C080 Certification Report

Micro Focus ArcSight Data Platform V2.11

File name: ISCB-5-RPT-C080-CR-v1
Version: v1
Date of document: 15 November 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
Malaysia.
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999
www.cybersecurity.my

C080 Certification Report

Micro Focus ArcSight Data Platform V2.11

15 November 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:	C080 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C080-CR-v1
ISSUE:	v1
DATE:	15 November 2017

DISTRIBUTION: UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright and Confidentiality Statement

Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – 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 15 November 2017 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).

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	19 October 2017	All	Initial draft of certification report
v1	1 November 2017	All	Final version of certification report

Executive Summary

The Target of Evaluation (TOE) is ArcSight Data Platform (ADP) 2.11 from Micro Focus. ADP is a next-generation data collection and storage engine functionality that unifies log data collection, storage, and security data management in a scalable, high-performance software or appliance solution. It provides capabilities to collect machine data from any source (such as logs, clickstreams, sensors, stream network traffic, security devices, web servers, custom applications, social media, and cloud services) and to monitor and search that data for security intelligence.

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 functional 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 03 October 2017.

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 http://www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that Micro Focus ArcSight Data Platform (ADP) V2.11 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

The TOE, ArcSight Data Platform (ADP), has been rebranded from Hewlett Packard Enterprise (HPE) to Micro Focus. All HPE guidance documentation is effectively in the process of being renamed to Micro Focus and the contents of the documents themselves remain unchanged and are applicable to the TOE.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The TOE is ArcSight Data Platform (ADP) V2.11 from Micro Focus. ADP is a next-generation data collection and storage engine that unifies log data collection, storage, and security data management in a scalable, high-performance software or appliance solution.

2 The functionality defined in the Security Target (Ref [6]) that was subsequently evaluated is as follows:

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

1.2 TOE Identification

3 The details of the TOE are identified in

4 Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C080
TOE Name	Micro Focus ArcSight Data Platform (ADP)
TOE Version	2.11
Security Target Title	Micro Focus ArcSight Data Platform (ADP) Security Target
Security Target Version	Version 1.0
Security Target Date	29 September 2017
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, Maryland 21046
Developer	Micro Focus 1160 Enterprise Way, Sunnyvale CA, 94089
Evaluation Facility	BAE Systems Applied Intelligence – MySEF (Malaysia Security Evaluation Facility) Level 28, Menara Binjai, 2 Jalan Binjai, 50450 Kuala Lumpur, Malaysia

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 2.3 and Section 2.4 of the Security Target (Ref [6]).

7 The TOE architecture consists of the following components:

- ArcSight Management Center (ArcMC)
- ArcSight Logger
- ArcSight Data Platform (ADP) Event Broker
- ArcSight SmartConnectors, specifically;
    - Syslog NG Daemon
    - Microsoft Windows Event Log – Native (WINC)

8 The ArcSight Management Center (ArcMC) is a centralised management tool that supports security policy configuration, deployment maintenance, and monitoring. It provides a single management interface to administer ArcSight managed nodes, including Loggers, SmartConnectors, Event Brokers, and other ArcMCs.

9 ArcSight Logger is a log management solution designed to handle high event throughput, support data analysis, and provide efficient long-term storage. Logger receives and stores events, supports search, retrieval, and reporting, and can optionally forward selected events (e.g., to ArcSight ESM).

10 The ADP Event Broker centralises event processing, enabling integration of ArcSight events to third party solutions. It enables scalable, high-throughput, multi-broker clusters for publishing and subscribing to event data.

11 ArcSight SmartConnectors collect and process events generated by devices throughout an enterprise. SmartConnectors are specifically developed to work with network and security products using multiple techniques, including simple log forwarding and parsing, direct installation on native devices, SNMP, and syslog.

12 The following figure illustrates how the TOE components can be deployed in an enterprise network. Communications between the TOE components are protected using TLS. Although SmartConnectors collecting from IDS and firewall devices are depicted, only the Syslog NG Daemon and the Microsoft Windows Event Log – Native (WINC) SmartConnectors are formally included in the scope of the evaluation.

