MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity
MALAYSIA

M015 Maintenance Report

File name: ISCB-5-RPT-M015-AMR-v1
Version: v1
Date of document: 13 January 2021
Document classification: PUBLIC

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

M015 Maintenance Report

13 January 2021

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:	M015 Maintenance Report
DOCUMENT REFERENCE:	ISCB-5-RPT-M015-AMR-v1
ISSUE:	v1
DATE:	13 January 2021
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

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
D1	06 January 2021	All	Initial draft
V1	13 January 2021	All	Final Release

Table of Contents

1 Introduction

1 The TOE is RSA NetWitness Platform v11.4 (or collectively as “NetWitness”), 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. 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 Open Systems Interconnection (OSI) model. This data allows NetWitness to perform real-time session analysis. NetWitness recognizes over 250 event source types, which are aggregated, analyzed, and stored for long-term use. The TOE implements Collection Methods to support collection from the event sources

2 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) can run two ESA services on the ESA host:

- ESA Correlation (ESA Correlation Rules) supports Endpoint and User and Entity Behavior Analysis (UEBA) content.
- Event Stream Analytics Server (ESA Analytics) uses this data to provide advanced stream analytics such as correlation and complex event processing at high throughputs and low latency.

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

Table 1 – Identification Information

Assurance Maintenance Identifier	M015
Project Identifier	C108
Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Impact Analysis Report	Impact Analysis Report RSA NetWitness Platform V11.4
New TOE	RSA NetWitness Platform v11.4
Certified TOE	RSA NetWitness Platform v11.3
New Security Target	RSA NetWitness Platform v11.4 Security Target Version 1.0, 09 December 2020

Evaluation Level	EAL2+ALC_FLR.1
Evaluation Technical Report (ETR)	RSA NetWitness Platform v11.3, Evaluation Technical Report, Version 1.0, 6 March 2020 (GOXX2223-S050-ETR 1.0, 6 March 2020)
Criteria	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, April 2017, Version 3.1, Revision 5 Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, April 2017, Version 3.1, Revision 5 Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, April 2017, Version 3.1, Revision 5
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, April 2017, Version 3.1 Revision 5
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL2 Augmented (ALC_FLR.1)
Protection Profile Conformance	None
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive Columbia, MD 21046, United States of America
Developer	RSA 10700 Parkridge Blvd, Reston, VA 20191, United States of America
Evaluation Facility	BAE Systems Lab - MySEF

2 Description of Changes

4 RSA has issued a new release of the RSA NetWitness Platform v11.4. There were a series of minor updates to the RSA NetWitness Platform since its certification version 11.3 on 3 April 2020.

2.1 Changes to the product associated with the certified TOE

5 The following features have been added in RSA NetWitness Platform version 11.4, 11.4.0.1, 11.4.1.0 and 11.4.1.1 as below:

Table 2 – General changes/additions

Version	Description of Changes	Rationale	Impact
RSA NetWitness Platform v11.4	**Investigation - Security Information & Event Management (SIEM) and network traffic analysis** • Streamlined workflow to analyse Events • Text search filter in a Query • Auto-suggestion of meta values while constructing a Query • Query profiles in the Events View • Custom column groups in the Events View • Sort results in the Events List • Use recent queries to help with query construction in the Events View • Find and highlight text in the Events List • Shorthand notations, numerical ranges, and parentheses while constructing complex queries in Guided Mode • Download PCAPs, metadata, and logs in the Events view • Event Meta panel layout • Query Auto-Complete indicates meta key index level • Create and edit Incidents from Investigate **NetWitness User and Entity Behavior Analytics** • Advanced Analytics using network data • Filtering entities to Investigate • Trending data support • Quick Sorting Options • Improved pivoting option from UEBA to Events	The updates do not affect the Security Functional Requirements of the TOE, as it is been reflected to be out-of-scope.	CB consider it as **Minor**

