C076 Certification Report

Hewlett Packard Enterprise ArcSight ESM

File name: ISCB-5-RPT-C076-CR-v1
Version: v1
Date of document: 14 December 2016
Document classification : PUBLIC

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

C076 Certification Report

Hewlett Packard Enterprise ArcSight ESM

14 December 2016

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:	C076 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C076-CR-v1
ISSUE:	v1
DATE:	14 December 2016

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

The copyright of this document, which may contain proprietary information, is the property of CyberSecurity Malaysia.

The document shall be held in safe custody.

©CYBERSECURITY MALAYSIA, 2016

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

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 14 December 2016 and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associated certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	25 November 2016	All	Initial draft of certification report
d2	6 December 2016	All	Second draft version of certification report
v1	14 December 2016	All	Final version of certification report

Executive Summary

The TOE is ArcSight Enterprise Security Management (ESM) 6.9.1c from Hewlett Packard Enterprise (HPE). 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, analyze, and report the results of its analysis of security event data generated by various Intrusion 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.

The scope of the evaluation is defined by the Security Target (Ref [6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security function requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by BAE Systems Applied Intelligence MySEF (Malaysia Security Evaluation Facility) and completed on 4th November 2016.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that HPE ArcSight ESM v6.9.1c (ESM) meets their requirements. It is recommended that a potential user of the TOE refers to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 HPE ArcSight ESM v6.9.1c (the TOE) is a Security Information and Event Management (SIEM) solution that normalizes and aggregates data from devices across the enterprise network, provides tools for analysis and investigation, and offers options for automatic and workflow-managed remediation. The TOE provides authorized users with capabilities to monitor events, correlate events for in-depth investigation and analysis, and resolve events with automated escalation procedures and actions.

2 ArcSight ESM is deployed in the enterprise network. It uses entities called ArcSight SmartConnectors to gather event data from the network. SmartConnectors translate event data from devices into a normalized schema that becomes the starting point for correlation. SmartConnectors are outside the TOE boundary.

3 The functionality defined in the Security Target that was subsequently evaluated is as follows:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channels
- Intrusion Detection System

1.2 TOE Identification

4 The details of the TOE are identified in Table 1 below.

Table 1: TOE Identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C076
TOE Name	HPE ArcSight ESM v6.9.1c (ESM)
TOE Version	6.9.1c
Security Target Title	ArcSight ESM v6.9.1c
Security Target Version	Version 1.0
Security Target Date	21 October 2016
Assurance Level	Evaluation Assurance Level 2
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [2])

Methodology	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL 2
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive, Columbia 21046 MD
Developer	Hewlett Packard Enterprise HP Moffett Towers Building, 1140 Enterprise Way, Sunnyvale 94089 CA
Evaluation Facility	BAE System Applied Intelligence MySEF

1.3 Security Policy

5 There are no organisational security policies that have been defined regarding the use of the TOE.

1.4 TOE Architecture

6 The TOE includes both logical and physical boundaries as described in Section 2 of the Security Target (Ref [6]).

7 The TOE architecture consists of the following components:

- ArcSight Manager
- CORR-Engine (Correlation Optimized Retention and Retrieval Engine)
- ArcSight Console
- ArcSight Command Center (ACC)
- ESM Service Layer APIs.

8 The ArcSight Manager, CORR-Engine, and ArcSight Command Center web server are installed on the same server. The ArcSight Manager processes and stores event data in the CORR-Engine. Users monitor events using ArcSight Console (a workstation-based application) or the ArcSight Command Center (a web-based interface), which can run reports, develop resources, and perform investigation and system administration. In addition, ESM Service Layer APIs expose ESM functionality as web services, enabling users to integrate ESM functionality into their own applications. The primary means for authorized users to interact with the TOE is via the ArcSight Console or the ArcSight Command Center.

9 The ArcSight Manager and ArcSight Console components also rely on properties files that are stored in the file system of the underlying operating system supporting that component.

10 The TOE can be configured in either of two modes: non-FIPS mode (the default mode); and FIPS 140-2 compliant mode. The configured mode determines the cryptographic protocols

and the underlying cryptographic provider the TOE uses to implement secure communications. In non-FIPS mode, the TOE supports secure communications using TLS v1.0 (the default), TLS v1.1, or TLS v1.2.

