MINISTRY OF
COMMMUNICATIONS AND DIGITAL

CyberSecurity
MALAYSIA

M018 Maintenance Report

File name: ISCB-5-RPT-M018-AMR-v1
Version: v1
Date of document: 30 January 2023
Document classification: PUBLIC

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

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

M018 Maintenance Report

30 January 2023

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:	M018 Maintenance Report
DOCUMENT REFERENCE:	ISCB-5-RPT-M018-AMR-v1
ISSUE:	v1
DATE:	30 January 2023
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

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	17 January 2023	All	Initial draft
v1	30 January 2023	All	Final version

Table of Contents

1 Introduction

1 The TOE is the LogRhythm Integrated Solution v7.8 with Microsoft SQL Server 2016 SP1 Standard Edition software. The TOE is a fully integrated Security Information and Event Management (SIEM) solution that collects, categorizes, identifies, and normalizes log data from log sources such as Windows events, syslog, flat file, NetFlow, sFlow, databases, and applications, and provides automated alerting capabilities. The TOE can detect security and compliance issues, such as anomalies in authentication activity, and brute force attacks on monitored servers.

2 The TOE provides automated centralization of log collection, archival and recovery, automated reporting, forensic investigation abilities, anomaly and insider threat detection, turnkey appliance configuration, and a console management interface.

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 the TOE as in Table 1 identification below.

Table 1 – Identification Information

Assurance Maintenance Identifier	M018
Project Identifier	C074
Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Impact Analysis Report	LogRhythm Integrated Solution v7.8.0 with Microsoft SQL Server 2016 SP1 Standard Edition Impact Analysis Report
New TOE	LogRhythm Integrated Solution v7.8.0 with Microsoft SQL Server 2016 SP1 Standard Edition
Certified TOE	LogRhythm Integrated Solution v7.3 with Microsoft SQL Server 2016 SP1 Standard Edition
New Security Target	LogRhythm Integrated Solution v7.8 with Microsoft SQL Server 2016 SP1 Standard Edition, Version 1.0, 13 May 2022
Evaluation Level	EAL2 Augmented (ALC_FLR.2)
Evaluation Technical Report (ETR)	Evaluation Technical Report V0.2, 11 February 2019 (EAU000631.01-S034-ETR)
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 Assurance Continuity: CCRA Requirements version 2.1, June 2012
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.2)
Protection Profile Conformance	None
Sponsor	LogRhythm Incorporated 4780 Pearl East Circle, Boulder, Colorado 80301 USA.
Developer	LogRhythm Incorporated 4780 Pearl East Circle, Boulder, Colorado 80301 USA

2 Description of Changes

4 LogRhythm Inc. has issued a new release of the LogRhythm Integrated Solution v7.8 with Microsoft SQL Server 2016 SP1 Standard Edition since its re-certification version 7.3 on April 2019.

2.1 Changes to the SFRs claimed in the ST

5 The changes that have been made do not affect the Security Functional Requirements (SFRs) in the ST (Ref [2]). The lists of changes have been documented in the Impact Analysis Report (IAR) (Ref [2]).

Table 2 – SFR Mapping

SFR	Changes (Yes/No)	Description of Changes	Impact	Rationale
FAU_GEN.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FAU_SAR.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FAU_SAR.2	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FAU_SAR.3	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FAU_SEL.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FAU_STG.2	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FAU_STG.4	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.

SFR	Changes (Yes/No)	Description of Changes	Impact	Rationale
FIA_UAU.2	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FIA_ATD.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FIA_UID.2	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FMT_MOF.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FMT_MTD.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FMT_SMF.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FMT_SMR.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FPT_ITT.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
SEM_ANL_EXT.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
SEM_RCT_EXT.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
SEM_RDR_EXT.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
SEM_STG_EXT.1(1)	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.

SFR	Changes (Yes/No)	Description of Changes	Impact	Rationale
SEM_STG_EXT.1(2)	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
SEM_STG_EXT.1(3)	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
SEM_STG_EXT.2(1)	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
SEM_STG_EXT.2(2)	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
SEM_STG_EXT.2(3)	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
SEM_LDC_EXT.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.

3 Affected Developer Evidence

6 The affected developer evidence submitted for the assurance continuity required by the CCRA Assurance Continuity: CCRA Requirements Version 2.1 (2012-06-01) June 2012 (Ref [4]) are as below:

Table 3 – Affected Developer Evidence

Evidence Identification	Description of Changes	Rationale	Impact
Security Target: LogRhythm Integrated Solution v7.3 with Microsoft SQL Server 2016 SP1 Standard Edition, Version 0.93, 16 Jan 2019	**Maintained Security Target:** LogRhythm Integrated Solution v7.8 with Microsoft SQL Server 2016 SP1 Standard Edition Security Target, Version 1.0, 30 Apr 2022 Changes in the maintained ST are: • Section 1.1 - Updated identification of ST • Section 1.1 - Updated TOE software version • Section 2 – product version number • Section 2.2.1.1 – product version number • Section 2.2.3 - excluded functionality • Section 2.3 – Updated list of TOE documentation for updated guides	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
Guidance: LogRhythm Client Console Reference Guide, Version 7.3.3, March 21, 2018	**Maintained Guidance:** LogRhythm Enterprise SIEM, September 14, 2021 (LogRhythm NextGen-SIEM-7.8.0-Help RevA.pdf) The content of the Client Console Reference Guide has been included in the Enterprise SIEM document. Some material has been rearranged to support on-line display in a web browser.	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
Guidance:	**Maintained Guidance:**	The changes/ update that have been	CB consider

