C096 Certification Report

RSA NetWitness Suite V11.0

File name: ISCB-5-RPT-C096-CR-v1
Version: v1
Date of document: 31 July 2018
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

C096 Certification Report

RSA NetWitness Suite V11.0

31 July 2018

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 D Fax: +603 8992 6841
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C096 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C096-CR-d1
ISSUE:	v1
DATE:	31 July 2018

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 31 July 2018 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	13 July 2018	All	Initial draft of certification report
v1	20 July 2018	All	Final Certification report

Executive Summary

The Target of Evaluation (TOE) is RSA NetWitness Suite v11.0. The TOE 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). It provides real-time visibility into the monitored network and long-term network data storage to provide detection, investigation, analysis, forensics, and compliance reporting. The RSA NetWitness Suite capture infrastructure imports log data and collects packet data from the network. Packet collection extracts metadata, reassembles, and globally normalizes all network traffic at layers 2 through 7 of the OSI model. This data allows the TOE to perform real-time session analysis. The RSA NetWitness Suite recognizes over 250 event source types, which are aggregated, analyzed, and stored for long-term use. It implements Collection Methods to support collection from the event sources

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) Augmented 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 June 2018.

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 RSA NetWitness Suite v11.0 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.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The TOE is a collection of appliances that form a security infrastructure for an enterprise network. This architecture provides converged network security monitoring and centralised security information and event management (SIEM). RSA NetWitness Suite provides real-time visibility into the monitored network and long-term network data storage to provide detection, investigation, analysis, forensics, and compliance reporting.

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

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Monitoring with Security Information and Event Management (SIEM)
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

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	C096
TOE Name	RSA NetWitness Suite
TOE Version	11.0
Security Target Title	RSA NetWitness Suite v11.0 Security Target
Security Target Version	Version 1.0
Security Target Date	31 May 2018
Assurance Level	Evaluation Assurance Level 2 Augmented ALC_FLR.1

Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [2])
Methodology	Common 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 EAL 2 with Augmented ALC_FLR.1
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive, Columbia, Maryland 21046
Developer	RSA Security LLC 10700 Parkridge Blvd. Suite 600, Reston, VA 20191
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 2.2 of the Security Target (Ref [6]).

7 The TOE architecture consists of the following components:

- Decoder: The Decoder performs capture for either packets or logs.
- Windows Legacy Log Collector - also identified as Windows (legacy): The Windows Legacy Log Collector is deployed in a Windows Legacy domain(s).
- Concentrator: Concentrators are deployed as either a packet or log Concentrator. These appliances aggregate and store metadata received from multiple Decoders.
- Broker: Brokers facilitate queries between Concentrators, allowing the NetWitness Server access to metadata across the network.
- NetWitness Server: The NetWitness Server hosts the user interface. This interface enables an administrator to perform incident detection, management, investigation, and device and user administration.
- Archiver: The Archiver receives, indexes, and compresses log data from Log Decoders.

- Event Stream Analysis: The Event Stream Analysis (ESA) provides advanced stream analytics such as correlation and event processing. ESA receives event data from multiple Concentrators.
- Malware Analysis Enterprise: The Malware Analysis service analyzes file objects to assess the likelihood the file is malicious.
- Automated Threat Detection: The Automated Threat Detection (ATD) Service is deployed on the same appliance as ESA and receives metadata data from multiple Concentrators.
- Respond: Collects Alerts, displays the alerts on the RSA NetWitness Suite Respond user interface, and provides authorized users the ability to group the alerts logically and start an Incident response workflow to investigate and remediate the security issues raised.
- Reporting Engine: The Reporting Engine supports the definition and generation of reports and alerts.

8 The following figure depicts the TOE in its evaluated configuration. Note that each NetWitness Server and ESA host also contains a Mongo database though not shown in the figure. Also, not depicted is the Windows Legacy Log Collector deployed in a Windows Legacy domain(s). The Windows Legacy Log Collector sends log data over the network to the Log Decoder. The Malware Analysis component aggregates data from a Packet Decoder. This communication channel is not depicted in the figure.

