C077 Certification Report

RSA Security Analytics v10.6.1

File name: ISCB-5-RPT-C077-CR-v1
Version: v1
Date of document: 22 February 2017
Document classification: PUBLIC

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

C077 Certification Report

RSA Security Analytics v10.6.1

22 February 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:	C077 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C077-CR-v1
ISSUE:	v1
DATE:	22 February 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

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 22 February 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).

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	6 February 2017	All	Initial draft of certification report
v1	22 February 2017	All	Final version of certification report

Executive Summary

RSA Security Analytics v10.6.1 (SA) is the Target of Evaluation (TOE) for the Evaluation Assurance Level 2 Augmented with ALC_FLR.1 Evaluation.

SA is a collection of appliances that form a security infrastructure for an enterprise network. This architecture provides converged network security monitoring and centralized security information and event management (SIEM). SA provides real-time visibility into the monitored network and long-term network data storage to provide detection, investigation, analysis, forensics, and compliance reporting. SA's Capture infrastructure collects log and packet data from the network. Packet collection extracts metadata, reassembles, and globally normalizes all network traffic at layers 2 through 7 of the Open Systems Interconnection (OSI) model. This data allows SA to perform real-time session analysis; incident detection, drill-down investigation, reporting, and forensic analysis functions.

The scope of evaluation covers major security features as follows:

a) Security Audit: The TOE is able to generate audit records of security relevant events that include at least date and time of the event, subject identity and outcome for security events.

b) Cryptographic Support: The Transport Layer Security (TLS 1.2) protocol in FIPS mode is used to provide protection of the communications surrounding the remote administrative sessions from disclosure and from modification.

c) Identification & Authentication: The TOE allows the users to acknowledge end-user license agreements and view warning banners prior to providing identification and authentication data.

d) Security Monitoring with Security Information and Event Management (SIEM): The TOE receives network packets, reconstructs network transactions, extracts metadata, and applies rules. The TOE is able to identify potential misuse or intrusions and send an alarm to incident management SA views.

e) Security Management: The TOE allows only authorized administrators to manage the security functions and TSF data of the TOE via a web-based User Interface.

f) Protection of the TSF: The TOE provides protection mechanisms for its security functions.

g) TOE Access: The TOE terminates interactive sessions after administrative configured period of time.

h) Trusted path/channels: The TOE requires remote users to initiate a trusted communication path using TLS for initial user authentication.

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) Augmented with ALC_FLR.1. 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 27 January 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 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 RSA Security Analytics v10.6.1 meets their requirements. It is recommended that a potential user of RSA Security Analytics v10.6.1 refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

1 Target of Evaluation

1.1 TOE Description

1 The TOE is RSA Security Analytics v10.6.1 (SA). SA is a collection of appliances that form a security infrastructure for an enterprise network. This architecture provides converged network security monitoring and centralized security information and event management (SIEM). SA provides real-time visibility into the monitored network and long-term network data storage to provide detection, investigation, analysis, forensics, and compliance reporting. SA's Capture infrastructure collects log and packet data from the network. Packet collection extracts metadata, reassembles, and globally normalizes all network traffic at layers 2 through 7 of the Open Systems Interconnection (OSI) model. This data allows SA to perform real-time session analysis. SA recognizes over 250 event source types, which are aggregated, analyzed, and stored for long-term use.

2 The TOE implements additional security functions such as Security Monitoring with Security Information and Event Management (SIEM); identification and authentication of TOE users; security management; and trusted path.

