Micro Focus Security ArcSight ESM

Software Version: 3.7

ESM Default Content 3.7 Release Notes

Document Release Date: May 2022
Software Release Date: May 2022

Legal Notices

Copyright Notice

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, “commercial computer software” is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation (“FAR”) and its successors. If acquired by or on behalf of any agency within the Department of Defense (“DOD”), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement (“DFARS”) and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S.Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/about/legal/.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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

This release contains new resources in the Security Threat Monitoring package to help protect Windows, AWS Security Hub, and Microsoft Office 365 environments [or] applications. It also contains new rules and a new dashboard to help you monitor the health of the CyberRes Galaxy Threat Acceleration Program (GTAP)1.0 Basic and Plus Model Import Connector. The following sections outline the key features and functions provided in this release.

Release 3.7 Security Threat Monitoring adds support for the following MITRE ATT&CK tactics and techniques:

- Defense Evasion: T1218 Signed Binary Proxy Execution
- Defense Evasion: T1218 Signed Binary Execution/T1218.008 Odbcconf
- Collection: T1560 Archive Collected Data
- Persistence: T1546 Event Triggered Execution/T1546.001 Change Default File Association
- Defense Evasion: T1574 Hijack Execution Flow/T1574.012 COR_PROFILER
- Credential Access: T1003.006 OS Credential Dumping: DCSync
- Collection: T1213 Data from Information Repositories/1213.002 SharePoint
- Collection: T1530 Data from Cloud Storage Object

Release 3.7 contains new rules and a new dashboard in the Threat Intelligence Program.

- Error messages from the GTAP Connector trigger alerts.
- An alert triggers if data feeds from the GTAP Connector do not update for a specified time frame. The default time frame is two hours.
- The new dashboard shows the health status of the GTAP Connector.

Content and Rules

The following resources have been created to detect various threats in Security Threat Monitoring 3.7.

Tactic/Technique	Rule Name	Description	Log Source	Events Monitored
Defense Evasion T1218	Signed Binary Proxy Execution	This rule triggers when an adversary bypasses process and signature-based defenses by proxying execution of malicious content with signed binaries.	Windows	Microsoft-Windows-PowerShell: 4104
Defense Evasion T1218.008	Odbccon to Proxy Execution of Malicious Payloads	This rule triggers when an adversary abuses odbcconf.exe to proxy execution of malicious payloads. Odbcconf.exe is a Windows utility that allows you to configure Open Database Connectivity (ODBC) drivers and data source names.	Windows	Microsoft-Windows-Security-Auditing: 4688
Collection T1560	Possible Archive of Collected Data Using PowerShell	This rule triggers when an adversary compresses data that is collected using PowerShell.	Windows	Microsoft-Windows-PowerShell: 4104
Persistence T1546.001	Possible Change of Default File Association	This rule triggers when an adversary establishes persistence by executing malicious content triggered by a file type association. When a file is opened, the default program used to open the file (also called the file association or handler) is checked.	Windows	Microsoft-Windows-Security-Auditing: 4688
Defense Evasion T1574.012	COR+PROFILER to Hijack Program Execution Flow	This rule triggers when an adversary leverages the COR_ PROFILER environment variable to hijack the execution flow of programs that load the .NET CLR. The COR_PROFILER is a .NET Framework feature that allows developers to specify an unmanaged (or external code from .NET) profiling DLL to be loaded.	Windows	Microsoft-Windows-PowerShell: 4104

Tactic/Technique	Rule Name	Description	Log Source	Events Monitored
Credential Access T1003.006	Possible DCSync OS Credential Dumping	This rule triggers when it detects DCSync OS Credential Dumping based on Windows Event 4662.	Windows	Microsoft-Windows-Security-Auditing: 4662
Collection T1213.002	SharePoint Activity by Privileged User	This rule triggers when a privileged user name accesses a file. You can customize privileged user accounts by adding all upper case user names (such as ADMIN) to the list: /All Active Lists/ArcSight Foundation/Common/Privilege User Account.	Microsoft Office 365	N/A
Collection T1530	AWS S3 Policy Misconfiguration	This rule triggers when it detects suspicious activity related to AWS S3 policy misconfiguration.	AWS Security Hub	PublicAccessDisabled BucketAnonymousAccessGranted BucketPublicAccessGranted
Collection T1530	AWS S3 Unauthorized Access	This rule triggers when it detects suspicious activity related to AWS S3 unauthorized access.	AWS Security Hub	MaliciousIPCaller.Custom TorIPCaller

New GTAP Model Import Connector Rules and Dashboard

This package introduces a new dashboard and rules to help you monitor GTAP Import Model's health status.

Note: To use this dashboard and rules you must have this log source: GTAP SmartConnector.

Resource Name	Description
/All Rules/ArcSight Foundation/Threat Intelligence Platform/GTAP SmartConnector Health/Error in GTAP SmartConnector Service Message	This rule triggers when the GTAP Model Import Connector has an error receiving or processing a malicious list.
/All Rules/ArcSight Foundation/Threat Intelligence Platform/GTAP SmartConnector Health/No Update from GTAP SmartConnector	This rule triggers when a connector from the Track GTAP Model Import Connector does not update for a time-frame defined by the active list TTL. By default, it is set to show red after two hours.
/All Rules/ArcSight Foundation/Threat Intelligence Platform/GTAP SmartConnector Health/Track GTAP SmartConnector Service Message	This rule tracks the GTAP SmartConnector service message events and adds them to an active list.
/All Dashboards/ArcSight Foundation/Threat Intelligence Platform/GTAP SmartConnector Status	This dashboard shows the latest status of GTAP SmartConnector. It appears red if there is no update for certain time-frame or error messages from the connector, otherwise, it appears green.

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 1.0 SmartConnector
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

Note: You can install the latest version of the package through the console directly without uninstalling the previous version.

To install the package:

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 3.7 Release Notes (ESM 3.7)

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!