MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity
MALAYSIA

C125 Certification Report

RSA NetWitness Platform v11.6

File name: ISCB-5-RPT-C125-CR-v1
Version: v1
Date of document: 22 June 2022
Document classification: PUBLIC

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

Best Brand Internet Security 2008 & 2009
CERTIFIED TO ISO/IEC 27001:2013 CERT. NO.: AR 4656
MS ISO/IEC 17025 TESTING SAMM NO. 456 (MySEF LABORATORY)
MSC MALAYSIA Status Company
Best Child Online Protection Website

Securing Our Cyberspace

CyberSecurity Malaysia
(726630-U)
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999

Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C125 Certification Report

RSA NetWitness Platform v11.6

22 June 2022

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:	C125 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C125-CR-v1
ISSUE:	v1
DATE:	22 June 2022
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. 201601006881 (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 29 June 2022, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

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	08 June 2022	All	Initial draft
v1	22 June 2022	All	Final Version

Executive Summary

The Target of Evaluation (TOE) is RSA NetWitness Platform v11.6. 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). The TOE 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 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 MySEF and the evaluation was completed on 18 May 2022.

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 v11.6 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 Target of Evaluation (TOE) is RSA NetWitness Platform v11.6. 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). The TOE provides real-time visibility into the monitored network and long-term network data storage to provide detection, investigation, analysis, forensics, and compliance reporting.

2 NetWitness Capture Architecture collects log data and 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 NetWitness to perform real-time session analysis. NetWitness recognizes over 250 event source types, which are aggregated, analysed, and stored for long-term use. The TOE implements Collection Methods to support collection from the event sources.

3 Data is collected and aggregated by the Decoder and Concentrator appliances. Log Collectors support data collection for use-cases such as importing Legacy Windows log data. The Endpoint Log Hybrid collects host inventories, processes, user activity, and Windows logs from Windows, Mac, or Linux hosts via the NetWitness Insight Agents. The NetWitness Insight Agents are not considered to be part of the evaluated configuration. The Collected data is aggregated into a complete data structure across all network layers, logs, events, and applications. The Event Stream Analysis (ESA) consists of the ESA Correlation (ESA Correlation Rules) service and supports Endpoint and UEBA content.

4 ESA uses Event Processing Language to bring meaning to the event flows. The TOE's user interface uses this aggregated data to provide incident detection, and drill-down investigation. The Archiver appliance is a specialized concentrator or variant that receives, indexes, and compresses logs. The Archiver is adapted to hold indexed and compressed raw log and metadata, and indices for an extended period of time. The Reporting Engine and TOE user interface use the data to provide compliance reporting and in-depth network analysis. Raw packets and packet metadata are not stored in the Archiver.

5 The NetWitness Platform provides functions for Data Privacy Management. The functions provide users with the Data Privacy Officer (DPO) or Administrator role the

ability to manage and protect privacy-sensitive data, without significantly reducing analytical capability. NetWitness Platform can be configured to limit exposure of meta data and raw content (packets and logs) using a combination of techniques. The methods available to protect data in NetWitness Platform include Data Obfuscation, Data Retention Enforcement, and Audit Logging. Data privacy officers and administrators can specify which meta keys in their environment are privacy-sensitive and limit where the meta values and raw data for those keys are displayed in the NetWitness Platform network. In place of the original values, NetWitness Platform can provide obfuscated representations to enable investigation and analytics. In addition, DPOs and administrators can prevent persistence of privacy-sensitive meta values and raw logs or packets. The Audit Logging feature generates audit log entries that are relevant to data privacy.

6 The TOE implements additional security functions such as identification and authentication of TOE users; auditing; security management; and trusted path.