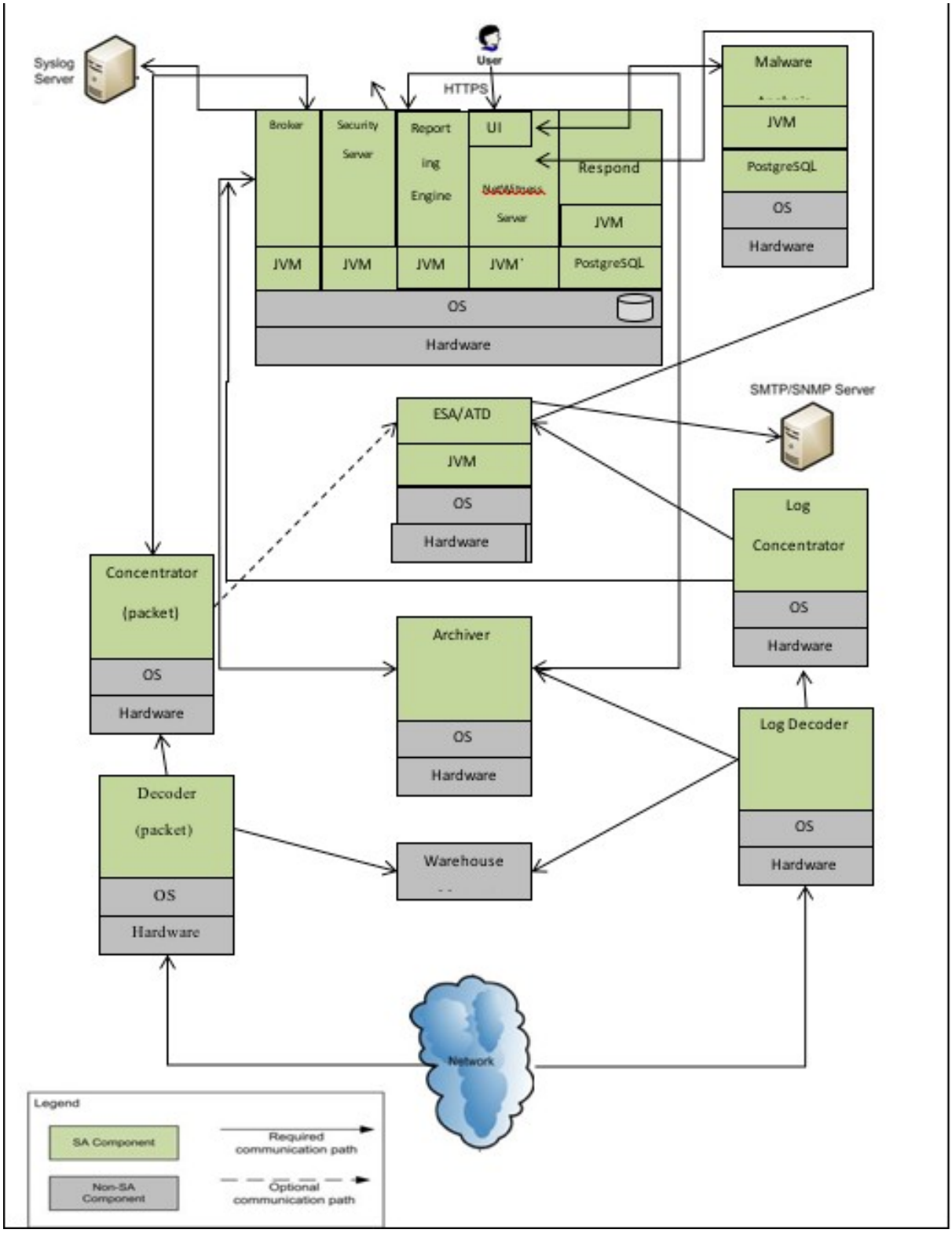

Figure 1: Evaluated Configuration

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:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Monitoring with Security Information and Event Management (SIEM)
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

10 **Security Audit:** The TOE generates audit records of security relevant events that include at least the 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.

11 **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) for both SSH and TLS communications. The TOE uses the RSA BSAFE Crypto-J cryptographic library: BSAFE SSL-J 6.2.1.1 for Java applications, which incorporates BSAFE Crypto-J 6.2 (FIPS 140-2 Certificates #2468).

12 **Identification & 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).

13 **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 RSA NetWitness Suite Respond User Interfaces. The interfaces 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, Administrator, and Respond Administrator roles can read the metadata, raw logs, raw packet data, and incident management (including alerts) from the IDS data.

14 **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, Respond Administrator, Analyst, Operator, SOC_Manager, Malware Analyst, and Data Privacy Officer. 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.

15 **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.

16 **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.

17 **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 RSA NetWitness Suite 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

1.5 Clarification of Scope

18 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.

19 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]).