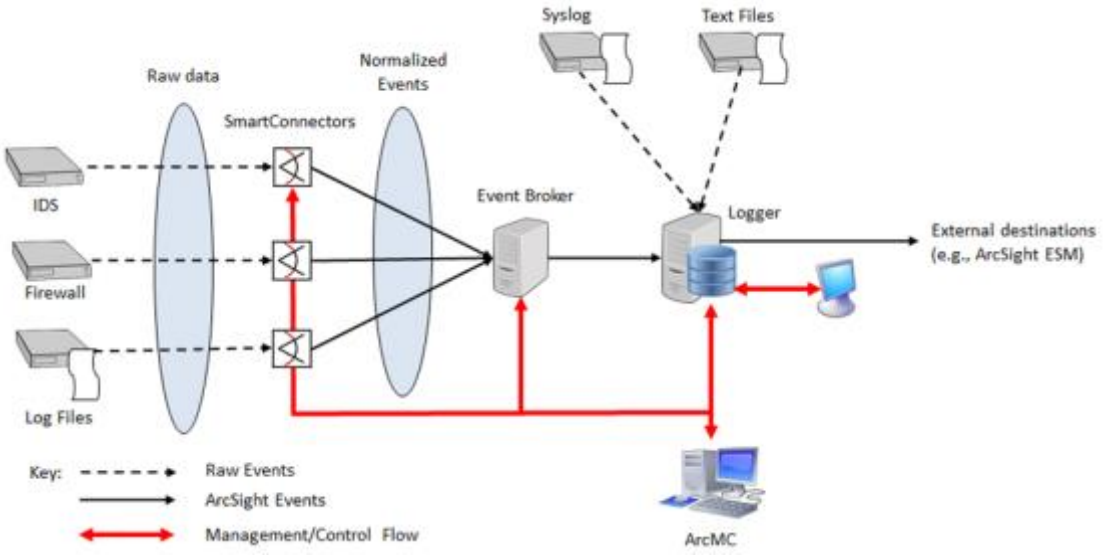

Figure 1: Physical Scope of the TOE

1.4.1 Logical Boundaries

13 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:

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

14 **Audit:** Both the ArcMC and Logger components of the TOE are able to generate and store audit records of security-relevant events. The stored audit records are protected from unauthorised modification and deletion. Audit records generated by ArcMC can be viewed only by users in the ArcMC Default System Admin or ArcMC Read Only System Admin roles, while audit records generated by Logger can be viewed only by users in the Logger System Admin or Logger Read Only System Admin roles.

The ArcMC and Logger components of the TOE provides capabilities for selecting audit records based on date and time range and, optionally, subject identity and outcome, and ordering the selected records based on date and time, the subject associated with the audit event, and the type of audit event.

15 **Identification & Authentication:** The TOE maintains accounts of the authorised users of the system. The user account includes the following attributes associated with the user: user identity; authentication data; authorisations (groups or roles); and e-mail address information. The TOE supports both passwords and certificates for authentication and users can be configured for password-only, certificate-only, or password and certificate-based authentication. The TOE additionally supports external LDAP and RADIUS authentication servers. 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 15 minutes. The TOE requires users to provide unique identification and authentication data before any administrative access to the TOE via the ArcMC GUI or Logger GUI is granted.

16 **Security Management:** The ArcMC component provides authorised ArcMC users with a GUI that can be used to configure and manage ArcMC security functions and TSF data, depending on the security management roles assigned to the user. ArcMC supports the following security management roles: Default System Admin Group; Read Only System Admin Group; Default ArcMC Rights Group; and Read Only ArcMC Group.

The Logger component provides authorised Logger users with a GUI that can be used to configure and manage Logger security functions and TSF data, depending on the security management roles assigned to the user. Logger supports the following security management roles: Logger System Admin; Logger Read Only System Admin; Logger Rights; Logger Search; and Logger Reports.

17 **Protection of the TSF:** Communications between distributed components of the TOE (i.e., ArcMC, Loggers, Event Broker, and SmartConnectors) occur over TLS, which provides confidentiality and integrity of transmitted data.

Appliance-based Logger components maintain time internally and use this internal time as the source for reliable timestamps. In addition, they can be configured to synchronise their clocks with external NTP servers. Software-based TOE components use the system clock maintained by the underlying operating system as the source for date and time information.