11 The following figure illustrates how the TOE components can be deployed in a network.

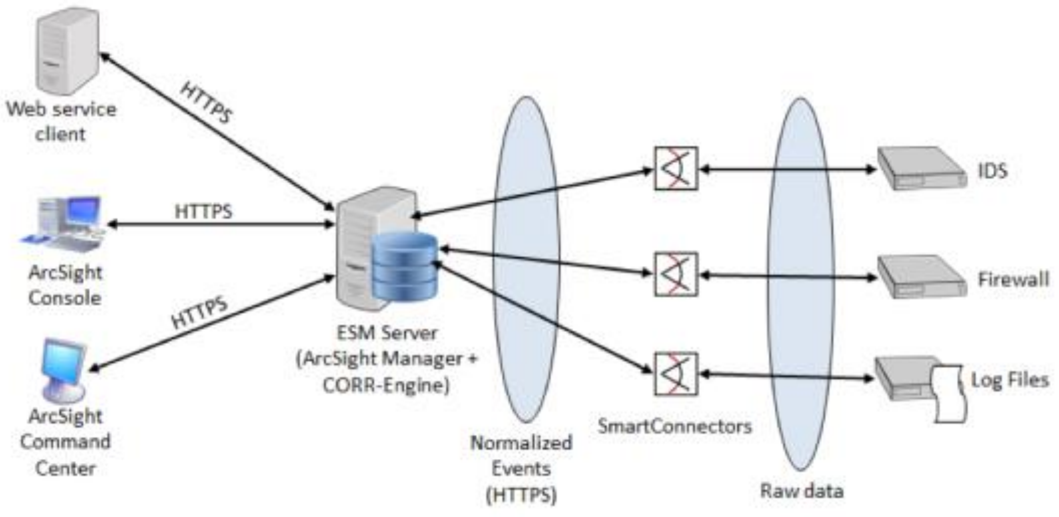

Figure 1: Example of TOE Deployment

1.4.1 Logical Boundaries

12 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

- Security audit
- Identification and authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channels
- Intrusion Detection System

13 **Security Audit:** The ArcSight Manager is able to generate audit records of security-relevant events, which it stores in CORR-Engine. The stored audit records are protected by CORR-Engine from unauthorized modification and deletion. The TOE provides Administrators and Analyst Administrators with capabilities to review the generated audit records, including capabilities for sorting audit records based on such characteristics as date and time the event is recorded, the type of audit event, the subject associated with the audit event, and the outcome of the event.

14 **Identification & Authentication:** The TOE maintains accounts of the authorized users of the system. The user account includes the following attributes associated with the user: user

identity; authentication data; authorizations (groups or roles); and e-mail address information. This information is stored in CORR-Engine. The TOE supports both passwords and certificates for authentication and users can be configured for password-only, certificate-only, password or certificate, and password and certificate. The TOE enforces restrictions on password structure, including minimum length and minimum number of different character types (i.e., alphabetic, numeric, special).

By default, the TOE allows a maximum three consecutive failed login attempts, after which the user account is locked for 10 minutes. The TOE requires users to provide unique identification and authentication data before any access to the TOE via the ArcSight Console or the ArcSight Command Center is granted. Users have the ability to terminate their own interactive sessions by logging out of the ArcSight Console or ArcSight Command Center. Users that have been identified and authenticated by the underlying operating system are able to execute a limited set of shell commands for ArcSight Manager and ArcSight Console, although some of these commands also require entry of a user identity and matching password.

15 **Security Management:** The TOE provides the following default security management roles: Administrator; Analyzer Administrator; Operator; and Analyst. The TOE enforces restrictions on which management capabilities are available to each role. Administrators and Analyzer Administrators are able to modify the behavior of the IDS analysis and reaction function. Only the Administrator role is able to manage user accounts and to modify passwords of other users. The TOE's security management functions are accessible via the ArcSight Console and ArcSight Command Center.

16 **Protection of the TSF:** The TOE uses HTTPS to protect TSF data communicated between the ArcSight Console and the ArcSight Manager components of the TOE.

17 **Trusted Path/Channels:** The TOE provides a trusted channel between itself and the following external IT entities that protects transmitted information from disclosure and modification:

- Web service clients—connect to the TOE via the TOE's Service Layer APIs. All such connections are made over HTTPS.
- SmartConnectors—SmartConnectors establish HTTPS connections with the TOE to forward events to the TOE.

