M007 Maintenance Report

File name: ISCB-5-RPT-M007-AMR-v1
Version: v1
Date of document: 14 July 2017
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726630-U)

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan

M007 Maintenance Report

14 July 2017

ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines,
No 7 Jalan Tasik,The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 Fax: +603 8992 6841
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	M007 Maintenance Report
DOCUMENT REFERENCE:	ISCB-5-RPT-M007-AMR-v1
ISSUE:	v1
DATE:	14 July 2017

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:
Level 5, Sapura@Mines
No 7, Jalan Tasik,
The Mines Resort City,
43300 Seri Kembangan
Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee
Company No. 726630-U

Printed in Malaysia

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	13 July 2017	All	Initial draft
v1	14 July 2017	Table 1, Section 2, Section 4	Change developer's address, change format, update information.

Table of Contents

1 Introduction

1 The TOE is ArcSight Enterprise Security Management (ESM) version 6.11.0 from Hewlett Packard Enterprise. ArcSight ESM is a Security Information and Event Management (SIEM) solution that combines event correlation and security analytics to identify and prioritize threats in real time and remediate incidents early. It is able to concentrate, normalize, analyse and report the results of its analysis of security event data generated by various Instrusion Detection System (IDS) sensors and scanners in the operational environment. ArcSight ESM allows users to monitor events in real-time, correlate events for in-depth investigation and analysis and resolve events with automated escalation procedures and actions.

2 The purpose of this document is to enable developers to provide assured products to the IT consumer community in a timely and efficient manner against the certified and updated version of TOE as in table 1 identification below.

3 Identification Information

Table 1 – Identification Information

Assurance Maintenance Identifier	M007
Project Identifier	C076
Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Impact Analysis Report	Impact Analysis Report – HPE Security ArcSight ESM
New TOE	HPE Security ArcSight ESM 6.11.0
Certified TOE	HPE Security ArcSight ESM 6.9.1c
New Security Target	HPE ArcSight ESM Security Target
Evaluation Level	EAL2
Evaluation Technical Report (ETR)	Evaluation Technical Report – HPE ArcSight ESM v6.9.1c EAU000426-S035ETR – Version 1.2, 6 December 2016
Criteria	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, September 2012, Version 3.1, Revision 4 Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, September 2012, Version 3.1 Revision 4
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref[VIII])
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL2

Protection Profile Conformance	None
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive Columbia, MD 21046
Developer	Hewlett Packard Enterprise 1160 Enterprise Way Sunnyvale, CA 94089
Evaluation Facility	BAE Systems Applied intelligence - MySEF

2 Description of Changes

4 Hewlett Packard Enterprise (HPE) has issued a new release of the HPE Security ArcSight ESM version 6.11.0. There were a series of minor updates to the HPE Security ArcSight ESM since its certification version 6.9.1c of 14 December 2016.

2.1. Changes to the product associated with the certified TOE

5 The following features have been added in HPE Security ArcSight ESM v6.11.0 (Ref [I]):

Table 2 – General changes/additions

Change	Description
FIPS Compliance Enhancement	ESM uses Bouncy Castle Java cryptography which replaces Mozilla Network Security Services (NSS). Bouncy Castle enables the support of TLS 1.2 in FIPS mode as well as in Default mode.
IPv6 Connectivity Support	ArcSight components such as Console, Command Center, Web Service Layer APIs, Forwarding Connector, SmartConnectors (which is including hosted on the ArcSight Management Center) and High Availability ESM clusters can communicate with each other using IPv6 communication – both in dual (IPv4/IPv6) and IPv6-only modes.
IPv6 Data Support	ArcSight is using latest SmartConnectors which is supporting both IPv4 and IPv6 and updated parsers, all address fields (such as Attacker, Source, Target, Destination and so on) in the ESM schema now display IPv4 or IPv6 address as appropriate.
Region (Geo) Codes	The region code standard is now based on ISO 3166-2. This standard includes support for IPv4 and IPv6 addresses. Not all IPv6 addresses are mapped to a region code.
Zones	For accurate asset modeling, system-supplied zones have been updated to include IPv6 addresses. In the ArcSight Console, you now have /All Zones/ArcSight System IPv6. This category has its own list of addresses for Dark Address Space, Private Address Space, and Public Address Space Zones specific to IPv6 addresses. The existing /All Zones/ArcSight System continues to include IPv4 addresses.
Field-Based Active and Session Lists	The Address data type was enhanced to support an IPv4 or IPv6 address value. IPv6 addresses are presented in simplified format, if applicable. A new data type, MAC address, is added for MAC address values.