	Incident Response • Nodal graph improvements • Alert Search improvements • Incident Search improvements • Improvements to respond email notifications • Export and import Incident rules • Enable or disable multiple incident rules at the same time • Access to Incidents can be restricted **Health and Wellness (BETA)** • The Health and Wellness (BETA) feature is an advanced, robust, and a simplified solution for hosts and services monitoring, such as performance or resource utilisation. Health and Wellness provides great visualisations and allows user to easily alert or notify anomalies on critical hosts and services in a large NetWitness deployment. For 11.4, users can only deploy Health and Wellness Search (BETA) on a dedicated, virtual host. **Endpoint Investigation** • Isolate infected hosts from network • Advanced forensic investigation • Usability enhancements for process analysis • Usability enhancements for host aggregation • Support of additional REST APIs • Filters in host details • Support for automatic file download **Endpoint Configuration** • Endpoint Agent log file collection • Support for new operating system versions in Endpoint Agent • In addition to the operating system versions supported in 11.3, the agent now supports the following operating systems: – macOS 10.15 Catalina – CentOS 8.x – Red Hat Enterprise Linux 8.x – Windows 10 version 1909		

	Broker, Concentrator, Decoder and Log Decoder Services • Berkeley Packet Filters (BPF) supported for 10g environments • IPv4 Index CIDR range optimisation – Core Database indexes for IPv4 data types automatically index CIDR Ranges for the common /8, /16, and /24 subnet sizes. Query operations that search for these types of CIDR ranges are now significantly faster. • Gain visibility into HTTP/2 Sessions – User can search for metadata items derived from headers in the HTTP/2 stream to gain visibility into HTTP/2 sessions. **Event Stream Analysis (ESA)** • Added the ability to remove sensitive meta keys from all Alert output for data privacy – For data privacy reasons, users can now remove some sensitive meta keys from all alert output globally, regardless of the data source. In the ESA Correlation service, the user can add sensitive meta keys to the global-private-fields parameter, which removes them from the output of all alerts. • Esper version upgraded from version 7.1.0 to 8.2.0 – In NetWitness Platform version 11.4, ESA Correlation supports Esper version 8.2.0. **Log Collection** • Export of Syslog RFC-5424 logs imported from the NetWitness Platform user interface • Log stats performance improvements **Administration and Configuration** • Single Sign-On authentication – For Admins to streamline authentication for NetWitness Platform, Single Sign-On is supported. NetWitness Platform supports Active Directory Federation Services (ADFS) as an Identity Provider (IDP) and uses		

	SAML 2.0 as the protocol for single sign-on. • Configure menu improvements • Multiple NW-Server support for distributed Analyst User Interface (UI) – User can now deploy multiple NetWitness Platform UI instances for analyst purposes. These Analyst UI instances can be deployed to span across multiple Geographic locations. The feature helps reduce latency and improve performance as compared to accessing all functionality from the Primary UI on the NW Server Host. • Capability to provide silent NetWitness installation • New retention optimised Log Hybrid option • Capability to deploy the NW Server on Series 6 Analytics Hardware (Formerly ESA Physical Host) as an option • Install Endpoint server on existing Log Decoder host **Upgrade Improvements** • Respond service normalisation scripts are automatically backed up before being refreshed after an upgrade		
Version	**Description of Changes**	**Rationale**	**Impact**
RSA NetWitness Platform v14.0.1	**Reporting Engine** • Output action for blank reports : NetWitness Platform provides the analyst with the ability to exclude blank reports while processing the output actions. Users can configure this setting in the Reporting Engine service configuration view using Enable Output Actions for Reports with No Results option.	The updates do not affect the Security Functional Requirements of the TOE, as it is been reflected to be out-of-scope.	CB consider it as **Minor**

