



ArcSight Threat Detector

Software Version: 2.10

Release Notes

Document Release Date: July 11, 2017

Software Release Date: July 11, 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise 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

© Copyright 2001-2023 Hewlett Packard Enterprise Development, LP

Follow this link to see a complete statement of copyrights and acknowledgements:

<https://community.softwaregrp.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228>

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

- Threat Detector 2.10 4
 - Overview 4
 - What's New 4
 - Release Contents 5
 - Requirements 5
 - Installing Threat Detector 5
 - Pattern Discovery Considerations 5
 - Open Issues in this Release 6

- Publication Status 7

- Send Documentation Feedback 8

Threat Detector 2.10

The release notes provides the following topics:

- ["Overview" below](#)
- ["Release Contents" on the next page](#)
- ["Requirements" on the next page](#)
- ["Installing Threat Detector" on the next page](#)
- ["Pattern Discovery Considerations" on the next page](#)
- ["Open Issues in this Release" on page 6](#)

Overview

The Threat Detector solution, powered by ArcSight Pattern Discovery, helps you detect subtle, specialized, or long-term patterns in the flow of events. The Threat Detector product license enables the Pattern Discovery feature. Threat Detector provides the following Pattern Discovery profiles:

- AV Activity Profiler
- Browsing Pattern Detector
- Distributed Attacks Detector
- Early Stage Attack Detector
- Penetration Attempts

For an explanation of the profiles and information about using them, see the *Threat Detector 2.10 Solution Guide*.

What's New

The purpose of this release is to provide performance guidelines and configuration information for using the Threat Detector Pattern Discovery profiles. For details, see ["Pattern Discovery Considerations" on the next page](#).

Release Contents

The files included in this release are:

File name	Description
ESM_ThreatDetector_Solution_RelNotes_210.pdf	<i>Threat Detector 2.10 Release Notes</i> — Product description and open issues (this document).
ESM_ThreatDetector_SolutionGuide_210.pdf	<i>Threat Detector 2.10 Solution Guide</i> — Product architecture, installation, configuration, and operation instructions.
ArcSight-SolutionPackage-ThreatDetector.2.10.1282.0.arb	Contains all of the resources in the Threat Detector solution. Installable package for all operating systems. Note: If you use Internet Explorer to download the ARB file, it might convert the ARB file to a ZIP file. If this occurs, rename the ZIP file back to an ARB file before importing into ESM.

Requirements

Threat Detector 2.10 is supported on:

- ArcSight ESM 7.0 or later
- ArcSight ESM 6.0c with CORR-Engine or later
- ArcSight Express 4.0 with CORR-Engine or later

Installing Threat Detector

For installation and configuration instructions, see the [Threat Detector 2.10 Solution Guide](#).

Pattern Discovery Considerations

Using Pattern Discovery can cause performance degradation when discovery is performed over a large number of matching events in a high EPS environment. When using an environment with high EPS, define a filter to limit the events sent for Pattern Discovery processing to be less than 1000 EPS.

On supported ArcSight systems using Oracle, all of the Threat Detector Pattern Discovery Profiles support approximately 1,000 matching events per second (EPS).

On supported ArcSight systems using CORR-Engine, the profiles support approximately 1,000 matching EPS, but the following configuration is required to ensure acceptable performance:



Note: If `/opt/arcsight/logger/data/mysql/my.cnf`, `sort_temp_limit = 64G` is the default value, skip step 1 and 2.

1. On the ArcSight Manager, edit the `my.cnf` file located in `/opt/arcsight/logger/data/mysql` and increase the sort space to 30G, as shown below:
sort_temp_limit = 30G
2. Stop and restart all of the ArcSight services for the increase to take effect, by running the following commands:

```
/sbin/service arcsight_services stop manager /sbin/service arcsight_services start manager
```

To check the status of the services, run the following command:

```
/sbin/service arcsight_services status all
```
3. In the ArcSight Console, edit the Threat Detector profiles and decrease the **Start Time** to one hour (`$Now-1h`).
4. Run the profiles (right-click a profile, and select **Take Snapshot**).

For more information about editing and running the profiles, see the *Threat Detector 2.10 Solution Guide*.



Note: The EPS numbers provided above are only guidelines and might vary from system to system.

Open Issues in this Release

The following issues are open in this release.

Issue	Description
ESM-35048	A <code>java.lang.InterruptedExcep</code> tion might be logged in the ArcSight Manager <code>server.std.out.logs</code> file when a scheduled Pattern Discovery job is run. The exception is caused by an incorrect database pooling time-out mechanism in the ArcSight Manager. This does not have any adverse effect on database connections or the functionality of the Pattern Discovery job, and the exception can be safely ignored.
NGS-3527	Pattern Discovery jobs can be resource intensive. Pattern Discovery jobs can cause a degradation in performance, and may fail to return a matching result set. OpenText recommends that you reduce the number of events over which the Pattern Discovery search runs and/or the frequency of Pattern Discovery jobs. For more information, see " Pattern Discovery Considerations " on the previous page.

Publication Status

Released: July 11, 2017

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 (Threat Detector 2.10)

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!