7 The security management functions of the TOE are performed via the NetWitness Platform User Interface (UI), which is a web-based GUI. This interface allows authorized administrators to manage the user accounts, session lockout values and other TSF data, and view the IDS data and alerts. Navigation in the UI is based on Roles and is divided into major functional areas including Respond, Investigate, and Admin. The Respond view consolidates all alerts such as ESA Correlation Rules, Malware Analytics, and Reporting Alerts into one location and is used for incident tracking and triage. The Investigate view presents seven different views into a set of data, allowing authorized users to see metadata, events, and potential indicators of compromise. In the Admin view, Administrators can manage network hosts and services; manage system-level security; and manage Collection Methods/event sources.

8 NetWitness v11.6 includes the following pre-configured, out of the box (OOTB) dashboards; default dashboard, identity dashboard, Operation – Logs dashboard, Operations – Network dashboard, overview dashboard, Threat – indicators dashboard and Threat – Intrusion dashboard.

9 The dashboards consist of dashlets that provide the ability to view the key snapshots of the various components of interest to the user in a single space. In NetWitness Platform, users can compose custom dashboards to obtain high-level information and metrics that portray the overall picture of a NetWitness Platform deployment, displaying only the information that is most relevant to the day-to-day operations.

10 The TOE associates users with administrative roles and maintains the pre-defined roles: Root User, Administrator, Analyst, Operator, SOC_Manager, Respond Administrator, Malware Analyst, UEBA Analysts, and Data Privacy Officer. Note that pre-defined roles are not initially assigned to any user. Note also that though the administrator guidance refers to the roles as: 'Administrators', 'Analysts', 'Operators', 'SOC_Managers', 'UEBA Analysts', and 'Malware Analysts'; the roles identified in this ST are the same roles whether or not the 's' is included at the end.

1.2 TOE Identification

11 The details of the TOE are identified in Table 1: TOE Identification below.

Table 1: TOE Identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C125
TOE Name	RSA NetWitness Platform
TOE Version	v11.6
Security Target Title	RSA NetWitness Platform v11.6 Security Target
Security Target Version	V1.0
Security Target Date	26 May 2022
Assurance Level	Evaluation Assurance Level 2 Augmented 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 ALC_FLR.1
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive, Columbia, Maryland 21046, The United States of America

Developer	NETWITNESS, an RSA Business 10700 Parkridge Bvld, Reston, VA 20191, United States of America
Evaluation Facility	BAE Systems Lab - MySEF Level 28, Menara Binjai, 2 Jalan Binjai 50450 Kuala Lumpur, Malaysia

1.3 Security Policy

12 There is no organisational security policy defined regarding the use of TOE.

1.4 TOE Architecture

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

1.4.1 Logical Boundaries

14 The logical boundary of the TOE is summarized below:

- Security Audit

  The TOE generates audit records of security relevant events that include at least date and time of the event, subject identity and outcome for security events. The TOE provides the default Administrator and Operator roles with the ability to read the audit events. The environment stores the audit records and provides 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 4.1.4 (FIPS 140-2 validation certificate #2300) for both SSH and TLS communications.

The TOE uses the RSA BSAFE Crypto-J cryptographic library: BSAFE SSL-J 6.2.5 for Java applications, which incorporates BSAFE Crypto-J 6.2 (FIPS 140-2 Certificates #2468).

- 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 behaviour (locks the user account for a specified time period).

- 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 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 behavioural anomalies in the UEBA User Interface.

- Security Management

  Authorised 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 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 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

