MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C108 Certification Report

RSA NETWITNESS PLATFORM V11.3

File name: ISCB-3-RPT-C108-CR-v1
Version: v1
Date of document: 27 March 2020
Document classification : PUBLIC

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

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999
www.cybersecurity.my

C108 Certification Report
RSA NETWITNESS PLATFORM V11.3

27 March 2020
ISCB Department

CyberSecurity Malaysia
Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C108 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C108-CR-v1
ISSUE:	v1
DATE:	27 March 2020
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

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 3 April 2020, 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 associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (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	18 March 2020	All	Initial draft
v1.0	27 Mar 2020	All	Baselined

Executive Summary

The Target of Evaluation (TOE) is RSA NetWitness Platform v11.3. NetWitness 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). NetWitness provides real-time visibility into the monitored network and long-term network data storage to provide detection, investigation, analysis, forensics, and compliance reporting.

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 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 Lab – MySEF and the evaluation was completed on 24 January 2020.

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 Platform V11.3 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 RSA NetWitness Platform v11.3 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). NetWitness provides real-time visibility into the monitored network and long-term network storage to provide detection, investigation, analysis, forensics, and compliance reporting.

2 The TOE includes the following security functions:

- Security Audit
- Cryptographic Support
- Identification & 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 Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C108
TOE Name	RSA NetWitness Platform
TOE Version	V11.3
Security Target Title	RSA NetWitness Platform v11.3 Security Target
Security Target Version	V1.0
Security Target Date	19 February 2020
Assurance Level	Evaluation Assurance Level 2 Augmented with ALC_FLR.1

Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL 2 Augmented with ALC_FLR.1
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive, Columbia, Maryland 21046, United States of America
Developer	RSA The Security Division of EMC[2] 10700 Parkridge Blvd, Reston, VA 20191, United States of America
Evaluation Facility	BAE Systems Lab - MySEF

1.3 Security Policy

4 There is no organisational security policies defined regarding the use of TOE.

1.4 TOE Architecture

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

1.4.1 Logical Boundaries

6 The TOE consists of the following security functions identified in the Security Target (Ref [6]).

Table 2: RSA NetWitness Logical Boundaries

Security Audit	The TOE generates audits 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 authorized administrators with the ability to read the audit events.

	The TOE relies on its operational environment to store the audit records and to provide the system clock information that is used by the TOE to timestamp each audit record.
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).
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).
Security Monitoring with Security Information and	The TOE receives network packets, reconstructs network transactions, extracts metadata, and applies rules. The rules identify interesting events, effectively matching

Event Management (SIEM)	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 NetWitness Respond User Interfaces. The NetWitness Respond User 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. The UEBA_Analyst and Administrator can view the user behavioral anomalies in the UEBA User Interface.
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: Root User, Administrator, Respond Administrator, Analyst, Operator, SOC_Manager, Malware Analyst, UEBA_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.
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.
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.
Trusted Path/Channels	The TOE requires remote user 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 NetWitness 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 ensures the administrative session is secured from disclosure and modification.

1.4.2 Physical Boundaries

7 Product components included in the TOE are listed below. Figure 1 illustrates a representative diagram of the TOE in its evaluated configuration.

- Windows Legacy Log Collector
- Decoder
- Log Decoder
- Concentrator

- Log Concentrator
- Endpoint Log Hybrid
- Broker
- Event Stream Analysis (ESA)
- Archiver
- NetWitness Server
- Respond
- Malware Analysis
- Automated Threat Detection (one for each ESA host)
- Reporting Engine (one per NetWitness server)
- Java Virtual Machine (JVM) (one for each of the following services on the NetWitness Server: Broker, Respond, Malware Analysis, Reporting Engines Services, and one for the UI and NetWitness Server itself. Additionally, the ESA runs in its own JVM)
- PostgreSQL database (one for each of the following services: Malware Analysis, and Reporting Engine)
- Mongo database (one for each NetWitness Server, Endpoint Server, and ESA)
- NetWitness User and Entity Behavior Analysis (UEBA)

8 The TOE relies on the following services and products in its operational environment:

- Operating System: provides execution environment for NetWitness components. The OS is CentOS version 7.5 running on a Dell R630 or R730xd
- Customer provided hardware and Windows operating system for Legacy Windows Log Collector meeting minimum system requirements below:
  - Windows 2008 R2 SP1 64-Bit or Windows 2012 64-bit
  - Processor – Intel Xeon CPU @2.0Ghz or faster
  - Memory – 4GB or faster
  - Available Disk Space - 320GBMicrosoft .NET Framework 4.6.1 or 4.6.2
- Hypervisor: provides virtualization for NetWitness virtual appliances. The hypervisor is ESXi version 5.5, 6.0, 6.5, or 6.7
- Administrator Workstation / Browser: provides human users access to NetWitness Server user interface. Compatible browsers that support the required features for NetWitness 11.3 include modern (or current) versions of Google Chrome, Mozilla Firefox, and Apple Safari