Version	Description of Changes	Rationale	Impact
RSA NetWitness Platform v11.4.1.0 - v11.4.1.1	**Customer Experience Improvement Program** • The RSA NetWitness Platform Customer Experience Improvement Program (CEIP) is an initiative to continuously improve RSA NetWitness Platform. When a customer enables this program, the CEIP performs analytics about how individual users work in RSA NetWitness Platform without interrupting their workflow or personally identifying users. As part of this program, RSA gains insights on the user deployment and license usage and analytics on pages viewed and actions taken. RSA uses these analytics when making decisions about new features and enhancements to prioritise in upcoming releases. **Investigation** • Enhanced performance for faster Event Investigation • Improved email reconstruction in the Events View • Intra-session and related Events grouping in the Events View • Faster and easier query building in the Events View • New ability to view unsorted Events List in the Events View • Better Column sorting controls **Decoder, Log Decoder, and Log Collector Services** • Configure custom certificates on Log Decoders • Configure custom certificates on Log Collectors • Search for Event Sources using address (IP/Hostname) or name on Log Collectors • Metadata generated with SHA-256 fingerprints of SSL/TLS certificate – The Network Decoder can generate metadata with SHA-256 fingerprints of the SSL/TLS certificate (in addition to SHA-1 hash format) that are available for investigations and analytics.	The updates do not affect the Security Functional Requirements of the TOE, as it is been reflected to be out-of-scope.	CB consider it as **Minor**

	Administration • Event Source historical graphs moved from Health & Wellness to Event Source Management – All event source information, except Historical Graphs, was previously moved from the Health & Wellness view to the Event Sources Manage view. In 11.4.1, the graphs have been moved. Previously, these graphs were accessed in the Event Source Monitoring tab of the Admin > Health & Wellness view. Now, they are available in the Manage tab of the Admin > Event Sources view. • SSO Authentication is Supported for Analyst UI deployments • Single Sign-On (SSO) is supported for analysts in a multiple NetWitness Platform User Interface instances deployment. • Simplified management of the deploy_admin account – The deploy_admin account is a password-based system account that is used on every NetWitness Platform host, and must be kept synchronised between all hosts. It can require periodic updating depending on the deployment environment policies. Starting with 11.4.1, the deploy_admin password is centrally managed with the nw-manage script on the NW Server. The nw-manage script execution updates the password on all NetWitness Platform component hosts that use the deploy_admin account. • Change the IP Address of the warm standby NW Server **Integration** • Support to forward high-risk usernames to RSA SecurID Access		

	– With the NetWitness Platform Integration with RSA SecurID Access, the NetWitness Respond server can now also send the Active Directory username of high-risk users from incidents to RSA SecurID Access. **ESA (Event Stream Analysis)** • ESA Rule deployment troubleshooting metrics are available through Nw-Shell – Users can use Nw-Shell to view ESA Correlation Server metrics for each of users’ ESA rule deployments. These metrics show the number of sessions behind for the deployment data sources as well as the memory usage for the rules in the deployment.		

2.2 Changes to the SFRs claimed in the ST

6 The changes that have been made is not affecting Security Functional Requirements (SFRs) in the ST (Ref [2]).

3 Affected Developer Evidence

7 The affected developer evidences submitted for the assurance continuity required by the CCRA Assurance Continuity: CCRA Requirements Version 2.1 (2012-06-01) June 2012 (Ref [18]) are as below:

Table 3 – Affected Developer Evidence

Evidence	Description of Changes	Rationale	Impact
RSA NetWitness Platform v11.4 Security Target Version 1.0, 09 December 2020	• The ST version and document date have been updated. • TOE reference has been updated to reflect the change in TOE new version 11.4 from the developer. • Section 2.2.2.3 – Services and Products in the Operational Environment has been updated to include the latest Operating System support for CentOS version 7.7.1908. • Section 2.3 - TOE documentation has been updated to include the latest versions of administration and configuration guides for the RSA NetWitness Platform v11.4. • Section 6.4 - 6.4 Security Monitoring with Security Information and Event Management has been updated to describe the NetWitness User and Entity Behavior Analytics (UEBA) prioritises the potential risk from a user or network entity by using a simplified additive scoring formula. Each alert is assigned a severity that increases a user or network entity's score by a predefined number of points.	The changes/ update that have been made is not affecting to the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
RSA NetWitness Platform v11.4 Design Documentation Version 0.3, 15 September 2020	• The Design Documentation version and date have been updated. • TOE reference has been updated to reflect the change in TOE version 11.4 from the developer. • The TOE documentation has been updated to include the latest versions of administration	The changes/ update that have been made is not affecting to the SFRs or functionality that was included in	CB consider it as **Minor**