3 The details of TOE functions can be found starting in section 2.1 of the Security Target version 1.0

4 There are eight security functionalities covered under the scope of the evaluation which are:

Security Function	Description
Security Audit	The TOE is able to generate audit records of security relevant events that include at least date and time of the event, subject identity and outcome for security events.
Cryptographic Support	The Transport Layer Security (TLS 1.2) protocol in FIPS mode is used to provide protection of the communications surrounding the remote administrative sessions from disclosure and from modification. TLS is also used for distributed internal TOE component communications.
Identification & Authentication	The TOE allows the users to acknowledge end-user license agreements and view warning banners prior to providing identification and authentication data.
Security Monitoring with Security Information and Event Management (SIEM)	The TOE receives network packets, reconstructs network transactions, extracts metadata, and applies rules. The TOE receives log data, parses the

	data, extracts metadata, correlates events, and applies rules. Through statistical and signature analysis, the TOE can identify potential misuse or intrusions and send an alarm to incident management SA views.
Security Management	The TOE allows only authorized administrators to manage the security functions and TSF data of the TOE via a web-based User Interface.
Protection of the TSF	The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate and have the appropriate permissions before any administrative operations or access to TOE data and resources can be performed on the TSF
TOE Access	The TOE terminates interactive sessions after administrative configured period of time. The TOE also allows user-initiated termination of the user's own interactive session by closing the browser or explicitly logging off.
Trusted path/channels	The TOE requires remote users to initiate a trusted communication path using TLS for initial user authentication. The TOE also requires that the trusted path be used for the transmission of all SA interface session data.

1.2 TOE Identification

5 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	C077
TOE Name	RSA Security Analytics
TOE Version	v10.6.1
Security Target Title	RSA Security Analytics v10.6.1 Security Target
Security Target Version	1.0

Security Target Date	15 December 2016
Assurance Level	Evaluation Assurance Level 2 (EAL2) Augmented with ALC_FLR.1
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [2])
Methodology	Common Evaluation Methodology 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 EAL2 Augmented with ALC_FLR.1
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive, Columbia, Maryland 21046
Developer	RSA Security LLC (RSA) 10700 Parkridge Blvd. Suite 600, Reston, VA 20191
Evaluation Facility	BAE Systems Applied Intelligence MySEF

1.3 Security Policy

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

1.4 TOE Architecture

7 The TOE includes both logical and physical boundaries, which are described in Section 2.2 of the Security Target (Ref [6]).