18 **TOE Access**: The TOE enforces a limit on the number of simultaneous active sessions for each user account. The maximum number is configurable by an administrator and has a default value of 15.

The TOE will terminate interactive sessions after a period of inactivity configurable by an administrator. The TOE also allows user-initiated termination of the user's own interactive session by explicitly logging off.

The TOE displays a banner message on the user login page. The content of the message can be configured by an administrator.

19 **Trusted Path/Channels:** The TOE provides a trusted channel to communicate securely with external ArcSight ESM destinations. The trusted channel is implemented using HTTPS (i.e., HTTP over TLS).

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 ArcMC GUI and Logger GUI. Administrators initiate the trusted path by establishing a 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.

20 **Intrusion Detection System:** The TOE collects IDS data generated by devices in the IT system it is monitoring. The Logger component receives and stores events from SmartConnectors (directly or via the Event Broker), syslog, and text files. SmartConnectors collect raw events generated by devices in the operational environment, normalise them, process them into ArcSight security events, and transmit them to the Logger component (directly or via the Event Broker). The Logger component provides the repository for storing collected IDS data and capabilities for managing IDS data storage.

The TOE provides capabilities to search stored IDS data (events) using queries. Queries can be simple search terms or they can be complex enough to match events that include multiple IP addresses or ports, that occurred between specific time ranges from a specific storage group.

The TOE provides capabilities to define queries that can trigger alerts if specified conditions are met.

1.5 Clarification of Scope

21 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.

22 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]).

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

- Connector Hosting Appliances (also referred to as ArcMC appliances)
- Micro Focus ArcSight FlexConnectors
- Micro Focus ArcSight Load Balancer

24 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

25 This section summarises the assumptions regarding the operational environment and the intended usage of the TOE, as described in the Security Target (Ref [6]):

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

b) The underlying operating system of each TOE software component will protect the component and its configuration from unauthorised access.

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

1.7 Evaluated Configuration

26 As stated in the ST (Ref [6]), there are four (4) main components of the TOE that make up the evaluated configuration, namely the ArcSight Management Center (ArcMC), ArcSight Logger, ArcSight Data Platform (ADP) Event Broker, and ArcSight SmartConnectors.

27 The TOE components are deployed as software solutions in a multi-server environment in an enterprise network. The ArcMC component of the TOE provides a management interface that allows users to perform management and security functions on the TOE. In addition, the Logger component can also be deployed in a hardware appliance form factor. Multiple Loggers and multiple Event Brokers can be used to scale up to support extremely high event volume with search queries distributed across all Loggers.

28 The evaluated configuration requires that all communications between distributed components of the TOE occur over TLS, which provides confidentiality and integrity of transmitted data. The TOE can be configured in either of two modes: non-FIPS 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. To be fully FIPS 140-2 compliant, all components that work together need to be in FIPS mode.

29 The TOE supports the following components in the operational environment, however they are not required in the evaluated configuration:

- LDAP or RADIUS server to support user authentication.
- NTP server to provide time synchronisation to TOE appliances or hosting platforms.
- ArcSight Load Balancer, which provides a “connector-smart” load balancing mechanism by monitoring the status and managing the load of SmartConnectors.
- ArcSight ESM instances that can subscribe to the Event Broker component and can receive events and alert notifications from the Logger component of ADP.
- Other non-TOE subscribers of Event Broker, including ArcSight Investigate, Apache Hadoop, and/or a third party consumer.

1.8 Delivery Procedures

30 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.

31 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.

32 The TOE delivery procedures include two forms:

- Receipt of Order: Under the Original Shipment Business (OSB) and Upgrade Shipment Business (USB) delivery model employed by Micro Focus, customers purchase software products for electronic delivery through either a sales representative or reseller. Upon receipt of the order, the Micro Focus 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 Micro Focus website. By following the instructions in the EDR, the customer is directed to an Electronic Delivery website by a way of a URL that contains a temporary download key and further instructions to be followed.
- Electronic Download: Downloads are available to purchasers of the TOE from the Micro Focus Software Support website. First-time purchasers must create a Micro Focus Passport account on the Micro Focus Software Support website, which is available to Micro Focus customers with a service agreement ID (SAID).
- Hardware Shipment: When an order arrives for an appliance, the stored appliance is moved from the secure warehouse storage to production again, and unboxed. The chassis is labelled, and a Glis license is printed and attached to the appliance. A pair of power cords is included in the packaging. Finally, the appliance is boxed again and a box label is applied to the appliance box, which contains all the necessary details of the SKU ordered by the customer. As a final step, the box is sealed with Micro Focus tamper-proof tape and is now ready to send for shipment. The appliance is delivered by Micro Focus End to End Logistics, which has many secure shippers worldwide.

