C074 Certification Report

LogRhythm Integrated Solution v7.3 with Microsoft SQL Server 2016 SP1 Standard Edition

File name: ISCB-5-RPT-C074-CR-v1
Version: v1
Date of document: 12 April 2019
Document classification: PUBLIC

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

C074 Certification Report

LogRhythm Integrated Solution v7.3 with Microsoft SQL Server 2016 SP1 Standard Edition

12 April 2019

ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines,
No 7 Jalan Tasik,The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 □Fax: +603 8992 6841
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C074 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C074-CR-v1
ISSUE:	v1
DATE:	12 April 2019

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright and Confidentiality Statement

Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 12 April 2019 and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associated certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 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	14 March 2019	All	Initial draft of certification report
v1	12 April 2019	All	Final Certification report

Executive Summary

The Target of Evaluation (TOE) is LogRhythm Integrated Solution v7.3 with Microsoft SQL Server 2016 SP1 Standard Edition software. 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.

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.

The scope of the evaluation is defined by the Security Target (Ref [6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2) Augmented(ALC_FLR.2). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by BAE Systems Applied Intelligence MySEF (Malaysia Security Evaluation Facility) and completed on 7 March 2019.

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 LogRhythm Integrated Solution v7.3 with Microsoft SQL Server 2016 SP1 Standard Edition 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

1 Target of Evaluation

1.1 TOE Description

1 The TOE is LogRhythm Integrated Solution v7.3 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 functionality defined in the Security Target (Ref [6]) that was subsequently evaluated is as follows:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TSF
- SEM Component Requirements

1.2 TOE Identification

4 The details of the TOE are identified in Table 1 below.

Table 1: TOE Identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C074
TOE Name	LogRhythm Integrated Solution v7.3 with Microsoft SQL Server 2016 SP1 Standard Edition
TOE Version	7.3
Security Target Title	LogRhythm Integrated Solution v7.3 with Microsoft SQL Server 2016 SP1 Standard Edition Security Target
Security Target Version	Version 0.93
Security Target Date	16 January 2019
Assurance Level	Evaluation Assurance Level 2 Augmented with ALC_FLR.2

Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Criteria 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
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive, Columbia, Maryland 21046 USA
Developer	LogRhythm Incorporated 4780 Pearl East Circle, Boulder, Colorado 80301 USA.
Evaluation Facility	BAE Systems Applied Intelligence – MySEF (Malaysia Security Evaluation Facility) Level 28, Menara Binjai, 2 Jalan Binjai, 50450 Kuala Lumpur, Malaysia

1.3 Security Policy

5 There are no organisational security policies that have been defined regarding the use of the TOE.

1.4 TOE Architecture

6 The TOE includes both logical and physical boundaries as described in Section 2.2.1 and 2.2.2 of the Security Target (Ref [6]).

1.4.1 Physical Boundaries

7 The TOE architecture consists of the following components:

- Platform Manager (PM): The LogRhythm Platform Manager is a Windows server running Microsoft SQL Server 2016 SP1 Standard Edition. There is one Platform Manager per deployment to provide centralized event management, incident management, analysis, reporting, and configuration. The Platform Manager can be installed on a dedicated appliance (recommended for large environments) or on the same system as the DP/DX/AIE for smaller deployments.
- Data Processor (DP): The LogRhythm Data Processor is a Windows Server system. There can be one or more Data Processors per deployment to provide event processing and forwarding. In medium to large installations, Data Processors should be dedicated systems. In low volume deployments, a Data Processor can coexist on the same system as the PM/DP/AIE.