Evidence Identification	Description of Changes	Rationale	Impact
LogRhythm 7.3 Reference Card	This document was specific to LogRhythm 7.3 and is not included in documentation for LogRhythm 7.8.	made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	it as **Minor**
Guidance: LogRhythm Compatibility and System Monitor Functionality Guide, Version 7.3.3, Rev B	**Maintained Guidance:** LogRhythm System Monitor, May 04, 2022 (LogRhythm-System-Monitor-7.8.0.8012-RevA) Document updated to include details of System Monitor 7.8. Some material has been rearranged to support on-line display in a web browser.	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
Guidance: LogRhythm Release Notes Version 7.3.3, March 21, 2018	**Maintained Guidance:** LogRhythm / Enterprise SIEM / LogRhythm Release Notes / 7.8.0 GA Release Notes (https://docs.logrhythm.com/docs/enterprise/logrhythm-release-notes/7-8-0-ga-release-notes)	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
Guidance: LogRhythm Software Installation Guide, Version 7.3.3, March 21, 2018	**Maintained Guidance:** LogRhythm Install a New LogRhythm Deployment, August 9, 2021 (LogRhythm-Software-Install-Guide-7.8.0-RevA.pdf).	The changes/ update that have been made is not affecting the SFRs or functionality that was included in	CB consider it as **Minor**

Evidence Identification	Description of Changes	Rationale	Impact
	Document updated for updated version of LogRhythm. Some material has been rearranged to support on-line display in a web browser.	the scope of the previous evaluation.	
Guidance: LogRhythm Software Upgrade Guide 6.3.x to 7.3.3, Version 7.3.3, March 21, 2018	**Maintained Guidance:** This document was specific to LogRhythm 7.3.3 and is not included in documentation for LogRhythm 7.8.	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
Guidance: LogRhythm Web Console User Guide, Version 7.3.3, March 21, 2018	**Maintained Guidance:** LogRhythm Web Console User Guide, September 13, 2021 (LogRhythm-Web-Console-User Guide-7.8.0-RevA.pdf) Document updated for updated version of LogRhythm. Some material has been rearranged to support on-line display in a web browser.	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
Guidance: LogRhythm Software Upgrade Guide 7.x.x to 7.3.3, Version 7.3.3, March 21, 2018	**Maintained Guidance:** LogRhythm Upgrade a LogRhythm Deployment, September 13, 2021 (LogRhythm-Software-Upgrade Guide-7.8.0-RevA.pdf) Document updated for updated version of LogRhythm. Some material has been rearranged to support on-line display in a web browser.	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**

Evidence Identification	Description of Changes	Rationale	Impact
Guidance: What's New in LogRhythm 7.3, Version 7.3.3, March 21, 2018	**Maintained Guidance:** This document was specific to LogRhythm 7.3.3 and is not included in documentation for LogRhythm 7.8.	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
Guidance: LogRhythm MPE Rule Builder Parsing Guide, April 26, 2017 — Revision A	**Maintained Guidance:** LogRhythm Message Processing Engine Rule Builder, September 13, 2021 (LogRhythm-MPE-Rule Builder-Parsing-Guide-7.8.0 RevA.pdf) Document updated for updated version of LogRhythm. Some material has been rearranged to support on-line display in a web browser.	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
Guidance: LogRhythm Schema Dictionary and Guide, November 28, 2017 Revision A	**Maintained Guidance:** LogRhythm Schema Dictionary and Guide, September 13, 2021 (LogRhythm-Schema-Dictionary-and-Guide-7.8.0-RevA.pdf) Document updated for updated version of LogRhythm. Some material has been rearranged to support on-line display in a web browser.	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
Test Evidence: LogRhythm Integrated Solution v7.3 Test Plan, Version 0.21, 16 January	**Maintained Test Evidence:** LogRhythm Integrated Solution v7.8 Test Plan, Version 1.0, 11 November 2022	The changes/ update that have been made is not affecting the SFRs or	CB consider it as **Minor**

Evidence Identification	Description of Changes	Rationale	Impact
2019	All tests specified in the original test plan have been executed on LogRhythm Integrated Solution v7.8 and the results documented in the updated Test Plan. All tests passed, producing the same results as documented in the Test Plan for LogRhythm Integrated Solution v7.3.	functionality that was included in the scope of the previous evaluation.	

4 Result of Analysis

7 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 [2]) as required in accordance of Assurance Continuity: CCRA Requirements version 2.1 (2012-06-01) June 2012 (Ref [4]).

8 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.

Annex A References

[1] LogRhythm Integrated Solution v7.8 with Microsoft SQL Server 2016 SP1 Standard Edition Impact Analysis Report (IAR), Version 1.1, 23 November 2023

[2] LogRhythm Integrated Solution v7.8.0 with Microsoft SQL Server 2016 SP1 Standard Edition Security Target, Version 1.0, 13 May 2022

[3] Evaluation Technical Report - LogRhythm Integrated Solution v7.8.0 with Microsoft SQL Server 2016 SP1 Standard Edition V0.2, 11 February 2019 (EAU000631.01-S034-ETR

[4] Assurance Continuity: CCRA Requirements Version 2.2 September 2021

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

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

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

[8] MyCC Scheme Requirement (MyCC_REQ), v1a, January 2023.

[9] ISCB Evaluation Facility Manual (ISCB_EFM), v3, January 2023.

--- END OF DOCUMENT ---