Integration Commands	The following network tools have been added to support IPv6: • NsLookup-IPv6 (Linux) • Ping6 (Linux) The legacy NsLookup (Linux) and Ping (Linux) commands are still available for IPv4 addresses. The legacy NsLookup (Windows) and Ping (Windows) will ping both IPv4 and IPv6 nodes.
New Variable Functions	The following function is introduced in this release: • RoundN This function takes a double and rounds it off to the specified number of decimal places, from 0 to 5. Use RoundN to make long decimal numbers more readable on the Viewer or on reports, for example.
Variable Functions Enhancements	The following functions are enhanced to accept either an IPv4 or IPv6 address as input. These include: • ParseIPAddress • ConvertAddressToString • ConvertStringToIPAddress The old ConvertStringToIPv6Address is now removed from Type Conversion functions.
Integration with ArcSight Investigate	You can run searches on ArcSight Investigate from the ArcSight Console and ArcSight Command Center.
MSSP Reports on EPS Consumption	Two reports (one monthly and one daily) that track EPS (events per second) consumption per customer (tenant) are now available from the ArcSight Marketplace at: • https://marketplace.saas.hpe.com/arcsight These reports are specifically for our managed security service providers (MSSP) partners.
High Availability Primary Manager as Source of Forwarded Events	In the previous release, the primary ArcSight Manager in a High Availability ESM cluster could only be the destination of forwarded events. In ESM 6.11.0, the primary Manager can now be the source of events, and the forwarding function is picked up by the secondary Manager during a failover.
Web Service Layer APIs	The following fields have been added to support IPv6 addresses: • addressAsBytes • translatedAddressAsBytes The legacy address and translatedAddress fields are still available for backward compatibility.
Enable Scaling for Bytes In and Bytes Out Event Fields	A server property is introduced in this release: bytesInBytesOut.scaling.divider

	The property is set to 1 by default. If this value is set to be greater than 1, the values for Bytes In and Bytes Out event fields are scaled, and are saved in ESM in the scaled units.
Forwarding Connector	The Forwarding Connector bundled with ESM6.11.0 has the ability to forward events containing IPv4 or IPv6 addresses. If the destination is ESM6.11.0, the IPv6 addresses are forwarded to the address fields (for example, Attacker, Source, Target, Destination, and so on). If the destination ESM's version is earlier than ESM6.11.0, then the IPv6 addresses are forwarded to deviceCustomIPv6Address fields 1- 4.
Event Broker	ESM can now be a destination for ArcSight Event Broker 2.0. The destination configuration is done with SmartConnectors, followed by Manager integration done during ESM installation or Manager setup. Refer to the HPE Security ArcSight Data Platform Event Broker Administrator's Guide for deployment details. ESM provides data monitors and audit events to monitor Event Broker connectivity and forwarding status.

Table 3 – ArcSight Command Center changes/additions

Change	Description
Dashboard Navigator	The Dashboard Navigator has been enhanced to provide a streamlined view of dashboards, with navigation similar to that of active channels.
Query Viewers	Previously, only query viewers in tabular format were available on the Command Center dashboard page. Now, query viewers in chart format are also available.
Data Monitor Enhancement on the Dashboard and Dashboard Navigator	All data monitor types are now available in the Command Center. Note that the geographical graph is now available.
Event Graph Enhancement Dashboard Navigator page - Topology Graph	A variation of the Event Graph that displays event endpoints in relation to each other, in terms of Source Nodes, Event Nodes, and Target Nodes. This graph allows you to explore the relationships and connections among the nodes. Hover over a node to highlight that node's connections. Click individual