15 The physical boundaries of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

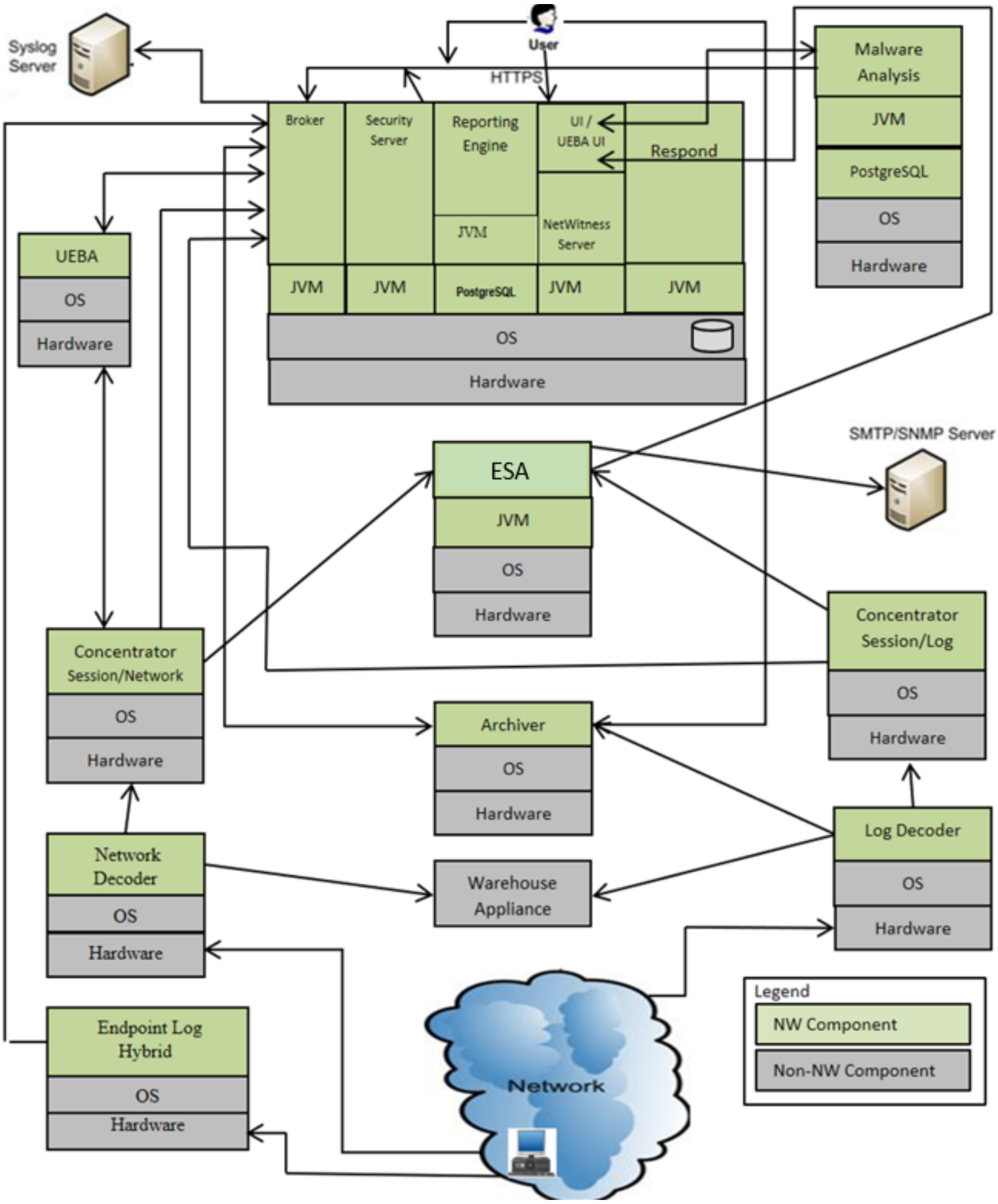


Figure 1 – TOE

16 Included Product Component

Product Component included in the TOE are listed below;