Evidence	Description of Changes	Rationale	Impact
	and configuration guides for the RSA NetWitness Platform v11.4 throughout the Design Documentation. • Section 2.5 – Services Provided by Operational Environment has been updated to include the latest Operating System support for CentOS version 7.7.1908. • Section 5 – References has been updated to include the latest references for TOE administration and configuration guides.	the scope of the previous evaluation.	
RSA NetWitness Platform Common Criteria ALC Life Cycle Support Guidance, Version 1.2, 09 December 2020	• The Life Cycle Documentation version and date have been updated. • Section 2.2 – List of Product components have been updated to include the latest components of the TOE. • Section 2.2.1 – Table 2 have been updated to include the latest TOE naming conventions. • Section 2.4 – Source Control have been updated to include the latest example for the TOE's ISO File Name. • Section 3.1.1 – Configuration List has been updated to include the latest iteration of TOE Components and SAR Evidence with their respective Version Number. • Section 4.2.2 – Pre-Delivery Activities have been updated to include the updated list of items in the TOE's delivery package. • Section 5.2 Flaw Remediation Procedures has been updated to describe new email addresses and web pages for flaw remediation process, as well as RSA NetWitness Engineering replacing the Product Security Response Center (PSRC) as the	The changes/ update that have been made is not affecting to the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**

Evidence	Description of Changes	Rationale	Impact
	tracker for the TOE's security flaws.		
RSA NetWitness Platform v11.4 Product Verification Checklist, 2020	• The title page of the Product Verification Checklist has been updated to reflect on the new TOE version, which is RSA NetWitness Platform v11.4. • The OVA and ISO file details have been updated to reflect the new TOE version 11.4.0.0.14000. • The MD5 hash checksum for the OVA file has been updated to reflect the new hash number for the TOE version 11.4.0.0.14000.	The changes/ update that have been made is not affecting to the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
RSA NetWitness Platform v11.4 Physical Host Installation Guide, May 2020	• The document product version and date have been updated. • Appendix A has been updated to reflect the Silent Installation option that enables administrator to automate the installation of a host by supplying responses to the scripts' prompts through the command line.	The changes/ update that have been made is not affecting to the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
RSA NetWitness Platform v11.4 Deployment Guide, July 2020	• The document product version and date have been updated. • Health and Wellness (BETA for Standalone Virtual Host Only) section has been added describing the installation and deployment as well as configuration of the service. • Deployment Optional Setup Procedures has been updated to reflect the Analyst UI service features and limitations, as well as methods of configuration and deployment for multiple NW (NetWitness) servers.	The changes/ update that have been made is not affecting to the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
RSA NetWitness Platform v11.4 System Security and	• The document product version and date have been updated. • Set Up Single Sign-On Authentication (SSO) section has been added describing	The changes/ update that have been made is not affecting to	CB consider it as **Minor**

Evidence	Description of Changes	Rationale	Impact
User Management Guide, April 2020	configuration, creation of public key authentication and workflow of enabling SSO on RSA NetWitness Platform. • Troubleshooting section has also been updated to include steps to disable SSO manually. • Configure PAM (Pluggable Authentication Module) Login Capability section has been updated to include the use of SecurID accounts configuration and troubleshooting.	the SFRs or functionality that was included in the scope of the previous evaluation.	
RSA NetWitness Platform v11.4 Getting Started Guide, August 2020	• The document product version and date have been updated. • NetWitness Platform Basic Navigation section has been updated to include changes in the menu such as a more streamlined workflow, various fix and upgrade to the user interface (UI) as well as the configuring the UI according to the preferences of the user.	The changes/ update that have been made is not affecting to the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
RSA NetWitness Platform v11.4 UEBA User Guide, May 2020	• The document product version and date have been updated. • Access NetWitness UEBA section has been updated to include option to pivot EUBA to events • How NetWitness UEBA Works section has been updated to mention that UEBA can be used to retrieve logs from a new source, Network Data and usage of advanced analytics. • Investigate High-Risk User or Network Entity section has been updated to include trending data score and quick sort option.	The changes/ update that have been made is not affecting to the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
RSA NetWitness Platform v11.4 Investigate User Guide,	• The document product version and date have been updated. • 11.4 Query Builder and the KeyWord Text Search section has been updated to include the examples and usage of IPv4	The changes/ update that have been made is not affecting to the SFRs or	CB consider it as **Minor**