The TOE provides a trusted path for TOE administrators to communicate with the TOE. The trusted path is implemented using HTTPS for access to the ArcSight Command Center. Administrators initiate the trusted path by establishing an HTTPS connection (using a supported web browser). The trusted path is used for initial authentication and all subsequent administrative actions. The use of HTTPS ensures all communication over the trusted path is protected from disclosure and modification.

18 **Intrusion Detection System:** The TOE collects information from network sources and subjects it to statistical and signature-based analysis, depending on configured rules. Rules trigger responses either on first match or after a given threshold has been passed. Notification destinations (e.g., authorized users) can be configured to be notified of a triggered rule at the GUI (ArcSight Console or ArcSight Command Center) or via e-mail. The authorized users can view all event information from the IDS data. To prevent IDS data loss, a warning is sent to a configured e-mail destination should CORR-Engine begin to run out of storage space for IDS data. The default setting for generating this notification is 90% of capacity. If no action is

taken to address the warning, an error is sent if IDS storage exceeds the configured error threshold (95% by default).

1.4.2 Physical Boundaries

19 ArcSight ESM is a software product provided in the following form:

ArcSightESMSuite-6.9.1.2022.0.tar file, the software distribution and installation file for the ArcSight Manager, CORR-Engine, ArcSight Command Center and Service Layer API components.

ArcSight-6.9.1.2195.0-Console-Win.exe, a self-extracting archive file and installer for the ArcSight Console.

ArcSight-6.9.1.2195.0-Console-Linux.bin, a self-extracting archive file and installer for the ArcSight Console on Linux.

20 The ArcSight ESM suite (ArcSightESMSuite-6.9.1.2022.0.tar) can be installed on 64-bit Red Hat Enterprise Linux (RHEL) 6.7 or 7.1 and CentOS 6.7 or 7.1. The following browsers are supported for accessing the ArcSight Command Center:

- Internet Explorer 11 on Windows
- Safari 8.x on Mac OS X
- Firefox 38 ESR on Linux, Windows and Mac OS X
- Chrome (latest version) on Windows.

21 The ArcSight Console for Windows (*ArcSight-6.9.1.2195.0-Console-Win.exe*) is supported on the following platforms in the evaluated configuration: Windows Server 2012 R2, 64-bit; Windows 7 and 8.1, 64-bit.

22 The ArcSight Console for Linux (*ArcSight-6.9.1.2195.0-Console-Linux.bin*) is supported on the following platform in the evaluated configuration: RHEL 7.1 Workstation

23 The following ESM components are outside the evaluated configuration since they are not considered part of the core product and/or require a separate license to activate. Licensing, installing, or enabling these components, which have not been subject to evaluation and are not part of the evaluated configuration of the TOE, will render the TOE out of its evaluated configuration.

- ArcSight Risk Insight
- Pattern Discovery
- ArcSight Express appliance
- ESM Express appliance.

1.5 Clarification of Scope

24 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, trained personnel and secure communication in accordance with user guidance that is supplied with the product.

25 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

26 The following features and capabilities of the TOE described in the guidance documentation are not included within the scope of the evaluation:

- Peer relationships between ArcSight Managers
- High Availability (HA) deployments
- The ability of the TOE to send Security Events as SNMP traps
- Support for external LDAP or RADIUS servers for user authentication.

27 Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirement for using functions and services outside of the evaluated configuration.

1.6 Assumptions

28 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the TOE as defined in the Security Target (Ref [6]).

1.6.1 Usage assumptions

29 Assumptions for the TOE usage as listed in the Security Target:

a) There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

1.6.2 Environment assumptions

30 In order to provide a baseline for the IT product during the evaluation effort, certain assumptions about the environment the product is to be used in have to be made. This section documents any environmental assumptions made about the IT product during the evaluation. Assumptions for the TOE environment listed in Security Target are:

a) The underlying operating system of each TOE component will protect the component and its configuration from unauthorized access.

b) The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

1.7 Evaluated Configuration

31 The evaluated configuration of the TOE consisted of the following configuration and environment set-up to sufficiently test the security functions claimed in the ST (Ref [6]).

32 As stated in the ST, there are five (5) main components of the TOE, namely the ArcSight Manager, CORR-Engine, ArcSight Console, ArcSight Command Center and Service Layer APIs.