- Data Indexer (DX): The LogRhythm Data Indexer can be installed on Windows or Linux (CentOS 7.4 minimal) systems. The Data Indexer provides high-performance, distributed, and highly scalable indexing and searching of machine and forensic data. Indexers store both the original and structured copies of data to enable search-based analytics. In medium to large installations, Data Indexers should be dedicated systems. In low volume deployments, a Data Indexer can coexist on the same system as the PM/DP/AIE.
- AI Engine: The AI Engine is a Windows Server system. It is LogRhythm's advanced analysis platform that identifies and categorizes the log messages to determine if they will be forwarded to the Platform Manager as an Event. It provides real-time visibility into risks, threats, and critical operations issues. In medium to large installations, AI Engines should be dedicated systems. In low volume deployments, an AI Engine can coexist on the same system as the PM/DP/DX
- Web Console: The LogRhythm Web Console allows users to monitor network log activity from supported browsers on desktop computers, laptops, and touch-based tablets. The Web Console provides a customizable user interface with analytical and forensic features.
- Client Console: The LogRhythm Client Console provides deployment administration and user interaction with a LogRhythm deployment. Administrators use the Client Console to configure LogRhythm (for example, selecting rules that identify Events) and to view log reports and analyses. The Client Console is a Windows .NET-based client application that can be installed on the following Windows operating systems:

  Operating Systems (64-bit)
  - Windows 7
  - Windows 10 Server
  - Windows Server 2008 R2
  - Windows Server 2012 R2
  - Windows Server 2016
  - Microsoft .NET Framework 4.5.2 or later
- Data Collector: The optional Data Collector Appliance provides remote, high-performance collection of all machine data, including log messages, application data, security events, and network flows. They encrypt, compress and transport data from remote locations to LogRhythm Data Processors, either in real time or on a schedule. The Data Collector can also be deployed as software. Local, agent-based collection is performed by LogRhythm System Monitors, software that also functions as an endpoint monitor. System Monitors can be installed on servers and virtual machines running Windows, Linux or UNIX. It consolidates and collects log and machine data from remote environments and cloud infrastructure. A single agent functioning as a Data Collector can collect thousands of messages per second from dozens of devices.
- System Monitors: (also called LogRhythm Agents), collect and forward raw log data to the LogRhythm Data Processors. System Monitors can be installed on both Windows and UNIX platforms. They are also integrated into the LogRhythm Data Collector appliances.

1.4.2 Logical Boundaries

8 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TSF
- Security Event Manager Component requirements

9 **Security Audit:** The TOE can generate audit records of the following security-relevant events:

- Startup and shutdown of the TOE's auditing function;
- Successful and unsuccessful attempts to read the audit records;
- Access to the TOE, the log records collected by the TOE, and events identified by the TOE;
- All use of identification and authentication mechanisms;
- Modifications in the behavior of the TOE security functions;
- Modifications to the values of TSF data; and
- Modifications to a user's security management role.

10 The TOE records the following information in each audit record it generates: the date and time of the event; the type of event; the subject identity; the outcome of the event; and other information specific to the event type. All security audit events are generated from the LogRhythm Console. The Web Console records the use of identification and authentication mechanisms. Other TOE components generate only operational and error logs.

11 The TOE provides an interface to authorized users to read audit records from the audit trail and this interface is restricted to authorized roles. The TOE provides the ability to filter audit records on various fields in the audit data, and to include or exclude auditable events from the set of audited events based on "event type". The TOE prevents unauthorized modifications and deletions to the stored audit records by minimizing the available interfaces and restricting these interfaces to the authorized authenticated administrator. In addition, the TOE prevents the loss of audit data in the event the space available for storing audit records is exhausted.

12 The TOE is a software only implementation and therefore relies on the operational environment to provide a reliable timestamp. Additionally, the audit logs are stored in the file system and therefore rely on the operational environment for protection of the logs due to file permission enforcement.

13 **Identification & Authentication:** LogRhythm requires all users to be identified and authenticated before accessing any TOE functionality through the LogRhythm Console or Web Console. Users and roles are defined in the TOE, operating at the application layer. When a user logs in to the TOE, Windows Active Directory or the local Windows operating system authenticates the claimed user identity. Windows Active Directory and the local Windows operating system support both password and Common Access Card (CAC) credentials for user authentication. The TOE enforces the result. If authentication is successful then the application table is checked for the user's rights. If the user is not in the table then access is denied.