- Windows Legacy Log Collector (zero or more)
  Note: A NetWitness deployment includes at least one Windows Legacy Log Collector
- Decoder (zero or more)
- Log Decoder (zero or more)
  Note: A NetWitness deployment includes at least one Decoder and one Log Decoder.
- Concentrator (zero or more)
- Log Concentrator (zero or more)
  Note: A NetWitness deployment that contains a Log Decoder must include a Log Concentrator. Likewise, a deployment that includes a Decoder for network packets must include a Concentrator for network packets.
- Endpoint Log Hybrid (one or more)
- Broker (zero or more)
  Note: A NetWitness deployment includes at least one Broker.
- Event Stream Analysis (ESA) (zero or more)
  Note: A NetWitness deployment includes at least one ESA.
- Archiver (zero or more)
  Note: A NetWitness deployment includes at least one Archiver.
- NetWitness Server (one or more)
- Respond (zero or more)
  Note: A NetWitness deployment includes at least one Respond.
- Malware Analysis (zero or more)
  Note: A NetWitness deployment includes at least one Malware Analysis.
- 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 Engine 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)

17 Excluded Product Component

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

- Warehouse appliance
- RSA Live (content delivery)
- Malware Community
- Malware Sandbox
- Endpoint Agent

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 appliance management capabilities
- Serial and USB device connections (Used during installation and maintenance only)

18 Services and Products in the Operational Environment

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

- Operating System: provides execution environment for NetWitness components. The OS is CentOS version 7.9 running on a Dell R630, R730xd (Series 5), R640, or R740xd (Series 6).
- Customer provided hardware and Windows operating system for Legacy Windows Log Collector meeting minimum system requirements below:

  a. Windows 2008 R2 SP1 64-Bit, Windows 2012 64-bit, Windows 2016 64-bit
  b. Processor – Intel Xeon CPU @2.0Ghz or faster
  c. Memory – 8GB or faster
  d. Available Disk Space - 320GB
- Hypervisor: provides virtualization for NetWitness virtual appliances. The hypervisor is ESXi version 5.5, 6.0, 6.5, 6.7, or 7.0.

- Administrator Workstation / Browser: provides human users access to NetWitness Server user interface. Compatible browsers that support the required features for NetWitness v11.6 include modern (or current) versions of Google Chrome, Mozilla Firefox, Microsoft Edge 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 that imports logs utilizing various Collection Methods. The Collection Methods supported as part of the baseline are:

  a. Syslog
  b. SNMP Trap
  c. NetFlow
  d. File (pushed by SFTP and FTPS)
  e. Windows (WinRM)
  f. Windows (Legacy)
  g. ODBC
  h. Check Point LEA
  i. VMWare
  j. SDEE
  k. Plugins (Including AWS CloudTrail, GCP, Microsoft Azure, Office 365)
  l. Windows Log Collection and Endpoint Data
  m. Logstash
- The Endpoint Log Hybrid collection methods: Windows, Mac, or Linux hosts for collecting host inventories, processes, user activity, and Windows logs.

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

a. Syslog server: NetWitness Server can forward security audit records and alerts to an external Syslog server.

b. SMTP Server: NetWitness Server can send email messages via SMTP server.

c. SNMP Server: NetWitness Server can send SNMP traps.

d. Authentication Servers: provides external authentication methods (such as Windows Active Director, RADIUS, and LDAP).

1.5 Clarification of Scope

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

21 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]).

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

1.6 Assumptions

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

1.6.1 Operational Environmental assumptions

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

Table 2: Assumptions for the operational environment

Environment	Statement
A.AUDIT_PROTECTION	The operational environment will provide the capability to protect audit information.
A.DATA_SOURCES	The data sources in the environment provide complete and reliable data to the TOE.
A.TIME	The environment will provide reliable time sources for use by the TOE.
A.DEPLOY	TOE Administrators will properly configure the network in the TOE operational environment and configure adequate network capacity for the deployed TOE components.

Environment	Statement
A.PHYSICAL	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	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.TRUSTED_ADMIN	TOE Administrators will follow and apply all administrator guidance in a trusted manner.
A.USER	Users will protect their authentication data.

1.7 Evaluated Configuration

25 This section describes the evaluated configurations of the TOE that are included within the scope of the evaluation.

26 As stated in the ST (Ref. [6]) there are two (2) main components that make up the TOE in its evaluated configuration, which are the Capture Architecture and Analysis Architecture.

