opentext™

OpenText Enterprise Security Manager

Software Version: 4.8

ESM Default Content 4.8 Release Notes

Document Release Date: November, 2025
Software Release Date: November, 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 4.8 introduces 30 new detection rules across 28 MITRE ATT&CK Techniques, strengthening visibility into Initial Access, Defense Evasion, and Lateral Movement Tactics. These rules enhance detection in both network and endpoint environments.

Summary of additions

- 30 new detection rules implemented
- MITRE ATT&CK Techniques introduced
  - T1006-Direct Volume Access
  - T1007-System Service Discovery
  - T1016.001-System Network Configuration Discovery: Internet Connection Discovery
  - T1027.003-Obfuscated Files or Information: Steganography
  - T1055.001-Process Injection: Dynamic-link Library Injection
  - T1059.004-Command and Scripting Interpreter: Unix Shell
  - T1069.001-Permission Groups Discovery: Local Groups
  - T1069.002-Permission Groups Discovery: Domain Groups
  - T1070-007-Indicator Removal: Clear Network Connection History and Configurations
  - T1074.001-Data Staged: Local Data Staging
  - T1090.001-Proxy: Internal Proxy
  - T1095-Non-Application Layer Protocol
  - T1110.002-Brute Force: Password Cracking
  - T1114.002-Email Collection: Remote Email Collection
  - T1120-Peripheral Device Discovery
  - T1124-System Time Discovery
  - T1127.003-Trusted Developer Utilities Proxy Execution: JamPlus
  - T1207-Rogue Domain Controller
  - T1497.001-Virtualization/Sandbox Evasion: System Checks
  - T1505.003-Server Software Component: Web Shell
  - T1552-Unsecured Credentials
  - T1552.004-Unsecured Credentials: Private Keys
  - T1564.012-Hide Artifacts: File/Path Exclusions

- T1564.013-Hide Artifacts: Bind Mounts
- T1572-Protocol Tunneling
- T1573.001-Encrypted Channel: Symmetric Cryptography
- T1590.004-Gather Victim Network Information: Network Topology
- T1594-Search Victim-Owned Websites

Security Threat Monitoring

Version 4.8 adds 30 new rules to the Security Threat Monitoring package, adding rules to the Network Monitoring, Vulnerability Monitoring, and Application Monitoring use cases.

Resource Type	Rule Name	Tactic (Technique)	Description	Rule Path	Data Source
Rule	Vssadmin Create Volume Shadow Copies	Defense Evasion (T1006)	This rule is fired when an adversary uses vssadmin to create volume shadow copies Note: To capture the Windows logs, please enable command-line auditing in the following policy location paths: • Administrative Templates\System\Audit Process Creation • Computer Configuration\Policies\ Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring	Windows Security Auditing:4688 cmd.exe
Rule	Possible System Service Discovery	Discovery (T1007)	This rule detects potential system discovery activity where a process commonly used for enumerating services or system information (for example, wmic.exe, sc.exe) is launched from an unexpected or non-standard folder, such as user Downloads or temporary directories. Execution from these locations is atypical for administrative or legitimate processes and may indicate adversary reconnaissance attempts.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring	Windows Security Auditing:4688 WMIC.exe net.exe tasklist.exe sc.exe