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

1.9 Documentation

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

The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product. Note: All Hewlett Packard Enterprise (HPE) guidance documentation is effectively in process of being renamed to Micro Focus. The contents of the documents are unaffected by the naming change.

- HPE Security ArcSight Logger Installation and Configuration Guide, Software Version 6.4, April 14, 2017
- HPE Security ArcSight Logger Administrator's Guide, Software Version 6.4, April 14, 2017
- HPE Security ArcSight Logger Web Services API Guide, Software Version 6.4, April 14, 2017
- HPE Security ArcSight Logger Release Notes, Software Version 6.4, April 14, 2017
- HPE Security ArcSight ArcSight Data Platform Support Matrix, April 21, 2017

- HPE ArcSight Management Center Administrator's Guide, Software Version: 2.6, April 14, 2017
- HPE ArcSight Management Center Release Notes, Software Version 2.6, April15, 2017
- HPE Security ArcSight Data Platform Event Broker Deployment Guide, Software Version 2.01, September 29, 2017
- HPE Security ArcSight Data Platform Event Broker Administrator's Guide, Software Version: 2.01, June 13, 2017
- HPE Security ArcSight Data Platform Event Broker Release Notes, Software Version 2.01, June 13, 2017
- HPE Security ArcSight Connectors SmartConnector User Guide, May 15, 2017
- HPE Security ArcSight SmartConnectors SmartConnector for Microsoft Windows Event Log—Native Configuration Guide, May 15, 2017
- HPE Security ArcSight Connectors SmartConnector for Syslog NG Daemon Configuration Guide, May 15, 2017
- HPE Security ArcSight Connectors SmartConnector Release Notes 7.6.0.8009.0, May 15, 2017
- Common Criteria Evaluated Configuration Guide – ArcSight Data Platform (ADP) 2.11, Version 1.3, September 29, 2017.

2 Evaluation

35 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 [4]).

2.1 Evaluation Analysis Activities

36 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

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

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

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

40 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

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

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

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

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

2.1.1.3 TOE Delivery

44 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.

2.1.2 Development

2.1.2.1 Architecture

45 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.

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

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

48 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

49 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,

50 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 error messages resulting from an invocation of each SFR-enforcing TSFI,

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

2.1.2.3 TOE Design Specification

52 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.

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

54 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.

55 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 Operational Guidance

56 The evaluators examined the operational user guidance 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.

57 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.

58 The evaluators examined the operational user guidance (in conjunction with other evaluation evidence 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.

59 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.

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

2.1.3.2 Preparation Guidance

61 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.

62 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.

63 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

64 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

65 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).

2.1.4.2 Independent Functional Testing

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

67 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 recorded by the evaluators and are consistent with the expected test results in the test documentation.