27 The Capture Architecture composed of:

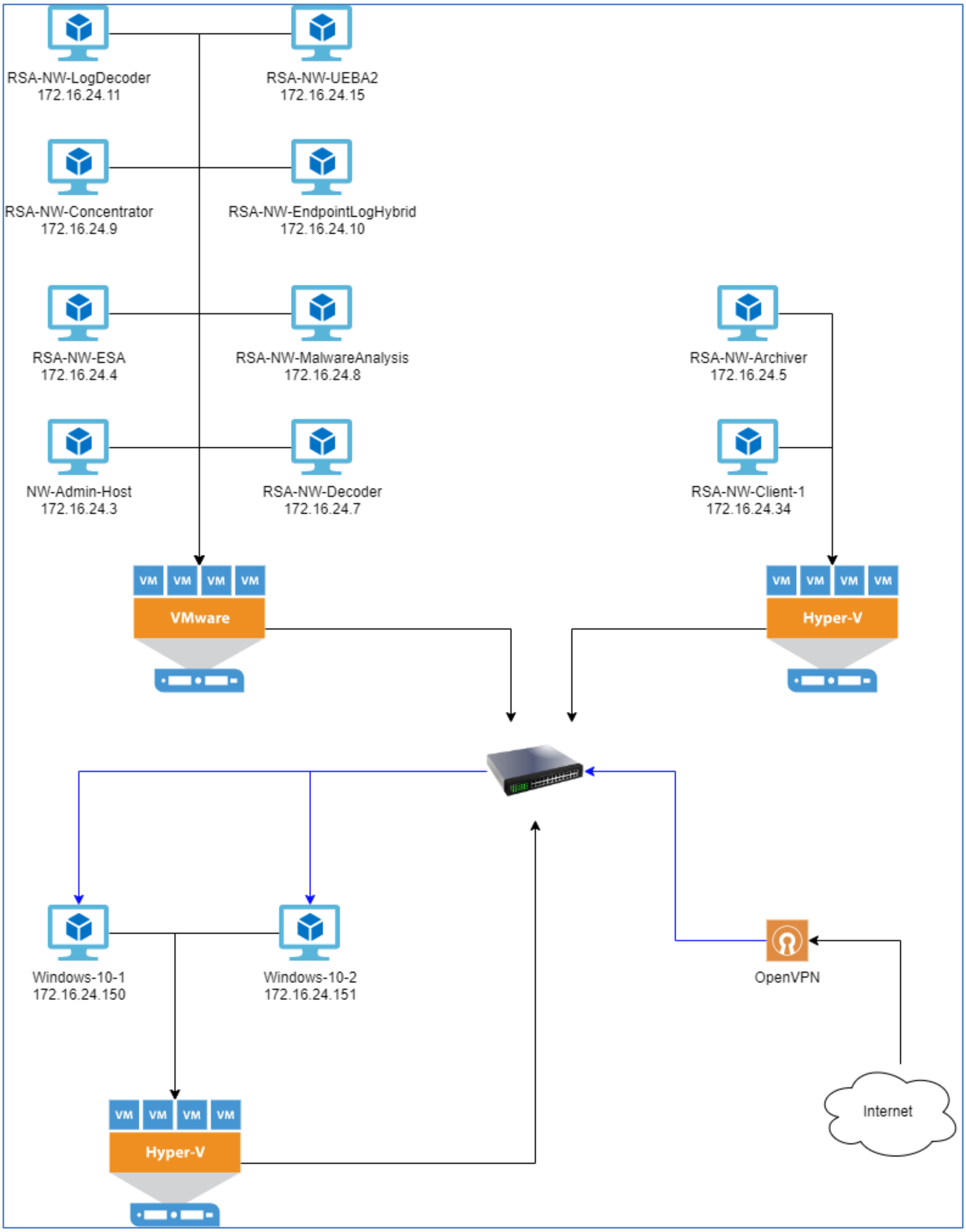
- Decoder – Captures for either packets or logs. When deployed, either the packet or log capture capability is enabled. The term 'Decoder' is used for Decoder (packet) and 'Log Decoder' for Decoder (log). Decoder (packet) can also be depicted as the appliance named "Network Decoder".
- Windows Legacy 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 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.