	nodes to drill down and explore the relationships among the nodes.
Field Summary Address Fields Are Now Strings	Previously, all Field Summary address fields were treated as numbers; these fields are now treated as strings to accommodate IPv6 addresses.
Save Dashlets as CSV Files	You can now save dashlets as CSV files.
Dark Theme	The Command Center now provides the ability to switch the web interface to a dark theme. The dark theme reduces glare from the screen, therefore providing visual comfort in dark room environments.
Navigate from a Dashboard to a Channel	You can now drilldown directly to a channel, view that channel, and save it as a resource.
Access Integration Commands from an Event List	You can now access Integration Commands directly from event links in an Active Channel Event List.
Access ArcSight Investigate from an Event List	You can now access ArcSight Investigate directly from four areas of the ArcSight Command Center interface. These access options are enabled on the Command Center user interface if ESM is configured to integrate with ArcSight Investigate, and are available in: • Event links in an Active Channel Event List. The commands available are: o ArcSight Investigate o ArcSight Investigate (Multiple Fields) • Event Details, for supported ArcSight Investigate fields. The commands available are: o ArcSight Investigate o ArcSight Investigate (Multiple Fields) • Event Visualization; click to access ArcSight Investigate for supported ArcSight Investigate fields. • Dashboards; click to access ArcSight Investigate for supported ArcSight Investigate fields. Additionally, there is a new integration command in /All Integration Commands/ArcSight Administration/ArcSight Investigate. With this integration command, you have two options: • By Source and Destination • By Vendor and Product

Case Descriptions in a Separate Dialog	Case descriptions now display in a separate, fully controllable dialog window so you can read the entire case description.
Storage Group - Ability to Manually Add Connectors	The Command Center now allows you to manually add a connector that you specify using the connector ID provided through the Event Broker when you add a Storage Mapping.

Table 4 – ArcSight Console changes/additions

Change	Description
Dark Theme	The Console now provides the ability to switch the graphical interface to a dark theme. The dark theme reduces glare from the screen, therefore providing visual comfort in dark room environments.
Advanced Selector for a Resource Attribute	Some resources need a resource attribute. For example, a query viewer needs a query to get data from the database. The Advanced Selector button on source resources' Edit panel provides the option to search, then select the resource.
Recents and Favorites in Navigator Panel	For active channels, actors, assets, and cases, the resource Navigator panel now includes two panels: Recents and Favorites. The Recents list is automatically populated, and you add resources to Favorites.
Integration with ArcSight Investigate	• ArcSight Investigate • ArcSight Investigate (Multiple Fields) These options are enabled on the Console UI's active channel or the event details' Inspect/Edit panel if ESM is configured to integrate with ArcSight Investigate. On the Console, the existing Investigate option associated with a specific event on an active channel is now renamed Analyze in Channel. Additionally, there is a new integration command in /All Integration Commands/ArcSight Administration/ArcSight Investigate • "Running ArcSight Investigate Searches" to run from an active channel or from the event details' Inspect/Edit panel. "Using the ArcSight Investigate Integration Commands" to define target parameters and search by source and destination, or by vendor and product.

6 There are no significant changes to secure delivery and distribution site, configuration management procedures, site security procedures and configuration management tools used to develop the TOE (Ref [II]).

3 Affected Developer Evidence

7 The affected developer evidence submitted for the assurance continuity required by the CCRA Assurance Continuity: CCRA Requirements Version 2.1 (2012-06-01) June 2012 are:

a) HPE Security ArcSight ESM Security Target version 1.3

b) HPE Security ArcSight ESM Software version 6.11.0 Release Notes

c) HPE Security ArcSight ESM Architecture Design version 0.6

d) HPE Security ArcSight ESM Functional Specification version 0.8

e) HPE Security ArcSight ESM Architecture Description version 0.6

4 Result of Analysis

8 The outcome of the review found that none of the modifications significantly affects the security mechanisms that implement the functional requirements of the Security Target (Ref [III]) as required in accordance of Assurance Continuity: CCRA Requirements version 2.1 (2012-06-01) June 2012 (Ref [IV]).

9 The nature of the changes leads to the conclusion that they are classified as minor changes. Therefore, it is agreed based on the evidences given that the assurance is maintained for this version of the product.

Annex A References

[I] Impact Analysis Report (IAR), EAU000426.08-IAR 1.0, 19 June 2017.

[II] Hewlett Packard Enterprise Secure ArcSight ESM Security Target, version 1.3, 13 June 2017 – version 6.11.0.

[III] Hewlett Packard Enterprise Secure ArcSight ESM Security Target, version 1.0, 21 October 2016 – version 6.9.1c.

[IV] Assurance Continuity: CCRA Requirements Version 2.1 (2012-06-01) June 2012

[V] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July 2014.

[VI] The Common Criteria for Information Technology Security Evaluation, version 3.1, Revision 4, September 2012.

[VII] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[VIII] MyCC Scheme Policy (MyCC_P1), v1e, August 2016.

[IX] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1d, August 2016.

[X] C076 Evaluation Technical Report – HPE ArcSight ESM v6.9.1c, EAU000426-S035-ETR, version 1.2, 6 December 2016.

--- END OF DOCUMENT ---