Test ID	Description	SFRs
TEST-IND-001-ARC TEST-IND-001-LOG	• Verify that all users are successfully identified and authenticated based on authentication mechanisms, verification of secrets and user attributes before allowing any other TSF-mediated actions. • Verify that all users are required to re-authenticate when their password has been changed. • Verify that authorised users are able to perform management of TSF data functions. • Verify that authorised users are able to determine and modify the behaviour of security management functions. • Verify that the TSF shall maintain security roles. • Verify that the TSF data is protected from disclosure or modification when it is transmitted between separate parts of the TOE, and all communication between the TOE and other trusted IT products/remote users are initiated via trusted path/channels. • Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_SAR.1.1(1), FAU_SAR.1.2(1), FAU_SAR.1.1(2), FAU_SAR.1.2(2), FIA_ATD.1.1, FIA_SOS.1.1, FIA_UAU.2.1, FIA_UAU.5.1, FIA_UAU.5.2, FIA_UAU.6.1, FIA_UID.2.1, FMT_MOF.1.1(1), FMT_MTD.1.1(1), FMT_MTD.1.1(5), FMT_MTD.1.1(6), FMT_SMF.1.1, FMT_SMR.1.1, FMT_SMR.1.2, FPT_ITT.1.1, FTA_SSL.4.1, FTP_ITC.1.1, FTP_ITC.1.2, FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3
TEST-IND-002-ARC TEST-IND-002-LOG	• Verify that the TSF performs TOE access functions such as limitation of concurrent sessions, user session termination, inactive session termination and displays a TOE access banner. • Verify that the TSF is able to detect unsuccessful authentications and disable a user account for a period of time. • Verify that authorised users are able to determine and modify the behaviour of security management functions.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_SAR.1.1(1), FAU_SAR.1.2(1), FAU_SAR.1.1(2), FAU_SAR.1.2(2), FIA_AFL.1.1, FIA_AFL.1.2, FIA_UAU.2.1, FIA_UID.2.1, FTA_MCS.1.1,

Test ID	Description	SFRs
	• Verify that the TOE generates audit records for auditable events and provides a means for authorised users to view the audit logs.	FTA_MCS.1.2, FTA_SSL.3.1, FTA_SSL.4.1, FTA_TAB.1.1, FMT_MOF.1.1(1)
TEST-IND-003-ARC TEST-IND-003-LOG	• Verify that the TSF restricts access to audit records, provides the capability to select and order audit records and protects audit records from unauthorised deletion and modification. • Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs. • Verify that the TSF is able to provide reliable time stamps.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_SAR.1.1(1), FAU_SAR.1.2(1), FAU_SAR.1.1(2), FAU_SAR.1.2(2), FAU_SAR.2.1, FAU_SAR.3.1, FAU_STG.1.1, FAU_STG.1.2, FPT_STM.1.1
TEST-IND-004-LOG	• Verify that the TSF provides the ability to collect IDS data and configure alerts, alert notifications, event archives, storage groups and retention policies for the IDS data. • Verify that the TSF restricts access to IDS data, provides the capability to view, select and order IDS data and protects the IDS data from unauthorised deletion and modification. • Verify that the TSF data is protected from disclosure or modification when it is transmitted between separate parts of the TOE, and all communication between the TOE and other trusted IT products/remote users are initiated via trusted path/channels.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_SAR.1.1(2), FAU_SAR.1.2(2), FMT_MOF.1.1(2), FMT_MTD.1.1(2), FMT_MTD.1.1(3), FMT_MTD.1.1(4), FMT_SMF.1.1, FMT_SMR.1.1, IDS_ARP.1.1, 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, IDS_ARP.1.2, IDS_IDC.1.1, IDS_IDR.1.1, IDS_IDR.1.2, IDS_IDR.1.3, IDS_IDR.2.1, IDS_STG.1.1, IDS_STG.1.2, IDS_STG.2.1

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

2.1.4.3 Penetration Testing

69 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.

70 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 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.

71 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) Secure Communication Path

72 The results of the penetration testing demonstrates that the TOE is resistant to an attacker possessing a basic attack potential. 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

73 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 analysed to identify possible vulnerabilities.

3 Result of the Evaluation

74 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 Micro Focus ArcSight Data Platform (ADP) version 2.11 performed by BAE Systems Applied Intelligence MySEF.

75 BAE Systems Applied Intelligence MySEF found that Micro Focus ArcSight Data Platform (ADP) v2.11 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).

76 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

77 EAL 2 provides assurance by a full Security Target and analysis of the SFRs in that Security Target (Ref [6]), using functional and interface specifications, guidance documentation and a basic description of the design and architecture of the TOE, to understand the security behaviours of the TOE.

78 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.

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

3.2 Recommendation

80 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] Micro Focus ArcSight Data Platform Security Target, Version 1.0, 29 September 2017

[7] EAU000427-S040-ETR, Evaluation Technical Report, Version 1.0, 17 October 2017

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
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.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.

Term	Definition and Source
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 ---