28 The Analysis Architecture composed of:

- 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 compresses 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.
- Respond - Provides authorised users 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.

29 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.



30

Figure 2 – Test environment components

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 evaluators also examined the aspects of the delivery process and determined that the delivery procedures are used.

1.8.1 TOE Delivery Procedures

33 Several procedures are necessary to maintain security of the TOE during distribution including the procedures that being followed during the production, packaging, and release of the TOE.

34 Pre-Delivery Activities

The release engineering group at RSA, located at the Reston, VA and Bedford, MA obtains 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[1] 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.

The Operations team loads the zip file onto the my rsa 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

[1] An ISO image is a duplicate of an optical disk such as a Compact Disc (CD) that can be used to directly replicate it.

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.

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.

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.

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.

In order to purchase the TOE, customers must contact a sales representative located in several territories across the United States where each location is capable of handling order requests. Orders may be placed via email, phone, or fax. The sales representatives pass orders to the Customer Order Management (COM) group in Bedford or Shannon, Ireland, for entry into the Systems, Applications and Products in Data Processing (SAP) Enterprise Resource Planning (ERP) system. The COM group then handles the processing and fulfillment of the order. Once an order has been placed, only members of the COM department have access to it.

Customers have 24-hour a day access to RSA Link, an online e-support center. RSA Link provides web support, including on-line case management and an extensive knowledge base. RSA Link also makes it easy for customers to locate technical support solutions, download current patches and hotfixes, and access complete online documentation.

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

S4 & S5 are legacy versions that can be updated to the current TOE configuration. S6E is current shipping version. The TOE can be delivered on All but one of the RSA NetWitness® Platform Series 6E (S6E) physical hosts are based on the Dell PowerEdge R640 chassis or the exception is the Hybrid host, which is based on the Dell PowerEdge R740xd chassis. The Series 6E physical hosts are shipped with NetWitness Platform software installed.

The accessory box contains:

- RSA NetWitness® Platform Series 6E Appliance
- Static Ready Rails 2U (1 set)
- Left Rail 2U Adapter for EMC deep rack (1)
- 2U RSA Bezel (1) - Keys are taped to the bezel
- Power Cord (2)
- Short Range (SR) SFP Optical Transceivers (2)
- Safety Environment and Regulatory Information booklet (1)
- RSA Documentation Folder (1)
- RSA EULA (1)

The entire package is places in a cardboard box bearing the logo of RSA and lined with form-fitting foam inserts. The box is then fixed with two product labels which contain the product name, part number and current version.

35 Shipping Process

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

The myRSA system makes the zip file available over a secure internet connection to customers who have purchased the TOE. Two email notifications are sent. The first email contains the login credentials and Universal Resource Locator (URL) for the myRSA server. The second email contains the serial number/license number information for the product. The emails are generated from different servers. After the initial purchase, customers are notified of product updates by RSA through email.

2 Evaluation

36 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 MyCC Scheme Requirement (MyCC_REQ) (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:

2.1.1 Life-cycle support

38 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

39 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Flaw Reporting Procedures

40 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.

41 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.

42 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.

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

44 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.

2.1.3 Development

45 The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).

46 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

47 The evaluators examined the TOE security architecture description; they 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.

48 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.4 Guidance documents

49 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

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

2.1.5 IT Product Testing

51 Testing at EAL 2 Augmented ALC_FLR.1 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by BAE Systems - MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.5.1 Assessment of Developer Tests

52 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.