20 RSA NetWitness Suite product components excluded from the TOE in the evaluated configuration are:

- Warehouse appliance
- RSA Live (content delivery and Live Connect)

- Malware Community
- Malware Sandbox

21 RSA NetWitness Suite product features excluded from the TOE in the evaluated configuration are:

- Direct-Attached Capacity (DAC) storage for Archiver
- Representational State Transfer, Application Programming Interface (REST API)
- External authentication services (such as RADIUS, LDAP, and Windows Active Directory)
- Export of security audit records to Syslog server
- Sending SMTP, SNMP, or Syslog alerts
- Integrated Dell Remote Access Controller (iDRAC) out-of-band appliance management capabilities
- Serial and USB device connections (Used during installation and maintenance only)

22 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

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

24 Intended usage assumptions:

a) The operational environment will provide the capability to protect audit information.

b) The data sources in the environment provide complete and reliable data to the TOE.

c) The environment will provide reliable time sources for use by the TOE.

25 Physical assumptions:

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.

26 Personnel assumptions:

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

b) TOE Administrators will follow and apply all administrator guidance in a trusted manner.

c) Users will protect their authentication data

1.7 Evaluated Configuration

27 As stated in the ST (Ref [6]), there are eleven (11) main components of the TOE that make up the evaluated configuration, namely the Decoder, Windows Legacy Log Collector, Concentrator, Broker, NetWitness Server, Archiver, Event Stream Analysis, Malware Analysis Enterprise, Automated Threat Detection, Respond, and Reporting Engine.

28 The TOE components are deployed as virtual appliances or hardware-based solutions in a multi-server environment. The NetWitness Server component of the TOE provides a management interface that allows user to perform management interface that allows users to perform management and security functions on the TOE.

29 The evaluated configuration requires that all communications between distributed components of the TOE occur over TLS in FIPS mode, which provides confidentiality and integrity of transmitted data. The configured mode determines the cryptographic protocols and the underlying cryptographic provider the TOE uses to implement secure communications.

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

- Syslog server to receive security audit record and alerts from the NetWitness Server.
- SMTP Server to send email messages or alerts from the NetWitness Server.
- SNMP Server to send SNMP traps from the NetWitness Server.
- Authentication Server (such as Windows Active Director, RADIUS, and LDAP) to support user authentication.

1.8 Delivery Procedures

31 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.

32 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.

33 The TOE delivery procedures include two forms:

- TOE Software: Users are provided access to the Download Center (DLC) system which provides the downloadable files over a secure internet connection. Email notifications containing the login credentials and Universal Resource Locator (URL) for the DLC server and serial number/license number information for the product are sent to customers. After the initial purchase, customers are notified of product updates by RSA through email.

- TOE Hardware: RSA NetWitness Suite appliances are shipped from UNICOM using either United Parcel Service (UPS) or FedEx to provide delivery.
- The RSA Product Verification Checklist provides the secure acceptance procedures for validating the hardware and software products received. For hardware acceptance, the TOE user should inspect the packaging of the hardware to ensure that it has not been tampered with, the TOE version upon booting the system and the appliance serial number. For software acceptance, the TOE user should validate the checksum of each OVA file and compare it to the checksum from the download site to ensure the authenticity of the software downloaded.

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

1.9 Documentation

35 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.

- RSA NetWitness Suite System Security and User Management, for version 11.0, October 2017
- RSA NetWitness Suite Hosts and Services Getting Started Guide, for version 11.0, November 2017
- RSA NetWitness Suite Getting Started Guide, for version 11.0, October 2017
- RSA NetWitness Suite System Configuration Guide, for version 11.1
- RSA NetWitness Suite Deployment Guide, for version 11.0, October 2017
- RSA NetWitness Suite Respond Configuration Guide, for version 11.0, October 2017
- RSA NetWitness Suite Respond User Guide, for version 11.0, October 2017
- RSA NetWitness Suite Investigate and Malware Analysis User Guide, for version 11.0, December 2017
- RSA NetWitness Suite System Maintenance Guide, for version 11.0, October 2017
- RSA NetWitness Suite Data Privacy Management Guide, for version 11.0, October 2017
- RSA NetWitness Suite Virtual Host Setup Guide, for version 11.0, October 2017
- RSA NetWitness Suite AWS Deployment Guide, October 2017
- RSA NetWitness Suite Licensing Management Guide, for version 11.0, October 2017

2 Evaluation

36 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 Augmented (ALC_FLR.1). The evaluation was performed conformant to the ISCB Product Certification Schemes Policy (PRODUCT_SP) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM)(Ref [5]).

2.1 Evaluation Analysis Activities

37 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

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

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

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

41 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

42 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.

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

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

2.1.1.3 TOE Delivery

45 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.

2.1.1.4 Basic Flaw Remediation

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

47 The evaluator 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.

48 The evaluator 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.

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

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

2.1.2 Development

2.1.2.1 Architecture

51 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.

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

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

54 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

55 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,

56 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,

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

2.1.2.3 TOE Design Specification

58 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.

