ArcSight Platform 2.3.0 Release Notes

July 2020

ArcSight Platform 2.3.0 (the Platform) enables you to deploy a combination of security, user, and entity solutions into a single cluster within the Container Deployment Foundation (CDF) environment. The core services for this CDF environment, including the Dashboard and user management, are provided by a common layer called Fusion. This release includes the following products:

- ArcSight Command Center for Enterprise Security Manager 7.3.0 - **NEW!**
- ArcSight Interset SE 6.1.0
- ArcSight Recon 1.0.0 - **NEW!**
- ArcSight Transformation Hub 3.3.0
- NetIQ Identity Intelligence 1.1.2

We designed this product in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope that you continue to help us ensure that our products meet all your needs.

The documentation for this product is available on the Documentation website in HTML and PDF formats. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the ArcSight Platform Documentation page or the documentation pages for the included products.

What’s New?

The following sections outline the key features and functions provided in this release. For more information about these enhancements, please see the release notes for the specific product solution.

- “Introducing ArcSight Command Center for Enterprise Security Manager” on page 2
- “Updates for ArcSight Interset SE” on page 2
- “Introducing ArcSight Recon” on page 3
- “Updates for ArcSight Transformation Hub” on page 3
- “Updates for NetIQ Identity Intelligence” on page 4
- “Changes to the Deployed Capabilities” on page 4
- “Introducing the Widget SDK” on page 5

Introducing ArcSight Command Center for Enterprise Security Manager

You can now view ArcSightCommand Center for Enterprise Security Manager (ESM for Fusion) in ArcSight Platform without having to switch to the ESM host for Command Center. When you deploy ESM for Fusion, all Command Center functionality is available from the Platform, with the following limitations:

- On the Logger configuration pages, the search, search filters, and peers functions do not work in Google Chrome. Instead, use Mozilla Firefox. Upon first use, you must clear the browser cache.
- The Tools menu does not work.
- If you enter the Command Center URL directly from ArcSight Platform and the ESM host is not configured, the Command Center login will display.
- To switch to Command Center from the Platform the first time, you must select the Back button three times. After the first time you access Command Center, you must select the Back button twice when you want to switch to Command Center from the Platform.

To use this feature, you must deploy the Fusion and ESM for Fusion capabilities, and then configure the ESM host in the CDF Management Portal. For more information, see the *Administrator’s Guide for Command Center for ESM 7.3* and the *ArcSight Enterprise Security Manager 7.3 Release Notes*.

Updates for ArcSight Interset SE

This release includes the following updates for ArcSight Interset SE:

- “Installation Using Scripts” on page 3
- “Integration with ArcSight Recon” on page 3
- “Support for New Data Types” on page 3

For more information, see the *ArcSight Interset SE 6.1 Release Notes*.

Installation Using Scripts

To enable an easier deployment, Interset provides installation scripts that automatically take care of all the prerequisites, software installations, and post-installation configurations. The scripts are applicable only for single-node, new deployments where high availability is not needed.

For more information about installing using scripts, see the "Deploy Interset Using Scripts" section in the *Interset 6.1.0 Deployment Guide for CDF*.

Integration with ArcSight Recon

You can now leverage the threat-hunting capabilities in Recon by integrating Recon with Interset. In addition to exploring events in Interset, you can gain further insight into events and identify hidden security threats through Recon.

Support for New Data Types

Interset now supports the ingestion and the analysis of the following data types:

- Access
- VPN

Interset also supports the full set of SmartConnectors for those sources that provide data of relevance to the Interset analytics models.

Introducing ArcSight Recon

This release introduces ArcSight Recon 1.0, which replaces ArcSight Investigate in the Platform.

Recon provides a modern log search and hunt solution powered by a high-performance column-oriented, clustered database. The **Search** feature helps you investigate security issues by visualizing search results and identifying outlier events. The **Reports** feature, including MITRE ATT&CK content, enables you to **hunt** for undetected threats as well as create charts and dashboard to visualize filtered data with tables, charts, and gauges. With the Outlier Analytics feature you can identify anomalous behavior by comparing incoming event values to typical values for your environment.

You can upgrade to Recon from Investigate 3.3.0. For more information, see the *Administrator’s Guide for ArcSight Recon*.

For more information, see the *ArcSight Recon 1.0 Release Notes*.

Updates for ArcSight Transformation Hub

This release includes the following updates for Transformation Hub:

- “Now Supports Microsoft Azure” on page 4
- “Can Upgrade More Easily from Prior Versions” on page 4
- “Introduces New CEF-to-Avro Stream Processor” on page 4

For more information, see the documentation for Transformation Hub 3.3.0.

Now Supports Microsoft Azure

You can deploy Transformation Hub on Microsoft Azure to leverage Azure services and capabilities.

Can Upgrade More Easily from Prior Versions

Upgrades to Transformation Hub 3.3.0 from prior version 3.x releases and patches/hotfixes are supported in the native CDF Installer, using rolling upgrades through the Master and Worker Nodes in the cluster.