8 The following figure 1 shows the evaluated configuration that comprise the TOE:

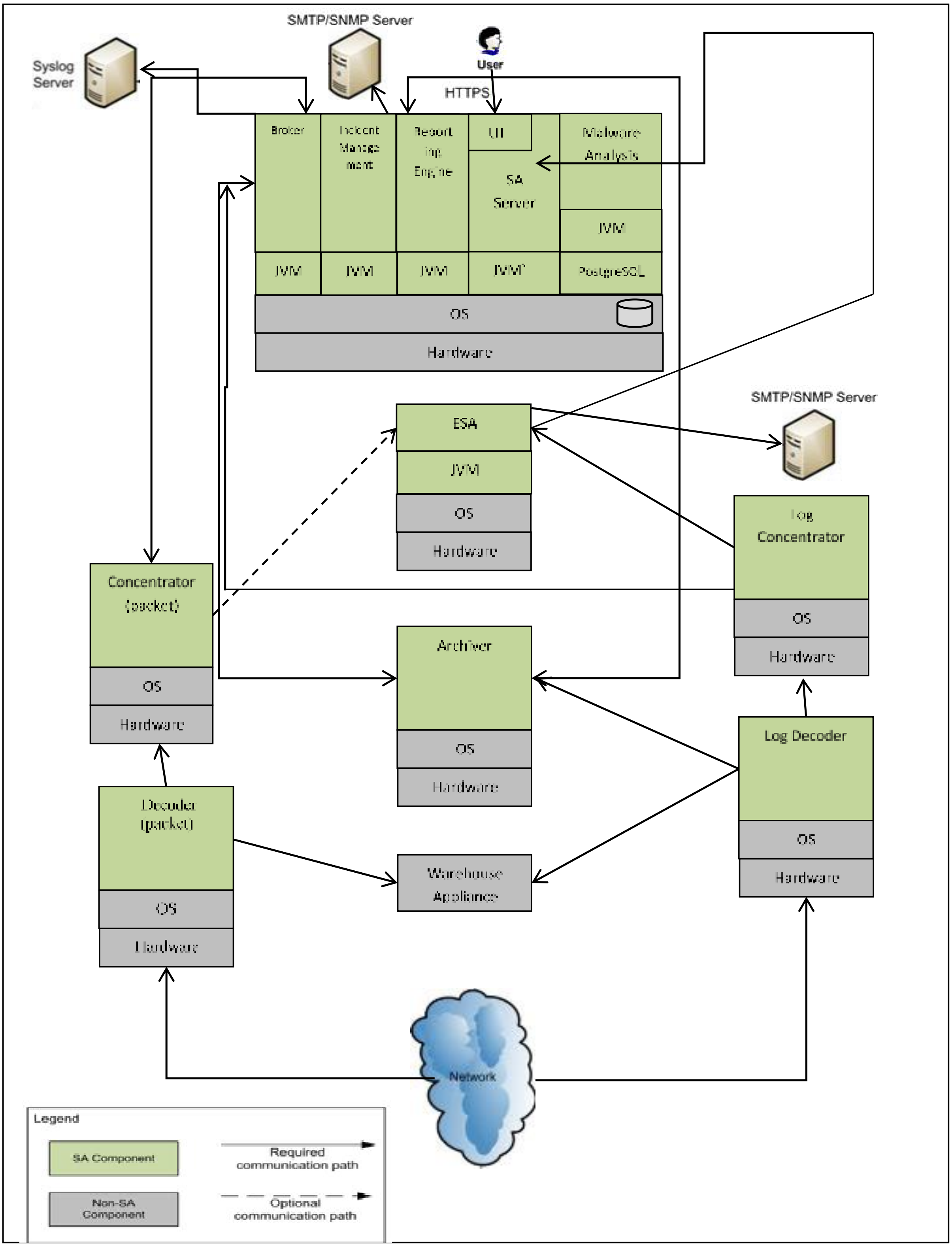
SMTP/SNMP Server
Syslog Server
User
HTTPS
Broker
Incident Management
Reporting Engine
UI
SA Server
Malware Analysis
JVM
JVM
JVM
JVM
JVM
JVM
PostgreSQL
OS
Hardware
SMTP/SNMP Server
ESA
JVM
OS
Hardware
Log Concentrator
OS
Hardware
Concentrator (packet)
OS
Hardware
Archiver
OS
Hardware
Log Decoder
OS
Hardware
Decoder (packet)
OS
Hardware
Warehouse Appliance
Network
Legend
SA Component
Non-SA Component
Required communication path
Optional communication path

Figure 1

1.4.1 Logical Boundaries

9 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:

a) Security Audit: The TOE generates audit records of security relevant events that include at least date and time of the event, subject identity and outcome for security events. The TOE provides the default Administrator and Operator roles with the ability to read the audit events. The environment stores the audit records and also provides the system clock information that is used by the TOE to timestamp each audit record.

b) Cryptographic Support: The Transport Layer Security (TLS 1.2) protocol in FIPS mode is used to provide protection of the communications surrounding the remote administrative sessions from disclosure and from modification. TLS is also used for distributed internal TOE component communications. The TOE uses a FIPS-validated module for SSH protected communication pathways for the transfer of file event source data from log data sources to the TOE.

The TOE uses Crypto-C ME 4.1.2 (FIPS 140-2 validation certificates #2300/2294) for both SSH and TLS communications.

The TOE uses the RSA BSAFE Crypto-J cryptographic library: BSAFE SSL-J 6.1.3.1 for Java applications, which incorporates BSAFE Crypto-J 6.1 (FIPS 140-2 Certificates #2058/2057).

c) Identification and Authentication: The TOE allows the users to acknowledge end-user license agreements and view warning banners prior to providing identification and authentication data. No other access to the TOE is permitted until the user is successfully authenticated. The TOE maintains the following security attributes belonging to individual human users: username, password and role.

