zip.
2. Extract the zipped files.
3. Go to the ArcSight Console.
4. Click **Packages**.
5. Click **Import**.
6. Select the corresponding .arb.
7. Follow the prompts to import and install this package.

Updating Threat Intelligence Platform 4.2

This section contains two sets of instructions for updating the Threat Intelligence Platform 4.2 package. Start with the option that applies to you.

Important: Upgrading ESM Default Content from 3.x to 4.2 has specific instructions that must be completed to install the new package.

- 3.x to 4.2
- 4.0 to 4.2

3.x to 4.2

1. Uninstall /ArcSight Foundation/Threat Intelligence Platform.

   Make sure all resources, especially active lists, have been removed from /ArcSight Foundation/Threat Intelligence Platform.
2. Restart the ESM Manager (`/opt/arcsight/services/init.d/arcsight_services stop manager`, then start manager).

   Note: If you do not restart the Manager, you will receive the following error: :Install Failed: invalid field name: creatorOrg".
3. Download Threat_Intelligence_Platform4.2.zip.
4. Extract the zipped files.
5. Go to the ArcSight Console.
6. Click **Packages**.
7. Click **Import**.
8. Select the corresponding .arb.

9. Follow the prompts to install this package.
10. After the initial install finishes, right-click **Threat Intelligence Platform** and click **Install Package**.

Note: If you get the error message below during installation, please select "Always skip DrilldownLists" and continue the installation. Some drilldown functions might not work properly.

Error:
/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Top Threat Intelligence Security Incidents by Attacker
Not Enough Privileges
Not enough privileges to modify '/All Drilldown Lists/Attachments/IoP7xRXABABCrr+s40+xvZQ==/Drilldown List for Top Threat Intelligence Alerts by Attacker

4.0 to 4.2

1. Download Threat_Intelligence_Platform4.2.zip.
2. Extract the zipped files.
3. Go to the ArcSight Console.
4. Click **Packages**.
5. Click **Import**.
6. Select the corresponding .arb.
7. Follow the prompts to import and install this package.

Important: All Threat Intelligence Platform resources have been rebranded from Galaxy Threat Acceleration Program (GTAP) to ArcSight Threat Acceleration Program (ATAP) with the exception of the column names in these 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
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Additional Suspicious Addresses
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform//Additional Suspicious Domain
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Additional Suspicious Email
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Additional Suspicious Hash
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Additional Suspicious URL
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Track ATAP Connector Type

Uninstallation Process

Right-click the package from the ArcSight Console, then select **Uninstall Package**.

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 ESM Default Content 4.2 Release Notes (ESM 4.2)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!