Micro Focus Security ArcSight ESM

Software Version: 4.1

ESM Default Content 4.1 Release Notes

Legal Notices

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 4.1 adds new content to the Security Threat Monitoring and Threat Intelligence Platform packages to help you monitor and protect your environment.

- Security Threat Monitoring
- Threat Intelligence Platform

Security Threat Monitoring

4.1 includes twelve new rules to help you detect attacks in Windows, Sysmon, and Powershell.

Rule Name	Tactic/Technique	Description	Log Source	Events Monitored
Credentials Gathered using Mimikatz Tool	Credential Access T1003.002-Security Account Manager	Detects attempts to extract credential material from the Security Account Manager using Mimikatz.	Windows, Sysmon	Microsoft-Windows-Sysmon:1 Microsoft-Windows-Security-Auditing: 4688
SystemRestore Task Disabled Using Schtasks	Persistence|Execution|Privilege Escalation T1053.005-Scheduled Task	Detects abuse to task scheduling functionality to facilitate initial orrecurring execution of malicious code using Schtasks.	Windows, Sysmon	Microsoft-Windows-Sysmon:1 Microsoft-Windows-Security-Auditing: 4688 schtasks.exe
File Encrypted Using Encryptor Tool	Impact T1486-Data Encrypted for Impact	Detects attempts to encrypt data on target systems using encryptor.exe.	Windows, Sysmon	Microsoft-Windows-Sysmon:1 Microsoft-Windows-Security-Auditing:4688

Rule Name	Tactic/Technique	Description	Log Source	Events Monitored
Credentials In Files	Credential Access T1552.001-Credentials In Files	Detects searches of local files and remote file shares for unsecured credentials.	Windows, Sysmon	Microsoft-Windows-Sysmon:1 Microsoft-Windows-Security-Auditing:4688
Specific Processes Killed Using PowerShell Command	Impact T1489-Service Stop	Detects specific stopped or disabled processes on a system.	Windows, Sysmon	Microsoft-Windows-Sysmon:1 Microsoft-Windows-Security-Auditing:4688
Spearphishing via Whatsapp	Credential Access T1552.001-Credentials In Files	Detects spearphishing messages via third-party services in an attempt to gain access to systems. Spearphishing via service is a specific variant of spearphishing.	SMS	1687016714
Disable Windows Recovery Using BCDedit Tool	Impact T1490-Inhibit System Recovery	Detects the deletion or removal of built-in operating system data and the turn off of services designed to aid in the recovery of a corrupted system to prevent recovery using BCDedit.	Windows, Sysmon	Microsoft-Windows-Sysmon:1 Microsoft-Windows-Security-Auditing:4688
Deletion of Active USN Change Journal Using Fsutil	Indicator Removal T1070.009-Clear Persistence	Detects if an active USN change journal is deleted using fsutil.	Windows, Sysmon	Microsoft-Windows-Sysmon:1 Microsoft-Windows-Security-Auditing:4688 fsutil.exe

Rule Name	Tactic/Technique	Description	Log Source	Events Monitored
Delete Backups Using WBadmin	Impact T1490-Inhibit System Recovery	Detects the deletion or removal of built-in operating system data and the turn-off of services designed to aid in the recovery of a corrupted system using WBadmin.	Windows, Sysmon	Microsoft-Windows-Sysmon:1 Microsoft-Windows-Security-Auditing:4688
Credential Dumping Using LaZagne	Credential Access T1555-Credentials from Password Stores	Detects searches for common password storage locations such as databases, mail, and WiFi, to obtain user credentials using LaZagne.	Windows, Sysmon	Microsoft-Windows-Sysmon:1 Microsoft-Windows-Security-Auditing:4688
Event Log Deleted Using Wevtutil Tool	Defense Evasion T1070.001-Clear Windows Event	Detects the clearing of Windows Event Logs to hide an intrusion using wevtutil.	Windows, Sysmon	Microsoft-Windows-Sysmon:1 Microsoft-Windows-Security-Auditing:4688 wevtutil.exe
Program Install	Privilege Escalation T1546.016-Installer Packages	Detects adversaries establishing persistent and elevate privileges by using and installer to trigger the execution of malicious content.	Windows, Sysmon	Microsoft-Windows-Sysmon:1 Microsoft-Windows-Security-Auditing:4688

Threat Intelligence Platform

4.1 releases a new active channel and three new rules designed to notify you of very high confidence alerts from the Galaxy Threat Acceleration Program (GTAP).