Evidence	Description of Changes	Rationale	Impact
April 2020	CIDR ranges notation to filter the IP addresses.	functionality that was included in the scope of the previous evaluation.	
System Maintenance: Manage the Deploy_Admin Account Online Document, 18 November 2020 (https://community.rsa.com/docs/DOC-114096)	• The document date have been updated. • The document has been created to include changes made to the deploy_admin account, which now can be used to synchronise with all NetWitness components. • The document also included steps to change the password for deploy_admin, as well as changing the deploy_admin account password for a component host that is unavailable.	The changes/ update that have been made is not affecting to the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
RSA NetWitness v11.4 System Configuration Guide, April 2020	• The document product version and date have been updated. • Customer Experience Improvement Program section has been added to describe the aim of the program, and configuration to either participate or decline on the program.	The changes/ update that have been made is not affecting to the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**

4 Result of Analysis

8 The outcome of the review found that none of the modifications significantly affects the security mechanisms that implement the functional requirements of the Security Target (Ref [3]), as required in accordance of Assurance Continuity: CCRA Requirements version 2.1 (2012-06-01) June 2012 (Ref [18]).

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

5 Recommendation

10 Based on the findings from the Impact Analysis Report (IAR) v1.1 submitted by developer, this IAR version maintenance for RSA NetWitness Platform v11.4 does not cover the RSA NetWitness Platform (the TOE) v11.4.2 onwards.

Annex A References

[1] RSA NetWitness Platform version 11.4 Impact Analysis Report (IAR), EAU000912-IAR, Version 1.1, 6 January 2021

[2] RSA NetWitness Platform Security Target, Version 1.0, 19 February 2020 – Version 11.3

[3] RSA NetWitness Platform Security Target, Version 1.0, 09 December 2020 – Version 11.4

[4] RSA NetWitness Platform v11.4 Design Documentation, Version 1.2, 09 December 2020

[5] Product Verification Checklist for RSA NetWitness Platform v11.4, 2020

[6] Deployment Guide for RSA NetWitness Platform v11.4, July 2020

[7] NetWitness Investigate User Guide for RSA NetWitness Platform v11.4, April 2020

[8] Physical Host Installation Guide for RSA NetWitness Platform v11.4, May 2020

[9] Getting Started Guide for RSA NetWitness Platform v11.4, August 2020

[10] Systems Security and User Management Guide for RSA NetWitness Platform v11.4, April 2020

[11] NetWitness UEBA User Guide for RSA NetWitness Platform v11.4, May 2020

[12] RSA NetWitness Platform v11.4 Systems Configuration Guide, April 2020

[13] System Maintenance : Manage the deploy_admin Account Online Documentation, 18 November 2020

[14] Release Notes for RSA NetWitness Platform 11.4, February 2020

[15] Release Notes for RSA NetWitness Platform 11.4.0.1, May 2020

[16] Release Notes for RSA NetWitness Platform 11.4.1.0, April 2020

[17] Release Notes for RSA NetWitness Platform 11.4.1.1, May 2020

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

[19] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2014.

[20] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

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

[22] MyCC Scheme Requirement (MyCC_REQ), v1, December 2019.

[23] ISCB Evaluation Facility Manual (ISCB_EFM), v2, December 2019.

[24] RSA NetWitness Platform v11.3, Evaluation Technical Report, Version 1.0, (GOXX2223-S050-ETR 1.0, 6 March 2020)

--- END OF DOCUMENT ---