CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science,
Technology and Innovation

M004 Maintenance Report

File name: ISCB-5-RPT-M004-AMR-v1
Version: v1
Date of document: 30 March 2016
Document classification: PUBLIC

Malaysian Common Criteria Evaluation & Certification Scheme
MyCC

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

M004 Maintenance Report

RSA Security Analytics v10.6

30 March 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:	M004 Maintenance Report
DOCUMENT REFERENCE:	ISCB-5-RPT-M004-AMR-v1
ISSUE:	v1
DATE:	30 March 2016

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

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

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

Printed in Malaysia

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	25/3/2016	All	Initial draft of maintenance report
v1	30/3/2016	All	Final version of maintenance report

Table of Contents

1 Introduction

1 RSA Security Analytics v10.4 (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.

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

3 Identification Information

Table 1 – Identification Information

Assurance Maintenance Identifier	M004
Project Identifier	C060
Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Impact Analysis report	Impact Analysis Report, RSA Security Analytics, ISSX1726-IAR-1.0, 17 March 2016, version 1.0
New TOE	RSA Security Analytics v10.6
Certified TOE	RSA Security Analytics v10.4
New Security target	RSA Security Analytics Security Target Version, v1.0, 17 March 2016
Certified Security Target	RSA Security Analytics Security Target Version, v0.3, 27 April 2015
Evaluation Level	Evaluation Assurance Level 2 (EAL2) Augmented with ALC_FLR.1
Evaluation Technical Report (ETR)	Evaluation Technical Report for RSA Security Analytics v1.0, 13 July 2015 (EAU000073-S026-ETR v1.0)
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [VI])

Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref[VII])
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL2 Augmented (ALC_FLR.1)
Protection Profile Conformance	None
Sponsor & Developer	RSA The Security Division of EMC 10700 Parkridge Blvd. Suite 600 Reston, VA 20191
Evaluation Facility	BAE Systems Applied Intelligence MySEF

2 Description of Changes

4 RSA has issued a new release of the RSA Security Analytics v10.6. The changes to the TOE consist of twelve (12) new features and five (5) minor fixes, where no additional security functionality was added and no existing security functionality was removed (ref[I]).

2.1. Changes to the product associated with the certified TOE

5 The following features have been added in RSA Security Analytics v10.6 (ref[III]):

a) RSA Secure Analytics Archiver

b) RSA Secure Analytics Platform

c) RSA Secure Analytics Log Collector

d) RSA Secure Analytics Investigation

e) RSA Secure Analytics Malware Analysis

f) RSA Secure Analytics Reporting

g) RSA Secure Analytics Administration

h) RSA Secure Analytics Health & Wellness

i) RSA Secure Analytics Event Source Management

j) RSA Secure Analytics Live

k) RSA Secure Analytics Event Stream Analysis

l) RSA Secure Analytics Core Services

6 The following items provide clarification or describe issues fixed in this release (ref[III]):

a) Security Enhancement

b) Log Collector Fixes

c) Malware Analysis Fixes

d) Incident Management Fixes

e) Reporting FixesChanges to the development environment associated with the certified TOE

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

3 Affected Developer Evidence

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

a) RSA Security Analytics Security Target, 17 March 2016, version 1.0

b) RSA Security Analytics Release Notes, version 10.6, 2016

c) RSA Security Analytics ALC Life Cycle Support Guidance, version 0.2, 17 March 2016

Annex A References

[I] Impact Analysis Report (IAR), ISSX1726-IAR-1.0, 17 March 2016, version 1.0

[II] RSA Security Analytics Security Target Version, v0.3, 27 April 2015

[III] RSA Security Analytics Security Target Version, v1.0, 17 March 2016

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

[V] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014.

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

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

[VIII] MyCC Scheme Policy (MyCC_P1), v1d, CyberSecurity Malaysia, 26 February 2016.

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

[X] C060 Evaluation Technical Report for RSA Security Analytics, EAU000073-S026-ETR v1.0, 13 July 2015

Result of the Analysis

9 The outcome of the review changes that were made to the TOE of this report found that none of the modifications significantly affects the security mechanisms that implement the functional requirements of the Security Target (ref[III]) as required in accordance of Assurance Continuity: CCRA Requirements Version 2.1 (2012-06-01) June 2012 (ref[IV]).

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

--- END OF DOCUMENT ---