Introduces New CEF-to-Avro Stream Processor

This release introduces a new CEF-to-Avro stream processor and its supporting topics for ESM events. Using CEF routing rules, ESM can read from a topic of filtered Avro events.

The Avro schema also has been updated such that events may now be stored in a common highly performant database shared by all ArcSight products.

Updates for NetIQ Identity Intelligence

Identity Intelligence now provides REST APIs for integration with third-party applications. You can use the REST API to get information about a user, get access rights details of an identity, and manage views. The REST API documentation contains detailed information for their use.

For more information about accessing the REST API documentation, see "Using Identity Intelligence REST API" in the *Administrator's Guide for Identity Intelligence*. For more information about this release of Identity Intelligence, see the *NetIQ Identity Intelligence 1.2 Release Notes*.

Changes to the Deployed Capabilities

This release includes modifications to a few of the deployable capabilities, including changes in their names. Some of these changes will affect the upgrade process. For example, you might need to deploy the capabilities in a specific order during the upgrade. Be sure to review the release notes and upgrade instructions for your product solution.

- "Fusion Capability Renamed to ArcSight Command Center for ESM" on page 4
- "Analytics Capability Renamed to Fusion" on page 5
- "New Capability Supporting Multiple Layers of Analytics" on page 5

Fusion Capability Renamed to ArcSight Command Center for ESM

ArcSight Command Center for ESM (formerly deployed as *Fusion*) provides dashboards and widgets for ArcSight Enterprise Security Manager use. This updated version of the container also adds some functionality that previously was available only in ArcSight Command Center.

The name of the administrator's guide that explains how to deploy, configure, and manage this product also changed to *Administrator's Guide for Command Center for ESM 7.3*.

Analytics Capability Renamed to Fusion

Fusion (formerly deployed as *Analytics*) now provides the services that are common for most deployed products. This container supports user management, single sign-on, dashboard, and other core services that the products deployed in ArcSight Platform need for a unified solution experience. The user's guide embedded with Fusion also changed its name to better demonstrate the functionality that it supports.

All products deployed in the Platform, except Transformation Hub, require Fusion as part of the deployment. If you use the provided scripts to deploy your product, the script also deploys Fusion. For more information about using Fusion, see the Help in the product or the *User's Guide for Fusion*.

New Capability Supporting Multiple Layers of Analytics

The new **Layered Analytics** capability provides the analytic results from other capabilities deployed in this suite, thus providing multiple layers of useful data that can lead to actionable insights. With this capability, you can use widgets that combine data from two or more deployed products. For example, the *Active Lists* widget can display data for both ArcSight Interset SE and ESM for Fusion.

You can deploy Layered Analytics with ArcSight Interset SE and ESM for Fusion. The deployment scripts do not deploy this capability. You must manually deploy Layered Analytics.

Introducing the Widget SDK

This release introduces the **Widget Software Development Kit** (the Widget SDK), which enables you to build new widgets for the Dashboard or modify existing widgets for deployed solutions. The entitlement for your deployed product also grants you access to the Dashboard and to the Widget SDK. You can download the Widget SDK to your local production or test environment to start creating custom widgets.

For more information about using the Widget SDK, see the Administrator's or Deployment Guide for your product solution.

Technical Requirements

For more information about the basic software and hardware requirements, which apply to the commonly needed Fusion component, see the *Technical Requirements for ArcSight Platform*. You can also access the *Technical Requirements* for the individual solutions that you might want to deploy from the ArcSight documentation site.

Downloading and Installing the ArcSight Platform Capabilities

You can download the installation packages for the products in the ArcSight Platform from the Micro Focus Downloads site. The installation packages include their respective signature files for validating that the downloaded software is authentic and not tampered by a third party.

Micro Focus provides several options for deploying products in your environment. For more information about downloading and deploying, see the documentation associated with your chosen solution.

Licensing Information

For information about activating a new license, see the Administrator's or Deployment Guide provided with the product.

Known Issues

We are currently researching the following issues that are common to all capabilities that you can deploy in the ArcSight Platform.

Micro Focus strives to ensure that our products provide quality solutions for your enterprise software needs. If you need assistance with any issue, visit Micro Focus Support (https://www.microfocus.com/support-and-services/), then select the appropriate product category.

- "Malware Scan Might Report a False Positive" on page 6

Malware Scan Might Report a False Positive

Issue: When scanning the `cdf-2020.05.00100-2.3.0.7.zip` file or an installer `*.tar` file that contains this file, certain malware detection programs might report a false positive in a subroutine called `updateRoleId`. This subroutine is within `/cdf/images/cdf-master-images.tgz` file.

Workaround: None needed. We validated that the code is not malware. We have verified that the package was built and compiled in a secure and trusted fashion. In an coming release, we will modify the packaging to avoid this false positive.

Contacting Micro Focus

For specific product issues, contact Micro Focus Support at https://www.microfocus.com/support-and-services/.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos: https://www.microfocus.com/support-and-services/
- The Micro Focus Community pages: https://www.microfocus.com/communities/

Legal Notice

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/.