14 **Security Management:** The LogRhythm Console provides deployment administration and user interaction with LogRhythm with a Graphical User Interface (GUI). The console provides the capability to manage the auditing, analysis and reaction functions. The Deployment Manager is a utility window in the LogRhythm Console. People with LogRhythm administrator

credentials use it to configure and manage LogRhythm components and functionality such as alarming and reporting. The management functions are restricted to administrative roles.

15 The TOE comes with the following pre-defined security roles: Global Administrator, Restricted Administrator, Global Analyst, and Restricted Analyst. These roles, when assigned to users, provide varying levels of access to the TOE interfaces and functions.

16 **Protection of the TSF:** The TOE protects itself from tampering and bypass through several mechanisms implemented by the TOE and the operational environment. The underlying operating system separates processes into separate domains and prevents one process from accessing memory space of another process. The TOE uses TLS/HTTPS to protect data transmitted between the TOE components from unauthorized disclosure and modification. The TOE supports both self-signed certificates and user-supplied certificates for establishing TLS-protected communication. All TLS/HTTPS functionality is provided by the operating system in the operational environment.

17 The TOE Establishes secure communication channels between physically distributed components using TDS over TLS (for SQL Server Clients) or TLS (Mediator/System Monitor Agent, AIComMgr/Mediator, Client Console, Web Console). Timestamps are provided by the operational environment. The TOE normalizes time stamps to account for time zone differences.

18 **SEM Component Requirements**: The System Monitors are able to collect logs from multiple sources. The TOE analyzes the collected logs and performs correlation, pattern recognition, classification assignment, the processing of metadata and event identification. The TOE can take the appropriate action such as writing the event to a log file or sending an alert to an administrator The analyzer and system logs and events can be viewed from the Client and Web Console. A potential loss of logs is prevented by the layered architecture of the TOE's solution and by providing administrative interfaces to configure allocated storage and available disk storage.

1.5 Clarification of Scope

19 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, trained personnel and secure communication in accordance with user guidance that is supplied with the product.

20 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]).

21 TOE guidance documentation describes how to configure third-party devices to generate logs and how to configure the TOE to collect the logs. The third-party devices are not within the scope of evaluation.

1.6 Assumptions

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

23 A.Protect – The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

24 A.Platform – The underlying operating system of each TOE component will protect the component and its configuration from unauthorized access.

25 A.Manage – There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

26 A.Noevil – The authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

1.7 Evaluated Configuration

27 As stated in the ST (Ref [6]), there TOE is evaluated as a software application only. The TOE consists several software components that coordinate with one another to provide automated centralisation of log collection and event management.

28 A deployment of the LogRhythm Integrated Solution consists of:

- 1 or more Data Processor(s) Software
- 1 Platform Manager Software
- 1 or more Data Indexer(s) Software
- 1 or more System Monitors Software
- 0 or more Data Collectors Software
- 1 or more Advanced Intelligence (AI) Engines Software
- 1 or more instances of LogRhythm Client Console Software
- 1 or more instances of LogRhythm Web Console Software
- 1 Microsoft SQL Server 2016 SP1 Standard Edition

29 For convenience, the TOE can be delivered on preconfigured dedicated LogRhythm appliances. The appliance hardware, if purchased in this configuration, is not part of the TOE.

30 A deployment of the LogRhythm Integrated Solution software components, with the exception of the System Monitor agent/Data Collector, is required to be the same version 7.3. The LogRhythm Client and Web Consoles provide interfaces for TOE configuration and user management. The Data Indexer is configured via a browser connecting to the local Data Indexer AllConf service for initial configuration, and once it is placed into the evaluated configuration, the AllConf service is no longer used.

31 The TOE requires an NTP Server in the operational environment to ensure time is synchronized among the distributed components. The product provides time stamps for its own use derived from the system clock managed by the underlying operating system.

1.8 Delivery Procedures

32 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.