The TOE provides authentication failure handling that allows administrators to configure the number of times a user may attempt to login and the time that the user will be locked out if the configured number of attempts has been surpassed. The TOE detects when the defined number of unsuccessful authentication attempts has been surpassed, and enforces the described behavior (locks the user account for a specified time period).

d) Security Monitoring with Security Information and Event Management (SIEM): The TOE receives network packets, reconstructs network transactions, extracts metadata, and applies rules. The rules identify interesting events, effectively matching signatures and performing statistical analysis. Likewise, the TOE receives log data, parses the data, extracts metadata, correlates events, and applies rules. Through statistical and signature analysis, the TOE can identify potential misuse or intrusions and send an alarm to incident management SA views. The incident management SA views provide the analytical results to authorized users in a manner suitable for the user to interpret the information. The analytical results are recorded with information such as date and time. Only users with the Analysis and Administrator roles can read the metadata, raw logs, raw packet data, and incident management data from the IDS data.

e) Security Management: Authorized administrators manage the security functions and TSF data of the TOE via the web-based User Interface. The ST defines and maintains the administrative roles: Administrator, Analyst, Operator, SOC Manager, and Malware Analyst. Authorized administrators perform all security functions of the TOE including starting and stopping the services and audit function, creating and managing user accounts, manage authentication failure handling and session inactivity values and read the audit and analyzer data.

f) Protection of the TSF: The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate and have the appropriate permissions before any administrative operations or access to TOE data and resources can be performed on the TSF. The TOE is a collection of special-purpose appliances. Each appliance provides only functions for the necessary operation of the TOE, and limits user access to authorized users with an administrative role.

Communication with remote administrators is protected by TLS in FIPS mode, protecting against the disclosure and undetected modification of data exchanged between the TOE and the administrator. The TOE runs in a FIPS compliant mode of operation and uses FIPS-validated cryptographic modules.

g) TOE Access: The TOE terminates interactive sessions after administrative configured period of time. The TOE also allows user-initiated termination of the user's own interactive session by closing the browser or explicitly logging off.

Before establishing a user session, the TOE displays an advisory warning message regarding unauthorized use of the TOE.

h) Trusted path/channels: The TOE requires remote users to initiate a trusted communication path using TLS for initial user authentication. The TOE also requires that the trusted path be used for the transmission of all SA interface session data. The use of the trusted path provides assured identification of end points and protection of the communicated data from modification, and disclosure. The TOE uses a FIPS-validated module for SSH protected communication pathways for the transfer of file event source data from log data sources to the TOE. TLS and SSH ensure the administrative session and file transfer communication pathways are secured from disclosure and modification.

1.4.2 Physical Boundaries

10 The TOE includes both logical and physical boundaries, which are described in Section 2.2.2 and 2.2.3 of the Security Target (Ref [6]).

1.5 Clarification of Scope

11 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.

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

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

1.6 Assumptions

14 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 that are required for secure operation of the TOE, which is defined in the Security Target (Ref [6]).

1.6.1 Usage assumptions

15 Assumption for the TOE usage as listed in Security Target:

a) It is assumed that there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

b) The authorized TOE administrators will follow and apply all administrator guidance in a trusted manner.

c) Users will protect their authentication data.

1.6.2 Environment assumptions

16 Assumptions for the TOE environment listed in the Security Target are:

a) TOE Administrators will properly configure the network in the TOE operational environment and configure adequate network capacity for the deployed TOE components.

b) The TOE hardware and software critical to the security policy enforcement will be located within controlled access facilities which will prevent unauthorized physical access.

1.7 Evaluated Configuration

17 The evaluated configuration (see Figure 2-1 Evaluated Configuration) is described in Section 2.2 of the Security Target (Ref [6]).