Resource Type	Rule Name	Description	Platform	Data Source
Active Channel	Very High Confidence Alerts	Monitors very high confidence alerts from suspicious sources and suspicious hashes.	N/A	N/A
Rule	GTAP Plus Very High Confidence Alerts with Suspicious File Hash	Detects alerts of suspicious file hash with very high confidence.	Hash Events with File Hash, like Sysmon	Correlation
Rule	GTAP Plus Very High Confidence Alerts to Suspicious Source	Detects suspicious outbound traffic with very high confidence.	ArcSight Internal Events	Correlation
Rule	Track GTAP Connector Type	Detects events of connector type.	ArcSight Internal Events	Correlation

Updated Content

ESM Default Content 4.1 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 4.1.

Tactic/Technique	Rule Name	What Changed
Impact T1490-Inhibit System Recovery	Chained Rule - Inhibit System Recovery	Updated this rule with new conditions.

Threat Intelligence Platform

The following resources have been updated for Threat Intelligence Platform 4.1.

Resource Type	Name	Location	What Changed
Rule	Email Sent To Suspicious Address	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/Email Sent To Suspicious Address	New conditions were added.
Rule	GTAP Plus High Confidence Alerts to Suspicious Source	/All Rules/ArcSight Foundation/Threat Intelligence Platform/High Confidence Alerts/GTAP Plus High Confidence Alerts to Suspicious Source	New conditions were added.
Rule	GTAP Plus High Confidence Alerts with Suspicious File Hash	/All Rules/ArcSight Foundation/Threat Intelligence Platform/High Confidence Alerts/GTAP Plus High Confidence Alerts with Suspicious File Hash	New conditions were added.
Rule	Dangerous Browsing to a Suspicious URL	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Dangerous Browsing/Dangerous Browsing to a Suspicious URL	New conditions were added.

Resource Type	Name	Location	What Changed
Rule	Outbound Traffic to a Suspicious Address	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Activity/Outbound Traffic to a Suspicious Address	New conditions were added.
Rule	Outbound Traffic to a Suspicious Domain	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Activity/Outbound Traffic to a Suspicious Domain	New conditions were added.
Rule	Suspicious File Hash Activity in Host	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious File Hash/Suspicious File Hash Activity in Host	New conditions were added.

Package Requirements

This package has ESM and Log Source requirements.

ESM Requirements

Requires ArcSight 7.2 or later.

Log Source Requirements

This package requires the following log sources:

Log Source	Requirement
AWS Security Hub	ArcSight Security Hub SmartConnector
GTAP	CyberRes Galaxy Threat Acceleration Program 2.0
Linux Audit	ArcSight Linux Audit File SmartConnector
Microsoft Office 365	ArcSight Microsoft 365 Defender SmartConnector
Microsoft Windows	ArcSight Windows Connector SmartConnector

Deployment

The .zip file contains three files:

- package .arb file
- signature .arb file
- Readme

Installing the 4.1 package

This section contains two sets of instructions for installing the 4.1 package. Start with the option that applies to you.

Important: Upgrading ESM Default Content from 3.x to 4.1 has specific instructions that must be completed to install the new package.

- 3.x to 4.1
- 4.0 to 4.1

3.x to 4.1

1. Uninstall /ArcSight Foundation/Threat Intelligence Platform.
   a. 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. Go to the ArcSight Console.
4. Click **Packages**.
5. Click **Import**.
6. Select the package .arb from the .zip file.
7. Follow the prompts to import and install this package.
8. 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 4.1

1. Go to the ArcSight Console.
2. Click **Packages**.
3. Click **Import**.
4. Select the package .arb from the .zip file.
5. Follow the prompts to import and install this package.

Uninstallation Process

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

Verifying the Downloaded Installation Software

Micro Focus provides a digital public key to enable you to verify that the signed software you received is indeed from Micro Focus 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

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 4.1 Release Notes (ESM 4.1)

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!