Resource Type	Rule Name	Tactic (Technique)	Description	Rule Path	Data Source
Rule	Suspicious Internet Connection Discovery	Discovery (T1016.001)	This rule detects suspicious use of built-in Windows utilities (for example, ping, nslookup, tracert, curl, wget, or PowerShell networking commands) that may indicate Internet Connection Discovery activity. Attackers often run these commands to test external connectivity or verify access to specific domains (such as Google DNS 8.8.8.8, Cloudflare 1.1.1.1, or Microsoft connectivity test sites like msftconnecttest.com and msftncsi.com).	/All Rules/ArcSight Foundation/Security Threat Monitoring/Application Monitoring	Windows Process Creation Event 4688
Rule	Steganography Tool Execution Detected	Defense Evasion (T1027.003)	This rule detects the execution of steganography tools in the environment.	/All Rules/ArcSight Foundation/Security Threat Monitoring	Windows Process Creation Event 4688
Rule	Dynamic-link Library Injection	Defense Evasion, Privilege Elevation (T1055.001)	This rule detects attempts to inject a DLL into a running process using the PowerSploit Invoke-DllInjection function, which might indicate malicious activity such as code execution or process manipulation using PowerShell.	/All Rules/ArcSight Foundation/Security Threat Monitoring	PowerShell:800, PowerSploit:4104
Rule	Command and Scripting Interpreter Tool Brightmetricagent.exe	Unix Shell (T1059.004)	This rule detects multiple executions of ping.exe with the -a flag against different IP addresses within a short time window. Adversaries may use this technique to resolve hostnames and enumerate network topology as part of reconnaissance activities. Multiple ping -a commands in sequence can indicate scripted or manual host discovery attempts.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring	Windows Security Auditing:4688 cmd.exe

Resource Type	Rule Name	Tactic (Technique)	Description	Rule Path	Data Source
Rule	Local Groups Permission Discovery	Discovery (T1069.001)	This rule detects when a net command is used to query the membership or permissions of local security groups.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring	Windows Security Auditing:4688
Rule	Domain Groups Permission Discovery	Discovery (T1069.002)	This rule detects when a net command is used to query the membership or permissions of domain groups.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring	Windows Security Auditing:4688
Rule	Remove Network Connection History and Configurations	Defense Evasion (T1070.007)	This rule triggers when an adversary removes network connection history and configuration. Note: To capture the Windows logs, please enable command-line auditing in the following policy location paths: • Administrative Templates\System\Audit Process Creation • Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring	Windows Security Auditing:4688 route.exe ipconfig.exe

Resource Type	Rule Name	Tactic (Technique)	Description	Rule Path	Data Source
Rule	Save ntds.dit or SYSTEM or SECURITY registry	Collection (T1074.001)	This rule triggers when ntds.dit, or the SYSTEM or SECURITY registry, are written to a directory like \Windows\Temp. Note: To capture the Windows logs, please enable command-line auditing in the following policy location paths: • Administrative Templates\System\Audit Process Creation • Computer Configuration\Policies\ Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring	Windows Security Auditing:4688 cmd.exe vssadmin.exe reg.exe
Rule	Port Forwarding Detected	Command and Control (T1090.001)	This rule is fired when an adversary makes configurations of port forwarding, also known as port proxying or tunneling, on endpoints or network devices within an organization. Note: To capture the Windows logs, you must enable command-line auditing in the following policy location paths: • Administrative Templates\System\Audit Process Creation • Computer Configuration\Policies\ Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring	Windows Security Auditing:4688 netsh.exe netsh interface portproxy add

Resource Type	Rule Name	Tactic (Technique)	Description	Rule Path	Data Source
Rule	Suspicious Use of ICMP for C2 in Application Layer	Command and Control (T1095)	This rule is designed to detect suspicious network traffic patterns that indicate ICMP tunneling or data exfiltration using the Internet Control Message Protocol (ICMP) for Command and Control (C2) channels.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/Suspicious Use of ICMP for C2 in Application Layer	/Traffic Anomaly /IDS/Network /Host/Application (or) /Network /Suspicious (or) /Compromise (or) /Hostile
Rule	Suspicious Password Cracking Tool Execution Detected	Credential Access (T1110.002)	This rule detects the execution of known password cracking tools (for example, Hashcat, John the Ripper, Cain & Abel) from suspicious or non-standard locations on Windows endpoints, such as Users, Downloads, Temp, and Desktop folders.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Application Monitoring	Windows Process Creation Event 4688
Rule	Possible Remote Email Collection Via PowerShell	Email Collection (T1114.002)	This rule detects potential mailbox enumeration or email collection in Exchange/Office 365 using PowerShell commands, which might indicate malicious activity using tools like MailSniper or custom scripts.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Application Monitoring	PowerShell:800