33 The ArcSight Manager, CORR-Engine, and ArcSight Command Center web server are installed on the same server. The ArcSight Manager processes and stores event data in the CORR-Engine. Users monitor events using ArcSight Console (a workstation-based application) or the ArcSight Command Center (a web-based interface), which can run reports, develop resources, and perform investigation and system administration. In addition, ESM

Service Layer APIs expose ESM functionality as web services, enabling users to integrate ESM functionality into their own applications.

34 The TOE can be configured in either of two modes: non-FIPS mode (the default mode); and FIPS 140-2 compliant mode. The configured mode determines the cryptographic protocols and the underlying cryptographic provider the TOE uses to implement secure communications. While it is recommended that the TOE operate in FIPS 140-2 mode, this is not required for the evaluated configuration.

35 During testing, the TOE was set up in non-FIPS mode. Two client PCs were used to access the ArcSight Console and access the web-based interface (ArcSight Command Center) over HTTPS, as mandated in the ST.

36 The evaluators conducted the functional testing and vulnerability assessment with the above-mentioned test environment and configuration. The details are described in Section 3.3 of the Evaluation Technical Report (Ref [7]).

1.8 Delivery Procedures

37 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

38 The evaluators determined that the delivery procedures are used when distributing versions of the TOE or parts of it to the consumer.

39 The delivery procedures should consider, if applicable, issues such as:

- ensuring that the TOE received by the consumer corresponds precisely to the evaluated version of the TOE;
- avoiding or detecting any tampering with the actual version of the TOE;
- preventing submission of a false version of the TOE;
- avoiding unwanted knowledge of distribution of the TOE to the consumer: there might be cases where potential attackers should not know when and how it is delivered;
- avoiding or detecting the TOE being intercepted during delivery; and
- avoiding the TOE being delayed or stopped during distribution.

40 In overall, delivery process consists of the following phases:

- **Receipt of Order:** Under the Original Shipment Business (OSB) and Upgrade Shipment Business (USB) for software delivery model employed by HPE, customers purchase software products for electronic delivery through either a sales representative or reseller. Upon receipt of the order, the HPE Licensing Team sends the customer, by email, an Electronic Delivery Receipt (EDR), confirming the order. The email includes a web link allowing the customer to view the EDR on the HPE web site.
- **Electronic Download:** Downloads are available to purchasers of the TOE from the HPE Software Support web site. First-time purchasers must create an HP Passport account on the HPE Software Support web site.

41 All delivery process details are described in Section 4 of the Life Cycle documentation.

1.9 Documentation

42 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage of the product.

43 The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product:

a) HPE Security ArcSight ESM—ESM Installation Guide, Software Version 6.9.1c, March 21, 2016

b) HP ArcSight ESM—Administrator's Guide, Software Version 6.9.1c, January 26, 2016

c) HP ArcSight ESM—ESM 101, Software Version 6.9.1c, January 24, 2016

d) HP ArcSight ESM—ArcSight Console User's Guide, Software Version 6.9.1c, February 3, 2016

e) HP ArcSight ESM Command Center—User's Guide, Software Version 6.9.1c, February 2, 2016

f) Common Criteria Evaluated Configuration Guide – ArcSight ESM 6.9.1c, Version 4.0, October 21, 2016

g) HP ArcSight ESM: Service Layer Developer's Guide, Software Version 1.0, February 16, 2016

h) ESM Service Layer API Reference Vol. 1: Core-Client Services, API Version: 1.0, August 1, 2015

i) ESM Service Layer API Reference Vol. 2: Manager-Client Services, API Version 1.0, August 1, 2015.

2 Evaluation

44 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]).The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref[5]).

2.1 Evaluation Analysis Activities

45 The evaluation activities involved a structured evaluation of the TOE, including the following components:

- The evaluators testing consisted of independent testing efforts, which comprise both functional and penetration test cases to address testing requirements for the ATE_IND.2 and AVA_VAN.2 evaluation components.
- The testing approach for both testing was commensurate with the respective assurance components (ATE_IND.2 and AVA_VAN.2). For functional testing the focus was on testing the claimed security functionality (SFRs within the ST) through the interfaces specified in the functional specification (TSFI). For the penetration testing, the effort was limited to those attacks that are commensurate to an attacker with equal or less than Basic attack potential.

