opentext™

ArcSight User Behavior Monitoring

Software Version: 1.0

Release Notes

Legal Notices

Open Text Corporation

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

Copyright Notice

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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

ArcSight User Behavior Monitoring (UBM) is a new solution for insider threats, with the previous ArcSight ESM IdentityView solution as a baseline. UBM has been modernized with newer analytics.

> **Note:** As this is a rebranded version of ArcSight ESM IdentityView, the binaries use version number 2.7. As part of the ArcSight portfolio, this initial version of UBM is also known as CE 24.2.

The UBM package maps some existing resources to the MITRE ATT&CK framework, provides optimized dashboards to work better with the ESM ArcSight Command Center, and introduces new resources to monitor user behavior in your environment.

The Privileged User Summary and Top Suspicious Actors Overview dashboards have been optimized to work with the ArcSight Command Center. You can find all of the resources optimized for the ArcSight Command Center in the new ACC Optimized Dashboards folder.

The following table contains all of the new resources added to the UBM package.

Resource Type	Resource Name	Description	Location
Dashboard	Privileged User Summary	Displays important aspects of actors added to privileged groups.	ArcSight Solutions/UBM/ACC Optimized Dashboards/
Dashboard	Threat Score Overview	Displays information about the threat score for each affected user. Before running this dashboard please make sure the following data monitor is enabled: All Data Monitors/ArcSight Solutions/UBM/Overview/Threat Score Overview.	ArcSight Solutions/UBM/Overview/
Dashboard	Top Suspicious Actors Overview	Displays a summary of top threat score actors.	ArcSight Solutions/UBM/ACC Optimized Dashboards/
Query Viewer	Top 20 Locations	Displays the number of actors in each location	/All Query Viewers/ArcSight Solutions/UBM/Actor Management/
Query Viewer	Top 20 Departments	Displays the number of actors in each department.	/All Query Viewers/ArcSight Solutions/UBM/Actor Management/

Updated Content

ArcSight User Behavior Monitoring (UBM) maintains the content previously provided in the IdentityView Package, but has enhanced and optimized the following content.

Optimizing with the ArcSight Command Center

UBM 2.7 optimizes the following resources to work with the ArcSight Command Center.

Resource Name	What Changed	Location
Actors Overview	Optimized to function with ArcSight Command Center and the name changed from Actor to Actors.	/All Dashboards/ArcSight Solutions/UBM/ACC Optimized Dashboards/Actors Overview
Last 20 Actors Added to Privileged Groups	Optimized with ArcSight Command Center.	/All Data Monitors/ArcSight Solutions/UBM/Privileged User Monitoring/Last 20 Actors Added to Privileged Groups

Enhancing with MITRE ATT&CK

UBM 2.7 enhances these rules with the MITRE ATT&CK framework.

Technique	Rule Name
T1110	Account Lockout
T1078	Activity from Badged Out Employee
T1078	Activity from Disabled Actor
T1078	Activity from Rogue Account ID
T1098	Actor Added and Removed From Privileged Group Within a Short Time
T1098	Actor Added to Privileged Group
T1098	Actor Deleted by Interactive Session
T1078	Actor Logged in from Two Countries
T1078	Actor Logged in from non-Windows Single-User Machine
T1078	Actor Logged into non-Windows Server
T1078	Actor Logged into Single-User Windows Machine
T1078	Actor Logged into Windows Server
T1098	Actor Removed From Privileged Group

Technique	Rule Name
T1098	Actor Updated by Interactive Session
T1078	After Hours Building Access by At Risk Actor
T1078	After Hours Database Access by At Risk Actor
T1090.002	Anonymous Proxy Access
T1070.001	Audit Log Cleared
T1189	Compromise - Attempt
T1110	Database Brute Force Login Success
T1078.001	Default Vendor Account Attempt
T1078	Detect Shared Accounts
T1078	Excessive Printing
T1078	Failed Building Access
T1588.002	Hacker Tool Website Access
T1135	IPC Share Browsing
T1005	Leak of Company Information
T1005	Leak of Personal Information
T1136.002	Local Admin Created
T1078	Login to Known Shared Account by Actor
T1110	Multiple Failed Database Access Attempts
T1046	Network Scan
T1098	Non-DBA Added to Oracle DBA Role
T1078	Physical Plus VPN Access
T1078	Printing After Hours
T1078	Printing Confidential Documents
T1078	Printing Suspicious Documents
T1562.001	Security Software Disabled
T1078	Suspicious Activity by Privileged Actor
T1078	Using Different Usernames
T1078	VPN Login from Competition Domain

ESM Requirements

Requires ArcSight ESM 7.6.5 or later.

Downloading and Verifying the Installation Files

To download and verify the signature of your downloaded files:

1. Log in to the host where you want to begin the installation process.
2. Change to the directory where you want to download the installer files.
3. Download the product solution package .arb file: ArcSight-SolutionPackage-UBM-2.7.0.0.12.arb. from the OpenText Downloads website along with their associated signature files (*.sig).

   > ✓ **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).

   Open Text provides a digital public key that is used to verify that the software you downloaded from the Open Text software entitlement site is indeed from Open Text and has not been tampered with by a third party. For more information and instructions on validating the downloaded software, visit the Open Text Code Signing site. If you discover a file does not match its corresponding signature (.sig), attempt the download again in case there was a file transfer error. If the problem persists, please contact Open Text Customer Support.
4. Begin the installation.

Publication Status

Released: NOT RELEASED

Updated: Friday, April 5, 2024

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, contact OpenText Customer Care.

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 Release Notes (User Behavior Monitoring 1.0)

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!