- Network Traffic Sources: source of network traffic. **Note:** The TOE has a direct physical connection to a network traffic source (Decoder (packet) network connection)
- Log Decoder and Collector Collection Methods: provide log data to the TOE. Within a Log Decoder appliance is a Log Collector service[1] that imports logs utilizing various Collection Methods. The Collection Methods supported as part of the baseline are::
  - Syslog
  - SNMP Trap
  - NetFlow
  - File (pushed by SFTP and FTPS)
  - Windows (WinRM)
  - Windows (Legacy)
  - ODBC
  - Check Point LEA
  - VMWare
  - SDEE
  - Cloud (Including AWS CloudTrail and Microsoft Azure)
  - Office365
  - Windows Log Collection and Endpoint Data
- The Endpoint Log Hybrid collection methods: Windows, Mac, or Linux hosts for collecting host inventories, processes, user activity, and Windows logs

9 The following services can be deployed in the operational environment but were not covered by the evaluation:

- Syslog server: NetWitness Server can forward security audit records and alerts to an external Syslog server
- SMTP Server: NetWitness Server can send email messages via SMTP server
- SNMP Server: NetWitness Server can send SNMP traps
- Authentication Servers: provides external authentication methods (such as Windows Active Director, RADIUS, and LDAP)

10 NetWitness product components excluded from the TOE in the evaluated configuration are:

- Warehouse appliance

[1] The Log Collector service can also be deployed separately from a Log Decoder appliance as a Virtual Log Collector.

- RSA Live (content delivery and Live Content)
- Malware Community
- Malware Sandbox
- Endpoint Agent

11 NetWitness 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 management capabilities
- Serial and USB device connections (Used during installations and maintenance only)