33 The delivery procedures should consider, if applicable, issues such as:

- ensuring that the TOE received by the consumer corresponds precisely to the evaluated version of the TOE;
- avoiding or detecting any tampering with the actual version of the TOE;
- preventing submission of a false version of the TOE;

- avoiding unwanted knowledge of distribution of the TOE to the consumer: there might be cases where potential attackers should not know when and how it is delivered;
- avoiding or detecting the TOE being intercepted during delivery; and
- avoiding the TOE being delayed or stopped during distribution.

34 The TOE delivery procedures include two forms:

- TOE Software: LogRhythm uses two methods of to ensure secure delivery of downloaded software. Secure connections over TLS (HTTPS) and SHA256 checksums. For the secure connections over TLS (HTTPS), login sessions to the LogRhythm Community, all downloads from the Community, as well as software downloads from logrhythm.com are secured using TLS over HTTP (HTTPS). This connection ensures that logins and downloads are encrypted and secure. SHA256 checksums ensures secure delivery of downloaded software. Customers can download a checksum file that corresponds to each software package received from LogRhythm support or downloaded from LogRhythm Community to ensure the package has not been compromised. After the installation package downloaded, use a checksum utility appropriate for your operating system to verify that the checksum of the downloaded file and the checksum provided by LogRhythm match. If the checksums match, the file is identical to what was built, and no corruption has occurred during the upload or download. If the checksums do not match, do not use the file and instead download the file again. If customers are unable to verify one or more downloaded files, customers are required to contact LogRhythm for assistance.
- TOE Hardware: LogRhythm uses FedEx distribution service or other, customer-preferred freight companies to distribute the package to the customer. On every TOE, a security label has been affixed to ensure that the TOE is not tampered with. If the unit is opened, then the label is broken, indicating the unit may have to be checked before accepting the package. The appliance package includes LogRhythm welcome letter, Appliances Installation Guide booklet and a packing list that customers can refer to ensure that all ordered items are in the box.

1.9 Documentation

35 It is important that the TOE is used in accordance with the guidance documentation in order to ensure secure usage of the product.

The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product.

- LogRhythm Client Console Reference Guide Rev. B, Version 7.3.3, 21 March 2018URL Reputation Filtering Deployment Guide, June 2018
- LogRhythm Web Console User Guide Rev. A, Version 7.3.3, 21 March 2018SMS Command Line Interface (CLI) Reference, June 2018
- LogRhythm Software Installation Guide Rev. C, Version 7.3.3, 19 February 2019
- LogRhythm TOE Hardware Delivery/Acceptance, Rev. A, 19 February 2019
- What's New in LogRhythm 7.3 Rev. D, Version 7.3.3, 21 March 2018

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 (ALC_FLR.2). The evaluation was performed conformant to the ISCB Product Certification Schemes Policy (PRODUCT_SP) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

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

- The evaluators testing consisted of independent testing efforts, which comprise both functional and penetration test cases to address testing requirements for the ATE_IND.2 and AVA_VAN.2 evaluation components.
- The testing approach for both testing was commensurate with the respective assurance components (ATE_IND.2 and AVA_VAN.2). For functional testing the focus was on testing the claimed security functionality (SFRs within the ST) through the interfaces specified in the functional specification (TSFI). For the penetration testing, the effort was limited to those attacks that are commensurate to an attacker with equal or less than Basic attack potential.

2.1.1 Life-cycle support

2.1.1.1 Configuration Management Capability

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

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

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

41 The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the CM documentation.

2.1.1.2 Configuration Management Scope

42 The evaluators confirmed that the configuration list includes the following set of items:

- the TOE itself;
- the parts that comprise the TOE; and
- the evaluation evidence required by the SARs in the ST.

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

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

2.1.1.3 TOE Delivery

45 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

2.1.2 Development

2.1.2.1 Architecture

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

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

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

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

2.1.2.2 Functional Specification

50 The evaluators examined the functional specification and determined that:

- the TSF is fully represented,
- it states the purpose of each TSF Interface (TSFI),
- the method of use for each TSFI is given,

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

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

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

2.1.2.3 TOE Design Specification

53 The evaluators examined the TOE design and determined that the structure of the entire TOE is described in terms of subsystems. The evaluators also determined that all subsystems of the TSF are identified. The evaluators determined that interactions between the subsystems of the TSF were described.