1.8 Delivery Procedures

18 The delivery process for the TOE consists of three phases:

a) Security Environment

b) Pre-Delivery Activities

c) Shipping Process

19 Further information about these procedures is provided in Section 4.2 of the Delivery documentation.

1.9 Documentation

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

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

[1]. RSA Security Analytics v10.6.1 Security Target v1.0

[2]. RSA Security Analytics Security Analytics Getting Started Guide for Version 10.6.1

[3]. RSA Security Analytics System Security and User Management Guide for version 10.6

[4]. RSA Security Analytics Command Line Interface for Version 10.6.1

[5]. RSA Security Analytics Data Privacy Management Guide for Version 10.6.1

[6]. RSA Security Analytics Deployment Guide for version 10.6.1

[7]. RSA Security Analytics Virtual Host Setup Guide for version 10.6.1

[8]. RSA Security Analytics Warehouse Analytics Guide for version 10.6.1

[9]. RSA Security Analytics Log Collection for version 10.6.1

[10]. RSA Security Analytics Hosts and Services Getting Started Guide for version 10.6.1

[11]. RSA Security Analytics Licensing for version 10.6.1

[12]. RSA Security Analytics System Maintenance Guide for version 10.6.1

[13]. RSA Security Analytics System Configuration Guide for version 10.6.1

[14]. RSA Security Analytics Archiver Configuration Guide for Version 10.6.1

[15]. RSA Security Analytics Broker and Concentrator Configuration Guide for Version 10.6.1

[16]. RSA Security Analytics RSA Product Verification Checklist

[17]. RSA Security Analytics Decoder and Log Decoder Configuration Guide for Version 10.6.1

[18]. RSA Security Analytics Incident Management Configuration Guide for Version 10.6.1

[19]. RSA Security Analytics Investigation and Malware Analysis Guide for Version 10.6.1

[20]. RSA Security Analytics User Documentation

[21]. RSA Security Analytics Reporting Engine Configuration Guide for Version 10.6.1

[22]. RSA Security Analytics Alerting Using ESA for Version 10.6.1

[23]. RSA Security Analytics Event Stream Analysis Configuration Guide for Version 10.6.1

[24]. RSA Security Analytics Malware Analysis Configuration Guide for Version 10.6.1

[25]. RSA Security Analytics System Security and User Management for Version 10.6.1

2 Evaluation

22 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 (EAL2) Augmented with ALC_FLR.1. 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

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

2.1.1 Life-cycle support

24 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators confirmed that the TOE provided for evaluation is labelled with its reference.

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

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

27 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.

28 The evaluators confirmed that the configuration list in CM documentation 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

29 The evaluators confirmed that the configuration list uniquely identifies each configuration item and configuration list indicates the developer of each TSF relevant configuration item.

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

31 The evaluators examined the flaw remediation procedures documentation and determined that it described the procedures used to track all reported security flaws in each release of the TOE.

32 The evaluators examined the flaw remediation procedures and determined that the application of these procedures would produce a description of each security flaw in terms of its nature and effects.

33 The evaluators examined the flaw remediation procedures and determined that the application of these procedures would identify the status of finding a correction to each security flaw.

34 The evaluators checked the flaw remediation procedures and determined that the application of these procedures would identify the corrective action for each security flaw.

35 The evaluators examined the flaw remediation procedures documentation and determined that it describes a means of providing the TOE users with the necessary information for each security flaw.

2.1.2 Development

36 The evaluators examined the security architecture description in the Design Documentation 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.

37 The evaluators examined the security 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.

38 The evaluators examined the functional specification in the Design Documentation and determined that the TSF is fully represented, it states the purpose of each TSF Interface (TSFI) and the method of use for each TSFI.

39 The evaluators examined the TOE design in the Design Documentation and determined that the structure of the entire TOE is described in term of subsystems.

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

2.1.3 Guidance documents

41 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.

