opentext™

ArcSight ESM

Software Version: 4.6

ESM Default Content 4.6 Release Notes

Document Release Date: January 2025
Software Release Date: January 2025

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 4.6 adds eleven new Security Threat Monitoring package rules to the Host Monitoring, Application Monitoring, and Network Monitoring use cases and one new rule in Threat Intelligence Platform package. These new rules support MITRE ATT&CK Framework v15.0.

- Security Threat Monitoring
- Threat Intelligence Platform

Security Threat Monitoring

4.6 includes adds eleven new rules to the Security Threat Monitoring package, adding rules to the Host Monitoring, Application Monitoring, and Network Monitoring use cases.

Resource Type	Rule Name	Tactic & ID	Description	Location	Log Source	Events Monitored
Rule	Domain Trust Modification Detected	Defense Evasion T1484.002	Alerts when ESM detects the addition of new domain trusts or modifications to the properties of existing domain trusts.	/All Rules/Real-time Rules/Security Threat Monitoring/Host Monitoring/	Windows PowerShell	Microsoft-Windows-Security-Auditing:4865 PowerShell:800 Microsoft-Windows-PowerShell:4104
Rule	Hide Artifacts to Evade Detection	Defense Evasion T1564	Alerts when ESM detects hidden artifacts that help adversaries avoid detection.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring	Windows	Based on ArcSight categorization

Resource Type	Rule Name	Tactic & ID	Description	Location	Log Source	Events Monitored
Rule	Possible Abnormal Execution via SyncAppvPublishingServer.vbs	Defense Evasion T1216.002	Alerts when ESM detects code execution on SyncAppvPublishingServer.vbs which can be used to gain unauthorized access to applications virtually.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Application Monitoring	Windows	Microsoft-Windows-Security-Auditing: 4688
Rule	Possible Abnormal Use of Electron Applications	Defense Evasion T1218.015	Alerts when ESM detects the usage of `--disable-gpu-sandbox`, and `--gpu-launcher` on your Electron applications. Adversaries use these parameters circumvent standard application behavior.	/All Rules/ArcSight FoundationSecurity Threat Monitoring/Application Monitoring/	Windows	Microsoft-Windows-Security-Auditing: 4688
Rule	Possible Audio Capture via PowerShell	Collection T1123	Alerts when ESM detects attempts to capture or record audio on a Powershell system.	All Rules/ArcSight Foundation/Security Threat Monitoring/Application Monitoring	PowerShell	PowerShell: 800
Rule	Possible Suspicious Redirect of cURL Command	Command and Control T1105	Alerts when ESM detects identifying commands that utilize flags associated with silent operation, output suppression, and logging of redirection URLs which could indicate suspicious activity related to URL redirection.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Application Monitoring	Windows	Microsoft-Windows-Security-Auditing: 4688

Resource Type	Rule Name	Tactic & ID	Description	Location	Log Source	Events Monitored
Rule	Possible System Language Discovery by Registry Key	Discovery T1614.001	Alerts when ESM detects attempts to query the system's language via the registry which can be used to discover information an adversary can use to tailor their attacks to your specific system.	/All Rules/Arcsight Foundation/Security Threat Monitoring/Application Monitoring	Windows	Microsoft-Windows-Security-Auditing: 4688
Rule	RDP Shadow Session Configuration Enabled	Persistence T1505.005	Alerts when ESM detects modifications to the registry settings that allow someone to view a remote desktop session without user permission.	/All Rules/Real-time Rules/Security Threat Monitoring/Host Monitoring	Windows	Microsoft-Windows-Security-Auditing:4657 Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1