2.1.5.2 Independent Functional Testing

53 At EAL 2 Augmented 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.

54 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 3: Independent Functional Test

Test ID	Description	Security Function	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. • Verify that the TSF shall maintain security roles. • Verify that the TSF data is protected from disclosure or modification when it is transmitted between separate parts of the TOE, and all communication between the TOE and other trusted IT products/remote users are initiated via trusted path/channels. • Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs.	FAU_GEN.1.1 FAU_GEN.1.2 FAU_GEN.2.1 FAU_SAR.1.1(1) FAU_SAR.1.2(1) FAU_SAR.1.1(2) FAU_SAR.1.2(2) FAU_SAR.2.1 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) 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	Passed.
TEST-IND-002	• Verify that the TSF shall display an advisory warning message regarding unauthorised use of the TOE.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FAU_SAR.1.1(2), FAU_SAR.1.2(2), FAU_SAR.2.1, FAU_STG.1.1, FAU_STG.1.2, FIA_AFL.1.1,	Passed.

Test ID	Description	Security Function	Results
	• 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. • Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs.	FIA_AFL.1.2, FIA_ATD.1.1, FIA_UAU.1.1, FIA_UAU.1.2, FIA_UID.1.1, FIA_UID.1.2, FTA_SSL.3.1, FTA_SSL.4.1, FTA_TAB.1.1	
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.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FAU_SAR.1.1(2), FAU_SAR.1.2(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.1.2(1) IDS_RDR_EXT.1.3(1) IDS_RDR_EXT.1.1(2)	Passed.

Test ID	Description	Security Function	Results

	• Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs.	IDS_RDR_EXT.1.2(2)
		IDS_RDR_EXT.1.3(2)
		IDS_RDR_EXT.1.1(3)
		IDS_RDR_EXT.1.2(3)
		IDS_RDR_EXT.1.3(3)
		FMT_MOF.1.1(2)
		FMT_MTD.1.1
		FMT_SMF.1.1	

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. • 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.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FAU_SAR.1.1(2), FAU_SAR.1.2(2), FIA_UAU.5.1, FIA_UAU.5.2, IDS_ANL_EXT.1.1, IDS_ANL_EXT.1.2, IDS_RCT_EXT.1.1, IDS_RDR_EXT.1.1(4) IDS_RDR_EXT.1.2(4) IDS_RDR_EXT.1.3(4) FMT_MOF.1.1(3), FMT_MTD.1.1, FMT_SMF.1.1, FMT_SMR.1.1, FMT_SMR.1.2	Passed.

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

2.1.5.3 Vulnerability Analysis

56 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.

57 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 equipment required for exploitation

2.1.5.4 Vulnerability testing

58 The penetration tests focused on:

a) Network Vulnerability Scan

b) Web Vulnerability Scan

c) Input Data Validation

d) Missing Function Level Access Control

e) Secure Communications

f) Unrestricted File Upload

g) SSH Audit

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

2.1.5.5 Testing Results

60 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 the test conducted were PASSED as expected.

3 Result of the Evaluation

61 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 v11.6 which is performed by BAE System Lab - MySEF.

62 BAE System Lab - MySEF found that RSA NetWitness Platform v11.6 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 ALC_FLR.1.

63 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

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

65 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.

66 EAL 2 Augmented ALC_FLR.1 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

67 The Malaysian Certification Body (MyCB) is strongly recommended 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 database 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] MyCC Scheme Requirement (MYCC_REQ), v1, CyberSecurity Malaysia, December 2019.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v2a, August 2020.

[6] RSA NetWitness Platform v11.6 Security Target, Version 1.0, 26 May 2022.

[7] Evaluation Technical Report, Version 1.0, 01 June 2022.

A.2 Terminology

A.2.1 Acronyms

Table 4: 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

Acronym	Expanded Term
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 5: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65

Term	Definition and Source
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---