2.1.1 Life-cycle support

2.1.1.1 Configuration Management Capability

46 The evaluators confirmed that the TOE provided for evaluation is labelled with its reference.

47 The evaluators confirmed that the TOE references used are consistent.

48 The evaluators examined the method of identifying configuration items and determined that it describes how configuration items are uniquely identified.

49 The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the CM documentation.

2.1.1.2 Configuration Management Scope

50 The evaluators confirmed that the configuration list includes the following set of items:

- the TOE itself;
- the parts that comprise the TOE;
- the TOE implementation representation; and
- the evaluation evidence required by the SARs in the ST.

51 The evaluators confirmed that the configuration list uniquely identifies each configuration item.

52 The evaluators confirmed that the configuration list indicates the developer of each TSF relevant configuration item.

2.1.1.3 TOE Delivery

53 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

54 The evaluators determined that the delivery procedures are used. All the details are provided in Section 4 of the Life Cycle documentation.

2.1.2 Development

2.1.2.1 Architecture

55 The evaluators examined the security architecture description and determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

56 The security architecture description describes the security domains maintained by the TSF.

57 The initialisation process described in the security architecture description preserves security.

58 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

2.1.2.2 Functional Specification

59 The evaluators examined the functional specification and determined that:

- the TSF is fully represented,
- it states the purpose of each TSF Interface (TSFI),
- the method of use for each TSFI is given,
- the completeness of the TSFI representation,
- it is a complete and accurate instantiation of the SFRs.

60 The evaluators also examined the presentation of the TSFI and determined that:

- it completely identifies all parameters associated with every TSFI,
- it completely and accurately describes all SFR-enforcing actions associated with every SFR-enforcing TSFI,

61 The evaluators also confirmed that the developer supplied tracing links the SFRs to the corresponding TSFIs.

2.1.2.3 TOE Design Specification

62 The evaluators examined the TOE design and determined that the structure of the entire TOE is described in terms of subsystems. The evaluators also determined that all subsystems of the TSF are identified. The evaluators determined that interactions between the subsystems of the TSF were described.

63 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

64 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

65 The evaluators determined that all Security Target SFRs were covered by the TOE design, and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.3 Guidance documents

2.1.3.1 Operating Guidance

66 The evaluators examined the operational user guidance (Ref. [b)], [d)]) and determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

67 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

68 The evaluators examined the operational user guidance (in conjunction with other evaluation evidence (Ref. [a)], [c)], [d)], [e)], [f)]) and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

69 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

70 The evaluators found that the operational user guidance is clear and reasonable.

2.1.3.2 Preparation Guidance

71 The evaluators examined the provided delivery acceptance documentation and determined that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

72 The evaluators determined that the provided installation procedures describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.

73 The evaluators performed all user procedures necessary to prepare the TOE during testing and determined that the TOE and its operational environment can be prepared securely using only the supplied preparative user guidance.

2.1.4 IT Product Testing

74 Testing at EAL2 consists of assessing developer tests, performing independent functional tests, and conducting penetration tests. The TOE testing was conducted by the evaluators of BAE Systems Applied Intelligence MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.4.1 Assessment of Developer Tests

75 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

76 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

77 At EAL2, independent functional testing is the evaluation conducted by the evaluator based on information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of developer's test plan and creating test cases that developer tests.

78 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were developed and performed by the evaluators and are consistent with the expected test documentation.

Test ID	Description	Security Function	Justification
TEST-IND-001	Verify the TOE generates an audit record upon start-up and shutdown of the audit function. Verify that audit records consist of date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. Verify the sorting capabilities on audit data based on date and time, subject identity, type of event, success or failure of related event. Verify that the TSF restricts the ability to create, delete, and modify user accounts to the Administrator. Verify that the TSF maintains the roles of Administrators, Analyzer Administrator, Operator and Analyst. Verify that all users are successfully authenticated before allowing any	FIA_UAU.1.1, FIA_UAU.1.2, FIA_UID.1.1, FIA_UID.1.2, FIA_ATD.1.1, FMT_SMR.1.1, FMT_SMR.1.2, FMT_MOF.1.1, FMT_MTD.1.1(1), FMT_MTD.1.1(2), FMT_SMF.1.1, FTA_SSL.4.1, FAU_GEN.1.1, FAU_GEN.1.2	This test aims to verify that the TOE performs following security functions: • Identification & Authentication • Security Management • TOE Access • Security Audit