42 The evaluators examined the provided delivery acceptance and determined that it describes the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

2.1.4 IT Product Testing

43 Testing at EAL2 Augmented with ALC_FLR.1 consists of assessing developer tests, performing independent functional tests, and performing penetration tests. The TOE testing was conducted by evaluators from 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 Report.

2.1.4.1 Assessment of Developer Tests

44 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).

45 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

46 At EAL2 Augmented with ALC_FLR.1, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of the developer's test plan, and creating test cases that augment developer tests.

47 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The evaluators confirmed that the developer supplied test documentation includes test plans, expected test results and actual test results. The results of the independent functional tests that were developed and performed by the evaluators are consistent with the expected test results in the test documentation.

Identifier	Security Function	Descriptions
TEST-IND-001	FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FIA_ATD.1, FIA_UAU.5, FMT_SMR.1 FMT_MTD.1, FMT_SMF.1 FTA_TAB.1	• To test the timing of the authentication of the user when authenticating to the TOE User Interface (UI) • To test that the user is successfully authenticated before allowing any other TSF-mediated actions on behalf of that user • To test that the user is successfully identified before allowing any other TSF-mediated actions on behalf of that user • To test that the TOE shall restrict the ability to enable or disable the functions of the TOE only to the associated roles • To test that the TSF shall maintain a list of security attributes belonging to individual users • To test that the TSF shall provide mechanisms needed to support user authentication • To test that the TSF shall maintain and associate user with a set of roles • To test that the TSF shall restrict the ability to manage the TSF data to a list of authorized identified roles • To test that the TOE shall be capable to perform

Identifier	Security Function	Descriptions
		security management functions • To test that before establishing a user session, the TSF shall display an advisory warning message
TEST-IND-002	FIA_UAU,1, FIA_UID.1 FIA_UAU.5, FCS_SSH_EXT.1 FCS_TLS_ExT.1, IDS_ANL_EXT.1 IDS_RCT_EXT.1, IDS_RDR_EXT.1 FMT_MTD.1, FMT_SMF.1 FPT_ITT.1, FTP_TRP	• To test that the TSF shall implement SSH protocol that supports public-key based encryptions • To ensure the SSH transport implements a set of fixed encryption algorithms and no other public key algorithm • To test the integrity of the data algorithms • To ensure that the TSF implements a set of protocols that supports a list of fixed cipher suites. • To test that the TSF could perform statistical or signature based functions on the IDS Data • To test that the TSF shall record each analytical result along with date & time, type of result and identification of data resource. • To test that the TSF shall send an alarm to the incident management SA views when an intrusion is detected. • To ensure that the TSF would provide Analyst and Administrator role the ability to read all metadata, raw logs, raw packet data and incident management data from the IDS • To ensure that the TSF provides the IDS data in a manner suitable for the user to interpret • To test that the TSF shall prohibit all users read access to the IDS data, except to those who have been granted read-access. • To test that the TSF shall protect the TSF data when transmitted between separate parts of the TOE • To test that the TSF shall provide a communication path between itself and users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data • The TSF shall permit remote users or authorized IT entities to initiate communication via the trusted path.
TEST-IND-003	FMT_MTD.1, FMT_SMF.1 FTA_SSL.3, FTA_SSL.4 FIA_AFL.1	• To test that the TSF shall restrict the ability to manage the TSF data to authorized identified roles • To test that the TSF shall be capable of performing the security management functions