Resource Type	Rule Name	Tactic & ID	Description	Location	Log Source	Events Monitored
Rule	SID-History Injection Detected	Defense Evasion T1134.005	Alerts when ESM detects the insertion of SID values into SID-History which allows an adversary to impersonate users or groups in your environment.	/All Rules/Real-time Rules/Security Threat Monitoring/Host Monitoring/	Windows	Microsoft-Windows-Security-Auditing:4765
Rule	Scripting Interpreters AutoHotKey or AutoIT Detected	Execution T1059.010	Alerts when ESM detects commands and tasks from AutoIT and AutoHotKey automation scripts.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/	Windows	Microsoft-Windows-Security-Auditing: 4688
Rule	Suspicious OpenAI Activity	Resource Development T1588.007	Alerts when ESM detects MITRE ATT&CK technique events that occur in conjunction with OpenAI communications from the same IP address within a short period of time, suggesting the abuse of AI capabilities, potentially allowing adversaries to exfiltrate data, automate scripting, or execute command and control processes.	All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring	Proxy Events MITRE Correlation Events	Based on Name Field Signatures

Threat Intelligence Platform

4.6 one new rule.

Resource Type	Tactic & ID	Rule Name	Description	Location	Data Source
Rule	N/A	Suspicious File Hash Activity in Host Sysmon Based	Uses Sysmon to detect suspicious file hash on your host. It verifies the following file hashes: SHA1, MD5, SHA-256, or the IMPHASH.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious File Hash	Sysmon

Updated Content

The following rule has been updated in the Security Threat Monitoring 4.6 package.

Tactic/Technique	Rule Name	What Changed
Credential Access, Discovery T1040	Suspicious Network Sniffing	Updated the rule's conditions to capture the following sniffing tools: PktMon, Tshark, and WinDump.

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.

Verifying the Downloaded Installation Software

ArcSight Marketplace has two .zip files for the ESM 4.6 Default Content release:

- Security_Threat_Monitoring4.6.zip
  - Security_Threat_Monitoring4.6.arb
  - ESM4.6DefaultContentReleaseNotes.pdf
  - Security_ThreatMonitoring4.6.arb.sig
- Threat_Intelligence_Platform4.6.zip
  - Threat_Intelligence_Platform4.6.arb
  - ESM4.6DefaultContentReleaseNotes.pdf
  - Threat_Intelligence_Platform4.6.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.

Tip: Evolving security needs imply the renewal of certificates for the signature verification procedure. To ensure a successful verification of your product signature, download the latest public keys file before proceeding with the verification process (step 1 of the Get the Public Keys procedure).

Visit the following site for information and instructions:

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

Installing and Updating Default Content 4.6

The following section contains instructions for you to install, update, or uninstall your STM and TIP packages.

Installing Security Threat Monitoring

1. Download Security_Threat_Monitoring4.6.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

Installing Threat Intelligence Platform 4.6

1. Download Threat_Intelligence_Platform4.6.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.

Upgrading Security Threat Monitoring

Important: If you previously customized standard resources in the resource's original location, back up the resources to an .arb file (exclude related resources) before you upgrade. If you copied the resources to a custom group and then customized them, the upgrade does not impact the custom group.

1. Download Security_Threat_Monitoring4.6.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.

Upgrading Threat Intelligence Platform

This section contains *two* sets of instructions for updating the Threat Intelligence Platform 4.6 package. Choose the option that applies to you.

Important: Customizations to the Threat Intelligent Platform package (TIP) v3.x to v4.x are not supported.

Export any custom packages created for TIP v3.x and then delete the original. This allows the upgrade process to cleanly uninstall TIP v3.x package.

Do not import custom packages created for TIP v3.x after the upgrade, as they can create resource conflicts with new version of Threat Intelligent Platform. You can manually add your customizations back once this upgrade is complete.

Updating TIP version 3.x to 4.6

1. Uninstall /ArcSight Foundation/Threat Intelligence Platform.

   Make sure all resources, especially active lists, have been removed from /ArcSight Foundation/Threat Intelligence Platform.

   Active Lists must be deleted manually since they might not uninstall automatically for many reasons like being part of other packages. You can find them under /All Active Lists/ArcSight Foundation/Threat Intelligence Platform.
2. Stop the ESM Manager, `/opt/arcsight/services/init.d/arcsight_services stop manager`.
3. Restart the manager.

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

11. 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

Updating TIP version 4.0 to 4.6

1. Download Threat_Intelligence_Platform4.6.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

Uninstalling the Packages

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

Publication Status

Released: January 2025

Updated: Tuesday, January 7, 2025

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 4.6 Release Notes (ESM 4.6)

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!