12 The following diagram is a representation of the evaluated configurations of the TOE and its components.

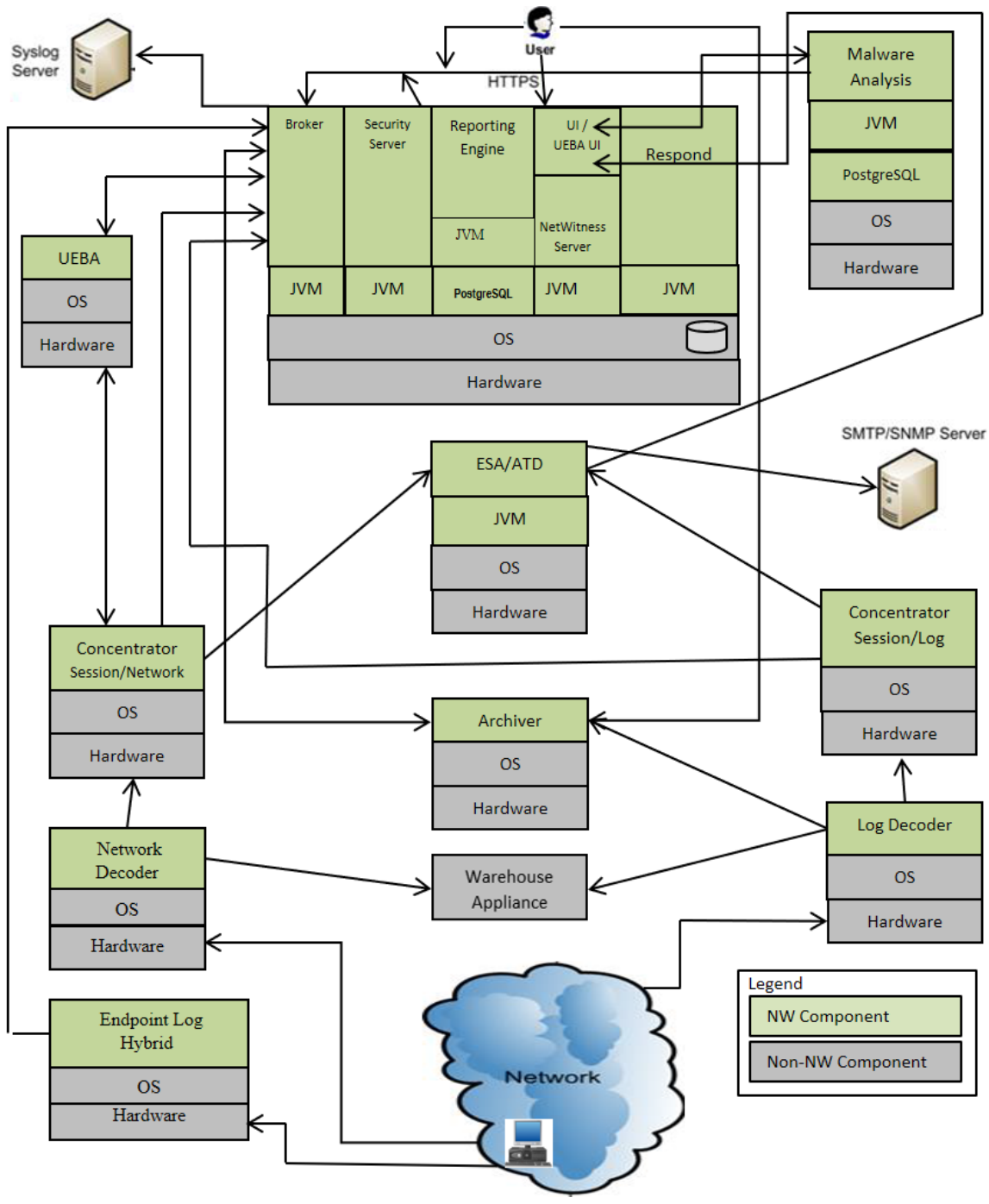

Figure 1: TOE Evaluated Configuration

1.5 Clarification of Scope

13 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

14 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]).

15 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 requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

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

1.6.1 Operational Environment Assumptions

17 Assumptions for the TOE environment as described in the Security Target (Ref [6]):

Table 3: Assumptions for the TOE environment

Assumption	Statements
A.AUDIT_PROTECTION	It is assumed that the operational environment will provide the capability to protect audit information.
A.DATA_SOURCES	It is assumed that the data sources in the environment provide complete and reliable data to the TOE.
A.TIME	It is assumed that the environment will provide reliable time sources for use by the TOE.
A.DEPLOY	It is assumed that TOE Administrators will properly configure the network in the TOE operational environment and configure adequate network capacity for the deployed TOE components.

Assumption	Statements
A.PHYSICAL	It is assumed that the TOE hardware and software critical to the security policy enforcement will be located within controlled access facilities which will prevent unauthorized physical access.
A.MANAGE	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.
A,TRUSTED_ADMIN	It is assumed that TOE Administrators will follow and apply all administrator guidance in a trusted manner.
A.USER	It is assumed that users will protect their authentication data.

1.7 Evaluated Configuration

18 The TOE may be deployed in a number of configurations consistent with the requirements identified in this Security Target (Ref [6]). There are two (2) main components that make up the TOE in its evaluated configuration.

19 Capture Architecture is composed of the Decoder, Windows Legacy Log Collector, Concentrator, Broker and Endpoint Log Hybrid, as described below;

- Decoder – captures for either packets or logs. When deployed, either the packet or log capture capability is enabled
- Windows Legacy Log Collector – performs log capture by retrieving the log records from a Legacy Windows event source
- Concentrator – aggregates and stores metadata received from multiple Decoders. Metadata received on a Concentrator is indexed and also may be sent to an ESA device for further analysis for detection and alerting
- Broker – facilitate queries between Concentrators, allowing the NetWitness Server access to metadata across the network
- Endpoint Log Hybrid – collects and manages endpoint (host) data from Windows, Mac, and Linux hosts

20 The Analysis Architecture is composed of the NetWitness Server, NetWitness User and Entity Behaviour Analytics (UEBA), Archiver, Event Stream Analysis (ESA), Malware Analysis, Automated Threat Detection, Respond, and Reporting Engine, as described below. Unless otherwise stated, each component is deployed on the same appliance as the NetWitness Server.

- Netwitness Server – this interface enables an administrator to perform incident detection, management, investigation, and device and user administration
- NetWitness UEBA – analytical solutions for administrators to discover, investigate, and monitor risky behaviours across all users and entities in the network environment
- Archiver – receives, indexes, and compress log data from Log Decoders
- Event Stream Analysis (ESA) – provides advanced stream analytics such as correlation and event processing
- Malware Analysis – analyses file objects to assess the likelihood the file is malicious
- Automated Threat Detection – applies rule logic across metadata to identify outliers, abnormal behaviour, and malicious activity
- Respond – provides authorised user the ability to group the alerts logically and start an Incident response workflow to investigate and remediate the security issues raised
- Reporting Engine – create rules that govern how data is represented in reports and alerts. The Reporting Engine also manages the alert queue, allowing administrators to enable and disable alerts

21 During the testing activities, the TOE components were deployed in a multi-server configuration, which consists of all components listed above deployed in a combination of physical and virtual environments.