Resource Type	Rule Name	Tactic (Technique)	Description	Rule Path	Data Source
Rule	Peripheral Device Discovery Using PowerShell	Discovery (T1120)	This rule triggers when an adversary discovers peripheral devices, such as printers, USB drives, or display devices. Note: To capture the Windows logs, please enable command-line auditing in the following policy location paths: • Administrative Templates\System\Audit Process Creation • Computer Configuration\Policies\ Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring	PowerShell:800
Rule	Possible WMIC Peripheral Device Discovery	Discovery (T1120)	This rule detects the use of WMIC to enumerate peripheral devices, such as USB controllers, sound devices, video controllers, serial ports, or CD-ROM drives. Adversaries may leverage this technique to gather information about connected hardware for further exploitation or persistence.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring	Windows Process Creation Event 4688
Rule	Possible System Time Discovery	Discovery (T1124)	This rule detects attempts to discover the system time using common Windows utilities through scripting.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring	Windows Process Creation Event 4688
Rule	JamPlus Executed on non Development Environment	Defense Evasion (T1127.003)	This rule detects if JamPlus.exe executed on a non-development machine.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Application Monitoring	Windows Process Creation Event 4688

Resource Type	Rule Name	Tactic (Technique)	Description	Rule Path	Data Source
Rule	Possible Rogue Domain Controller Activity	Defense Evasion (T1207)	This rule detects a sequence of events indicative of a DCShadow attack. It identifies the creation of a temporary rogue Active Directory Domain Controller object and the subsequent privilege escalation activities. Note: To use this rule, you must enable the lightweight rule /All Rules/Real-time Rules/Security Threat Monitoring/Host Monitoring/Directory Service Object Created.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring	Windows Security Auditing:4688 Windows Security Auditing:4928 Windows Security Auditing:4929 Windows Security Auditing:4662
Rule	Virtualization Evasion System Checks	Defense Evasion, Discovery (T1497.001)	This rule detects attempts to perform system checks commonly used by adversaries to automatically identify virtualization or sandbox environments.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring	Windows Process Creation Event 4688
Rule	Suspicious Web Shell Process Spawned by Web Server	Persistence (T1505.003)	This rule detects web server processes (IIS, Apache, Nginx, Tomcat) spawning command shells or system utilities, indicating potential web shell execution. Also, this rule will detect if the threat actor is running .aspx or .jspx web shell files chained with Initial Access or Execution Tactics.	/All Rules/ArcSight Foundation/Security Threat Monitoring/ Application Monitoring	Windows, Linux, Network Devices
Rule	New Processes with Parameters Indicating Credential Searches	Credential Access (T1552)	This rule detects processes executed from Temp or Downloads folders that include parameters related to credential searches.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Application Monitoring	Windows Process Creation Event 4688
Rule	Extraction of Private Keys Using Mimikatz	Credential Access (T1552.004)	This rule detects attempts to extract private keys using the Mimikatz executable.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Application Monitoring	Windows Process Creation Event 4688

Resource Type	Rule Name	Tactic (Technique)	Description	Rule Path	Data Source
Rule	Possible Artifacts Hidden Using WSL	Defense Evasion (T1564.012)	This rule detects potential malicious use of Windows Subsystem for Linux (WSL) to hide artifacts and evade security controls. Note: To capture the Windows logs, you must enable command-line auditing in the following policy location paths: • Administrative Templates\System\Audit Process Creation • Computer Configuration\Policies\ Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring	Windows Process Creation Event 4688
Rule	Bind Mounts on Linux	Defense Evasion (T1564.013)	This rule is triggered when an adversary is trying to bind mounts on the Linux system. To capture this use case, you must do the following: 1. Install Snoopy Logging (open source) on the Linux machine that is being monitored `sudo yum update` `sudo yum install` `sudo yum install snoopy` `sudo snoopyctl enable` Make sure snoopy events are collected in `/var/log/secure`. 2. Install Syslog file connector. 3. Provide the path as `/var/log/secure` in the Syslog connector.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Bind Mounts on Linux	Snoopy Unix mount --bind mount