59 The evaluators examined the TOE and determined that each SFR-non interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is SFR-non interfering.

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

61 The evaluators examined the TOE design and determined that it provided a complete and accurate high-level description of the SFR-supporting and SFR-non interfering behaviour of the SFR-enforcing subsystems. The evaluators determined that the TOE design provided a complete and accurate high-level description of the behaviour of the SFR-supporting subsystems.

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

63 The evaluators determined that all 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

64 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.

65 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.

66 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.

67 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.

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

2.1.3.2 Preparation Guidance

69 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.

70 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.

71 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

72 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

73 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

74 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.

75 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	• Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. • 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.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FAU_SAR.1.1, FAU_SAR.1.2, FCS_TLS_EXT.1.1, FIA_ATD.1.1, FIA_UAU.1.2, FIA_UAU.5.1, FIA_UAU.5.2, FIA_UID.1.2, FMT_MOF.1.1(1),

Test ID	Description	SFRs
	• 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.	FMT_MTD.1.1, FMT_SMF.1.1, FMT_SMR.1.1, FMT_SMR.1.2, FPT_ITT.1.1, FTA_SSL.4.1, FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3
TEST-IND-002	• Verify that the TSF performs identification and authentication, and TOE access functions such as detection of unsuccessful authentication attempts, account lockout, inactive session termination and display of TOE access banner. • Verify that authorised users are able to determine and modify the behaviour of security management functions. • Verify that the TSF restricts access to audit record 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.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.2.1, FAU_STG.1.1, FAU_STG.1.2., FIA_AFL.1.1, FIA_AFL.1.2, FIA_UAU.1.1, FIA_UAU.1.2, FIA_UID.1.1, FIA_UID.1.2, FMT_MTD.1.1, FMT_SMF.1.1, FTA_SSL.3.1, FTA_TAB.1.1
TEST-IND-003	• Verify that the TSF provides the ability to analyse IDS data and configure alarms, display alarm notifications, protect IDS sensitive data and enforce data retention limits. • Verify that the TSF provides the capability to view IDS data and restricts access to IDS data based on role access. • Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. • 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_GEN.2.1, FAU_SAR.1.1, FAU_SAR.1.2, FIA_UAU.5.1, FIA_UAU.5.2, IDS_ANL_EXT.1.1, IDS_ANL_EXT.1.2, IDS_DOR_EXT.1.1, IDS_RCT_EXT.1.1, IDS_RDR_EXT.1.1(1), IDS_RDR_EXT.1.1(2), IDS_RDR_EXT.1.1(3), IDS_RDR_EXT.1.2(1), IDS_RDR_EXT.1.2(2), IDS_RDR_EXT.1.2(3), IDS_RDR_EXT.1.3(1), IDS_RDR_EXT.1.3(2),

Test ID	Description	SFRs
		IDS_RDR_EXT.1.3(3), FMT_MOF.1.1(2), FMT_MTD.1.1, FMT_SMF.1.1

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

2.1.4.3 Penetration Testing

77 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.

78 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.

79 The penetration tests focused on:

a) Unnecessary Open Ports

b) Common Web Vulnerability Scan

c) Cookie Injection/Broken Authentication

d) Security Misconfiguration

e) Input and data validation

f) Secure Communication

80 The results of the penetration testing demonstrate 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

81 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 Augmented ALC_FLR.1 Common Criteria evaluation of the TOE was analysed to identify possible vulnerabilities.

3 Result of the Evaluation

82 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 NetWitness Suite v11.0 performed by BAE Systems Applied Intelligence MySEF.

83 BAE Systems Applied Intelligence MySEF found that RSA NetWitness Suite v11.0 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) Augmented ALC_FLR.1.

84 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

85 EAL 2 Augmented ALC_FLR.1 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.

86 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.

87 EAL 2 Augmented ALC_FLR.1 also provides assurance through use of a configuration management system, evidence of secure delivery procedures and basic flaw remediation.

3.2 Recommendation

88 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) Potential purchasers of the TOE should ensure that the administrators responsible for the TOE are provided sufficient training and are familiar with the guidance supplements prior to configuring and administering the TOE.

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] ISCB Product Certification Schemes Policy (PRODUCT_SP), v1a, CyberSecurity Malaysia, June 2017.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v1, June 2017.

[6] RSA NetWitness Suite v11.0 Security Target, Version 1.0, 31 May 2018

[7] EAU000427-S040-ETR, Evaluation Technical Report, Version 1.0, 5 July2018

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
ESA	Event Stream Analysis
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
OSI	Open System Interconnection
PP	Protection Profile

Acronym	Expanded Term
SIEM	Security information and event management
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.

Term	Definition and Source
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 ---