1.8 Delivery Procedures

22 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.

23 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.

1.8.1 TOE Delivery

1.8.1.1 Software Delivery

24 The release engineering group at RSA, located at Reston, VA and Bedford, MA obtain the source code from the development server, located in Bedford, Massachusetts, over a virtual private network (VPN) and creates the master build of the RSA NetWitness components in the Bedford, MA. Once the master build has been created, the release engineers generate an International Organization for Standardization (ISO) image containing the RSA NetWitness component and documentation. Additionally, they generate a second ISO image and a .zip file, both of which contain all of the other RSA NetWitness components and related documentation. Once the images and zip file have been created, the release engineers generate MD5 checksums for each file. The release engineers then transmit all files over Secure File Transfer Protocol (SFTP) to the Gold Master (GM) server located on the production floor in Bedford, Massachusetts. The GM Server is under strict and secure access control. The Operations group, located in Bedford, retrieves the files from the GM server, runs a virus scan of the contents, and verifies them with their checksums. Checksums are located in a separate repository.

25 The Operations team loads the zip file onto the MyRSA site (my.rsa.com) system through a secure SFTP. The myRSA system is located in Bedford, MA and is administered by the Information Technology (IT) group. At this time, the administrators of Download Central (my.rsa.com) are informed of the release. The Quality Engineering group performs all of the steps required for customer distribution, up to and including downloading the zip file from my.rsa.com. The Quality Engineering group then verifies the integrity of the downloaded zip file and confirms it with the Operations group.

26 Once both formats have been verified, the images are moved from the development server to the production server in Bedford, at which point they are available to the customer. The production server is administered by the IT group and access is available to members of the Operations and Manufacturing groups.

27 RSA contracts Unicom Engineering, Incorporated (hereinafter referred to as UNICOM), an ISO-9001-2000 and TL-9000 Quality Management System (QMS)-certified hardware appliance vendor in Canton, Massachusetts, to handle the assembly of the hardware appliance on which portions of the TOE run. Operations group copies the ISO files from the GM to UNICOM using a SFTP transfer. Patches and hot fixes are often released in zip file bundles.

28 Once UNICOM has verified the integrity of the ISO files, it will install the TOE onto a first article appliance. The hardware appliance UNICOM installs the TOE on is composed of parts selected by RSA and integrated by UNICOM. Testing is performed on the hardware appliance and this testing is verified in the first article kit. If RSA changes the hardware appliance the TOE runs on, additional testing will be performed by UNICOM. Quality Engineering personnel go to UNICOM to test, UNICOM then performs the appliance integration and ISO image installation.

1.8.1.2 Hardware Delivery

29 UNICOM handles the TOE packaging. TOE appliances are matched by part number to a Bill of Materials (BOM) that coincides with each shipment. Agile is the change management system used by UNICOM. UNICOM uses a list of part numbers that coincides with RSA's part numbers. These part numbers change when RSA's change, as do the version numbers. When a RSA NetWitness appliance is ordered, the request is passed along to UNICOM by RSA for processing. UNICOM handles the gathering and packing of all required material. UNICOM places a "WARRANTY VOID IF REMOVED" tamper-evident label on the top of the appliance cover. The entire package includes a Dell server containing a pre-installed copy of the TOE, and an accessory box.

30 RSA NetWitness appliances are shipped from UNICOM using either United Parcel Service (UPS) or FedEx to provide delivery.

1.9 Flaw Reporting Procedures

31 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 which would produce a description of each security flaw in terms of its nature and effects.

32 The evaluator examined the flaw remediation procedures and determined that the application of the procedures would identify the status of finding a correction to each security flaw and identify the corrective action for each security flaw.

33 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.

34 The evaluator examined the flaw remediation procedures and determined that it describes procedures for the developer to accept reports of security flaws or requests for corrections to such flaws.

35 The evaluator examined the flaw remediation procedures and determined that the application of the procedures would help to ensure reported flaw is corrected and that TOE users are issued remediation procedures for each security flaw.

36 The evaluators examined the flaw remediation procedures and determined that the application of the procedures would result in safeguards that the potential correction contains no adverse effects.

37 The evaluators examined the flaw remediation guidance and determined that the application of the procedures would result in a means for the TOE user to provide reports of suspected security flaws or requests for corrections to such flaws.