Test ID	Description	Security Function	Justification
	other TSF-mediated actions.		
TEST-IND-002	Verify that the TSF allows user-initiated termination of the user's own interactive session. Verify that the TOE provides the Administrator and Analyzer Administrator with the capability to read all audit information from the audit records. Verify that the TOE protects the stored audit records in the audit trail from unauthorised modification and deletion.	FTA_SSL.4.1, FAU_GEN.1.1, FAU_GEN.1.2, FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.2.1, FAU_SAR.3.1, FAU_STG.1.1, FAU_STG.1.2	This test aims to verify that the TOE performs following security functions: • TOE Access • Security Audit
TEST-IND-003	Verify that the TOE protects TSF data from modification and disclosure when data is transmitted between separate parts of the TOE. Verify that the TSF provides other trusted IT products to initiate communication via a trusted path. Detect when an administrator configurable positive integer in between 1-10 of unsuccessful authentication attempts occurred related to user login. Verify that the TSF provides a mechanism to verify that configurable secrets are met by all user accounts. Verify the authentication of passwords and/or digital certificates.	FIA_AFL.1.1, FIA_AFL.1.2, FIA_SOS.1.1, FIA_UAU.5.1, FIA_UAU.5.2, FPT_ITT.1.1, FTP_ITC.1.1, FTP_ITC.1.2, FTP_ITC.1.3, FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3	This test aims to verify that the TOE performs following security functions: • Identification & Authentication • Protection of the TSF • Trusted Path/Channels
TEST-IND-004	Verify that the TSF records within each analytical result, the date and time of the result, type of result and identification of data source. Verify that the TSF sends an alarm to the ESM Manager and to any monitoring ArcSight Console session, and take action specified by the rule that was triggered by the event when an intrusion is detected. Verify that the TSF provides the Administrator, Analyzer Administrator, Operator, Analyst with the capability to read all event information from the IDS data. Verify that the TSF protects stored IDS data from unauthorized modification and deletion.	IDS_ANL.1.1, IDS_ANL.1.2, IDS_RCT.1.1, IDS_RDR.1.1, IDS_RDR.1.2, IDS_RDR.1.3, IDS_STG.1.1, IDS_STG.1.2, IDS_STG.1.3, IDS_STG.2.1(1), IDS_STG.2.1(2)	This test aims to verify that the TOE performs following security functions: • Intrusion Detection System

Test ID	Description	Security Function	Justification
	Verify that the TSF sends a warning to a configured e-mail address when the IDS storage exceeds the configured threshold (default 95%).		

79 All testing performed by the evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration Testing

80 The evaluators performed vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, and TOE design and security architecture description.

81 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialist expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation.

82 The penetration tests focused on:

a) Port Scan

b) General Vulnerability Scan

c) Common web Vulnerability Scan

d) Cookie Injection/ Broken Authentication

e) Security Misconfiguration

f) Invalidated Redirects and Forwards

83 The results of the penetration testing notes that there is no residual vulnerability found. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref [6]).

2.1.4.4 Testing Results

84 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target (Ref [6]) and its functional specification. In addition, the documentation supplied as evidence for the EAL2 Common Criteria evaluation of the TOE was analyzed to identify possible vulnerabilities.

3 Result of the Evaluation

85 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of HPE ArcSight ESM v6.9.1c (ESM) performed by BAE Systems Applied Intelligence MySEF.

86 BAE Systems Applied Intelligence MySEF found that HPE ArcSight ESM v6.9.1c (ESM) upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance Level 2 (EAL2).

87 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

88 EAL 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and interface specifications, guidance documentation and a basic description of the TOE architecture, to understand the security behaviours of the TOE.

89 The analysis is supported by an independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to an attacker possessing a Basic attack potential.

90 EAL 2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

91 The following recommendations are made:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

Annex A References

A.1 References

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

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

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

[4] MyCC Scheme Policy (MyCC_P1), v1d, CyberSecurity Malaysia, February 2016.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1c, February 2016.

[6] Hewlett Packard Enterprise ArcSight ESM Security Target, Version 1.0, 21 October 2016

[7] EAU000426-S035-ETR 1.2, Evaluation Technical Report, Version 1.2, 6 December 2016

A.2 Terminology

A.2.1 Acronyms

Table 2: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target

Acronym	Expanded Term
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 3: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.

Term	Definition and Source
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---