Identifier	Security Function	Descriptions
		• To test that the TSF shall terminate an interactive session after a set of time interval of user inactivity configured by authorized administrator • To ensure the TSF shall allow user-initiated termination of the user's own interactive session • To test that the TSF shall detect when a number of unsuccessful authentication attempts occur related to SA UI • To ensure that when the defined number of unsuccessful authentication attempts has been surpassed the TSF shall lock account for a specified time period as configured by authorized administrator
TEST-IND-004	FAU_GEN1.1, FAU_GEN.1.2, FAU_GEN.2.1, FAU_SAR.1.2	• To ensure that the TSF shall be able to generate an audit record of the auditable functions of the TOE • To test that the TSF shall record within each audit record the date & time of the event, type of event, subject identity, and the outcome of the event • To ensure that for audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event. • To test that the TSF shall provide Operator and Administrator roles with the capability to read all audit information from the audit records. • To ensure that the TSF shall provide the audit records in a manner suitable for the user to interpret the information. • To test that the TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access • To ensure that the TSF shall protect the stored audit records in the audit trail from unauthorised deletion. • To test that the TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

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

2.1.4.3 Penetration Testing

49 The evaluators performed a 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, TOE design, and security architecture description.

50 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 (elapse time);

b) Specialist technical expertise required (specialised expertise);

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

d) Window of opportunity; and

e) IT hardware/software or other requirement for exploitation.

51 The penetration tests focused on:

a) General Vulnerability Scan

b) Unnecessary Open Ports

c) Web Vulnerability

d) Weak Cipher

e) Cookie & Session Tampering

52 The results of the penetration testing noted that there was 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

53 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in the Security Target and its functional specification. In addition, the documentation supplied as evidence for the EAL2 Augmented with ALC_FLR.1 Common Criteria evaluation of the TOE was analysed to identify possible vulnerabilities.

3 Result of the Evaluation

54 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 RSA Security Analytics performed by BAE Systems Applied Intelligence MySEF.

55 BAE Systems Applied Intelligence MySEF, found that RSA Security Analytics upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) assurance Level 2 Augmented with ALC_FLR.1 (EAL2+ ALC_FLR.1).

56 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

57 EAL2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

58 The analysis is supported by 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.

59 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

60 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.

b) The users should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

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, 26 February 2016.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1c, 26 February 2016.

[6] RSA Security Analytics v10.6.1 Security Target, Version 1.0, 15 December 2016

[7] C077 Evaluation Technical Report for RSA Security Analytics, EAU000437-S036-ETR v1.0, 27 January 2017

A.2 Terminology

A.2.1 Acronyms

Table 2: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
TSFI	TOE Security Functions Interface
SFR	Security Functional Requirement
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

Acronym	Expanded Term
MySEF	Malaysian Security Evaluation Facility
API	Application Programming Interface
CC	Common Criteria
EAL	Evaluation Assurance Level
EPS	Events per Second
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
LAN	Local Area Network
OS	Operating System
OSI	Open Systems Interconnection
PP	Protection Profile
SDEE	Security Device Event Exchange
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
Analyzer	The function of an IDS that applies analytical processes to collected IDS data in order to derive conclusions about potential or actual intrusions.
Concentrator	A concentrator that receives network packets.
Decoder	A decoder that captures network packets.
IDS	Intrusion Detection System —a combination of services or functions such as an Analyzer that monitors an IT System for activity that may inappropriately affect the IT System or its resources, and that can send alerts if such activity is detected.
IDS data	Refers both to raw data collected by the TOE and to the results of analysis applied by the TOE to that data.
Index	Indexes are internal RA data structures that organize for searching the metadata elements of sessions and are

Acronym	Expanded Term
	generated during data processing for a collection. The content of the index, and consequently the metadata elements that are displayed in the Navigation view, are controlled by settings in effect during collection processing.
Log Concentrator	A concentrator that receives log data,
Log Decoder	A decoder that captures log data.
Metadata	Specific data types (Service Type, Action Event, Source IP Address, etc.) created by the parsers which are counted and itemized in the captured data. A detailed list of metadata for each parser may be found in the SA Guidance.
Parser	A software module that defines tokens and instructions for lexical processing of network streams. Processing includes stream identification and metadata extraction.
Services	Components of the product that work together to provide the security functions of the TOE such as Analyzer, Concentrator, and Decoder

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

Term	Definition and Source
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.
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 ---