38 Therefore, the evaluator confirms that the information provided meets all requirements for content and presentation of evidence.

2 Evaluation

40 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 Augmented with 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

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

2.1.1 Life-cycle support

42 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 and the TOE references used are consistent.

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

44 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 ALC Life Cycle Support Guidance version 1.7.

2.1.2 Development

Architecture

45 The evaluators examined the security architecture description (contained in [26]) and determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

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

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

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

Functional Specification

49 The evaluators examined the functional specification and determined that:

- The TSF is fully represented;
- It states the purpose of each TSF Interface (TSFI); and
- The method of use for each TSFI is given.

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

- It completely identifies all parameters associated with every TSFI; and
- It completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI.

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

TOE Design Specification

52 The evaluators examined the TOE design (contained in [26]) and determined that the structure of the entire TOE is described in terms of subsystems.

53 The evaluators also determined that all subsystems of the TSF are identified.

54 The evaluators determined that interactions between the subsystems of the TSF were described.

55 The evaluators examined the TOE and determined that each SFR supporting or SFR-non-interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is not SFR-enforcing.

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

57 The evaluators examined the TOE design and determined that it provides a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

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

59 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

60 The evaluators examined the operational user guidance 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.

61 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.

62 The evaluators examined the operational user guidance in conjunction with other evaluation evidences 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.

63 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.

64 The evaluators confirmed that the TOE guidance fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

65 Testing at EAL 2 Augmented with ALC_FLR.1 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by BAE Systems Lab – 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

66 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, 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). The results of the evaluators' tests are consistent with the developers' test results defined in their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

67 At EAL 2 Augmented with ALC_FLR.1, 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.

68 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.

Table 4: Independent Functional Test

TEST ID	DESCRIPTIONS	RESULTS
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.	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	• 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.	
TEST-IND-002	• Verify that the TSF shall display an advisory warning message regarding unauthorised use of the TOE. • Verify that the TSF performs identification and authentication, and other TOE access security functions such as detection of unsuccessful authentication attempts, account lockout, and inactive session termination. • 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.	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	• Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs.	
TEST-IND-003	• 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 provides the ability to analyse IDS data, 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 the role access. • Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs.	Passed. Result as expected.
TEST-IND-004	• 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 provides the ability to analyse behavioural IDS data, configure alarms, display alarm notifications, and protect IDS sensitive NetWitness UEBA User Interface.	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	• Verify that the TSF provides the capability to view IDS data and restricts access to IDS data based on role access. • Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs.	

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

2.1.4.3 Penetration testing

70 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.

71 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack 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 (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

72 The evaluators' search for vulnerabilities also considered public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables. The following public domain sources were searched:

a) www.google.com

b) www.cvedetails.com

c) www.owasp.org

d) https://community.rsa.com/docs/DOC-104202

73 The penetration tests focused on:

a) Network vulnerability scan;

b) Web vulnerability scan;

c) Secure communication;

d) Unrestricted file upload;

e) Input and data validation;

f) Missing function level access control.

74 The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in Section 4 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

75 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all tests conducted were PASSED as expected.

3 Result of the Evaluation

76 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 PLATFORM V11.3 performed by BAE Systems Lab – MySEF.

77 BAE Systems Lab – MySEF found that RSA NETWITNESS PLATFORM V11.3 upholds the claims made in the Security Target (Ref [6]) and supporting documentations and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2 Augmented with ALC_FLR.1.

78 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

79 EAL 2 Augmented with ALC_FLR.1 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and complete interface specifications, guidance documentation and a description of the design of the TOE to understand the security behaviours.

80 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 penetration attackers with a basic attack potential.

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

3.2 Recommendation

82 The Malaysian Certification Body (MyCB) is strongly recommends that:

a) Potential purchasers of the TOE should consider the use of a CA signed certificate, as opposed to a self-signed certificate to fully secure access to the TOE environment.

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

c) Potential purchasers of the TOE should ensure there are appropriate security controls in the TOE operational environment to ensure protection of the network information, logs and its stored data.

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 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] ISCB Product Certification Schemes Policy (Product_SP), v1b, CyberSecurity Malaysia, March 2018.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v1a, March 2018.

[6] RSA NetWitness Platform v11.3 Security Target, Version 1.0, 19 February 2020.

[7] RSA NetWitness Platform v11.3, Evaluation Technical Report, Version 1.0, 6 March 2020.

[8] RSA NetWitness Platform v11.3 Design Documentation, Version 0.9, 30 January 2020

A.2 Terminology

A.2.1 Acronyms

Table 5: List of Acronyms

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

Acronym	Expanded Term
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 6: 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 ---