Resource Type	Rule Name	Tactic (Technique)	Description	Rule Path	Data Source
Rule	Suspicious Network Tunneling Tool Executed	Command and Control (T1572)	This rule detects potential malicious use of network tunneling tools such as nc.exe, ncat.exe, or plink.exe when executed from unexpected or non-standard locations on a host. These tools are commonly used to tunnel protocols, bypass network restrictions, or establish unauthorized remote access. This rule uses Windows Event ID 4688 (Process Creation) to identify suspicious command-line arguments, unusual parent processes, and execution paths that do not match known trusted locations.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring	Windows Process Creation Event 4688
Rule	Possible PowerShell Symmetric Encryption Abuse	Command and Control (T1573.001)	This rule detects suspicious PowerShell commands leveraging symmetric encryption functionality, such as the use of ConvertTo-SecureString or AES cryptography classes. Adversaries may abuse these methods to encrypt payloads, credentials, or communication channels in order to evade detection or facilitate data exfiltration.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Application Monitoring	PowerShell:800 Windows PowerShell:4103 Windows PowerShell:4104

Resource Type	Rule Name	Tactic (Technique)	Description	Rule Path	Data Source
Rule	Ping Based Topology Discovery	Reconnaissance (T1590.004)	This rule detects multiple executions of ping.exe with the -a flag against different IP addresses within a short time window. Adversaries may use this technique to resolve hostnames and enumerate network topology as part of reconnaissance activities. Multiple ping -a commands in sequence can indicate scripted or manual host discovery attempts.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring	Windows Security Auditing:4688 PING.EXE
Rule	Possible Victim Website Crawling Activity	Reconnaissance (T1594)	This rule triggers when an adversary attempts to crawl an organizational website. By default, it detects three distinct requests within one minute from the same IP address using the same suspicious User-Agent.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring	Web Servers (Apache)

Updated Content

ESM Default Content 4.8 includes updated rules in the ArcSight Foundation package.

The following rule has been updated in the Security Threat Monitoring 4.8 package.

- Security Threat Monitoring

Security Threat Monitoring

Tactic/Technique	Rule Name	What Changed
Resource Development T1588.007	Suspicious OpenAI Activity	The rule name and path was updated to Suspicious Generative AI Activity: /All Rules/Real-time Rules/Security Threat Monitoring/Host Monitoring/Suspicious OpenAI Activity This rule now covers the following generative AI platforms: OpenAI, Claude AI, Gemini, and Mistral AI.

ESM Requirements

Requires OpenText Enterprise Security Manager 7.2 or later.

Log Source Requirements

Security Threat Monitoring and Threat Intelligence Platform require the use of SIEM 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	OpenText Linux Audit File SIEM SmartConnector
Microsoft IIS File	SmartConnector for Microsoft IIS File
Microsoft Office 365	OpenText Microsoft 365 Defender SIEM SmartConnector
Microsoft Windows	OpenText Microsoft Windows Connector SIEM 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 4.8 Default Content release:

- Security_Threat_Monitoring4.8.zip
  - Security_Threat_Monitoring4.8.arb
  - ESM4.8DefaultContentReleaseNotes.pdf
  - Security_ThreatMonitoring4.8.arb.sig
- Threat_Intelligence_Platform4.8.zip
  - Threat_Intelligence_Platform4.8.arb
  - ESM4.8DefaultContentReleaseNotes.pdf
  - Threat_Intelligence_Platform4.8.arb.sig

Verifying the Downloaded Installation Software

OpenText provides a digital public key to enable you to verify that the signed software you received is indeed from OpenText 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 4.8

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_Monitoring4.8.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 4.8

1. Download Threat_Intelligence_Platform4.8.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_Monitoring4.8.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 4.8 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 4.8

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_Platform4.8.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 4.8

1. Download Threat_Intelligence_Platform4.8.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**.