Micro Focus Security ArcSight Investigate

Software Version: 2.20

Release Notes

Document Release Date: February 13, 2019
Software Release Date: June, 2018

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) 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. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

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://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Introduction

ArcSight Investigate enables you to search, analyze, and visualize machine-generated data gathered from such entities as websites, applications, sensors, and devices that comprise your IT infrastructure or business.

After Investigate ingests the data stream of individual events from Event Broker, you can view and search.

You can use the English-like search language to create searches.

What's New in this Release

The following new features and enhancements are included in this release.

SOAR Application Integration

ArcSight Investigate now supports integration with selected SOAR (Security Orchestration, Automation and Response) applications, including Demisto, Operations Orchestration, or Siemplify Enterprise. SOAR applications enable enterprises to automate their IT and security operations. When integrated with other applications and network devices, SOAR applications can orchestrate an automatic or manual response to an IT or security event in the enterprise network. SOAR applications provide a single-pane-of-glass view for the enterprise network operations personnel.

DNS Analytics

New pre-set visualizations let you track and analyze DNS and DGA events.

Debug Log Level Adjustment

You can now set ArcSight Investigate log levels for different degrees of information.

For details about these features, see the ArcSight Investigate 2.20 User's Guide, available from the ArcSight Product Documentation Community on Protect 724.]

Resolved issues are described under "Fixed Issues" on page 1.

Available documentation

In addition to the release notes, the following ArcSight Investigate documentation is available on Protect 724.

Document	Description
MicroFocus Security ArcSight Investigate Deployment Guide	Specifies requirements for Investigate. Describes the technology used in Investigate and how the product works. Also, describes the deployment architect and scenarios. How to deploy and implement Event Broker as part of the solution is also described. "Support Matrix" section provides details on support for ArcSight Investigate, browser support, and product compatibility.
MicroFocus Security ArcSight Investigate User's Guide	Addresses the needs of both analysts and administrators. Describes the technology and features used in Investigate and how the product works. Also describes product functions based on workflow.

Upgrading to ArcSight Investigate 2.20

ArcSight supports an upgrade from ArcSight Investigate 2.10 to version 2.20. Upgrading involves updating the Vertica database, Investigate containers, Event Broker, and ArcSight Installer. Ensure to update the last three of these from the ArcSight Installer (see the MicroFocus Security*ArcSight Event Broker Deployment Guide*).

For upgrade details, see the MicroFocus Security *ArcSight Investigate Deployment Guide*.

Fixed issues

The following issues are fixed in this release.

Issue	Description
HERC-5902	An issue has been resolved where using the right-click menu option, "Get Authentication User" from Events table would return an error: "Failed to Execute Search". The search will proceed normally.
HERC-5900	An issue has been resolved where after an upgrade, the retention policy would be broken.
HERC-5888	For all charts with Bytes in and Bytes out fields having null values, the charts are now rendering after refreshing in the Dashboard page.
HERC-5886	Drag and drop for IP, MAC, and IPv6 fields from the Events table to filters now works correctly.
HERC-5865	An issue has been resolved where multiply selecting saved results and then deleting them would cause an error.
HERC-5831	A newly saved search will now not appear in the Saved Results when you initially navigate away from the search and onto the Saved Results page.
HERC-5789	There is no longer any delay from the time you save a search and when it appears in Saved Results of the left navigation area.
HERC-5747	When exporting to a CSV file, the sorting and column positions are now retained correctly.
HERC-5746	An issue has been resolved where exported event table data to a CSV would have the suffix "Bin." The suffix will no longer appear.
HERC-5706	An issue has been resolved where a long query for a saved search would not appear cleanly in the Saved Result page.
HERC-5026	Getting authenticated users using null or empty values will no longer result in a bad query.

Open issues

This release contains the following open issues.

Issue	Description
HERC-7707	There is a known issue with the 7.10.x Microsoft DNS Trace Log Connector and 7.11.x Microsoft DNS DGA Trace Log Connectors, where events are not correctly flagged for the Investigate DNS Analytics reports. Until this is addressed in the Connector, use the Connector versions 7.8.x or 7.9.x Microsoft DNS Trace Log Connector if you want to flag events for the DNS Analytics feature.
HERC-6570	When using multiple windows, a saved search created in one window can be fully deleted from left side menu in the other window
HERC-6569	On the DNS analytics dashboard, the DGA table widgets shown when clicking the table widget flipping button fail to work correctly. Workaround: To view DGA data, use the chart widgets.
HERC-6415	When creating a lookup list, if there is an error in the CSV file, the page continues to show the loading icon without displaying an error message in the page. Workaround: 1. Navigate away from the lookup page, to stop the process. 2. Fix the issues in the CSV file. 3. Upload the CSV file again.
HERC-6412	After plotting a graph, if there is a significant number of ticks and tick labels in the x axis of a graph, the labels are not readable. Workaround: Hover on each tick label to read the text.
HERC-6406	The Dashboard order by chart widget does not pause even if its original search has finished the first chunk. As a result the widget does not shows the same data as the original search, as it has not been refreshed. Workarounds: -Add the visualization to the Dashboard before the search is completed. - Refresh from global button in dashboard. -Zoom in/out to force the chart to reload.
HERC-6403	This issue happens intermittently when you have two different browsers open and you are logged in to Investigate in both using the same credentials. If you delete all Two instances of a new default search will be created. One is healthy, and the second returns an error. Workaround: Delete the search that returns the error. This does not create any issues in the Investigate system.
HERC-6350	On Firefox, you may see user interface layout inconsistencies. These will be fixed in a future release.
HERC-6349	On Firefox, you may see user interface layout inconsistencies. These will be fixed in a future release.
HERC-6302	In some cases, when viewing visualization fields in Firefox, mousing over the field will cause the field display to move between columns.

Issue	Description
HERC-6121	Intermittently, the tImeline is not updated when moving to saved search and changing the search. Workaround: Rerun search, to recover correct count for timeline.
HERC-5901	After deployment or upgrade, browsing to https://master-ip fails. Intermittently, you may get an error such as a 502 or 504 type. Workaround: Delete arcsightinvestigate1 nginx-ingress-controller-* pod and wait for a new pod to be created. If deployment or upgrade still fails, repeat the operation.
HERC-4687	In the Firefox browser, if you log out of ArcSight Investigate from the Search page, you are not redirected to the login page and an error message appears. Workaround: Navigate from the Search page to Dashboard Page. Then logout from Investigate and the system will display the login page without showing any errors.
HERC-3836	Issue: For an ESM - ArcSight Investigate integration search, launching Investigate from ESM to search for Empty Device Custom Floating Point values will show the following query in the search query field: deviceCustomFloatingPoint1 = '' , Null The single quotes in this query will not allow the search to run and will display an error. Workaround: Remove the single quote from the query and run the search using the following query: deviceCustomFloatingPoint1 = Null

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 (Investigate 2.20)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!