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

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

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

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

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

58 The evaluators determined that all SFRs were covered by the TOE design and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.3 Guidance documents

2.1.3.1 Operational Guidance

59 The evaluators examined the operational user guidance and determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

60 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

61 The evaluators examined the operational user guidance (in conjunction with other evaluation evidence and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

62 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

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

2.1.3.2 Preparation Guidance

64 The evaluators examined the provided delivery acceptance documentation and determined that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

65 The evaluators determined that the provided installation procedures describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.

66 The evaluators performed all user procedures necessary to prepare the TOE during testing and determined that the TOE and its operational environment can be prepared securely using only the supplied preparative user guidance.

2.1.4 IT Product Testing

67 Testing at EAL2 consists of assessing developer tests, performing independent functional tests, and conducting penetration tests. The TOE testing was conducted by the evaluators of BAE

Systems Applied Intelligence MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.4.1 Assessment of Developer Tests

68 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

2.1.4.2 Independent Functional Testing

69 At EAL2, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan and creating test cases that are independent of the developer's tests.

70 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Test ID	Description	SFRs
TEST-IND-001-CLIENT	• To test the TOE identification and authentication process and security roles. • To test that only authorised users are able to configure and perform TOE security management functions. • To test whether the TSF data is protected from disclosure or modification when it is transmitted between separate parts of the TOE. • To test the TOE SEM function to collect SEM data, allow only authorised users to review SEM data and perform analysis functions on the SEM data collected. • To test whether the TOE is able to protect SEM data from unauthorised modification and deletion and to take preventative measures when SEM storage exhaustion occurs.	FIA_ATD.1.1, FIA_UID.2.1, FIA_UAU.2.1, FMT_MOF.1.1, FMT_MTD.1.1, FMT_SMF.1.1, FMT_SMR.1.1, FMT_SMR.1.2, FPT_ITT.1.1, SEM_LDC_EXT.1.1, SEM_LDC_EXT.1.2, SEM_ANL_EXT.1.1, SEM_ANL_EXT.1.2, SEM_RDR_EXT.1.1, SEM_RDR_EXT.1.2, SEM_RDR_EXT.1.3, SEM_STG_EXT.1.1*, SEM_STG_EXT.1.2*, SEM_STG_EXT.1.3*, SEM_STG_EXT.2.1*
TEST-IND-002-WEB	• To test the TOE identification and authentication process and security roles. • To test whether the TSF data is protected from disclosure or modification when it is transmitted between separate parts of the TOE.	FIA_ATD.1.1, FIA_UID.2.1, FIA_UAU.2.1, FMT_SMR.1.1, FMT_SMR.1.2, FPT_ITT.1.1, SEM_LDC_EXT.1.1, SEM_LDC_EXT.1.2,

Test ID	Description	SFRs
	• To test the TOE SEM function to collect SEM data, allow only authorised users to review SEM data and perform analysis functions on the SEM data collected. • To test whether the TOE is able to trigger an alarm when an certain trigger is triggered.	SEM_ANL_EXT.1.1, SEM_ANL_EXT.1.2, SEM_RCT_EXT.1.1, SEM_RDR_EXT.1.1, SEM_RDR_EXT.1.2, SEM_RDR_EXT.1.3
TEST-IND-003-AUDIT	• To test the TOE identification and authentication process and security roles related to the security audit function. • To test that the TOE generates audit records and prevents unauthorised deletion to the stored audit records. • To test that the TOE is able to maintain existing audit records when audit storage exhaustion occurs.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.2.1, FAU_SAR.3.1, FAU_STG.2.1, FAU_STG.2.2, FAU_STG.2.3, FAU_STG.4.1

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

2.1.4.3 Penetration Testing

72 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, and TOE design and security architecture description.

73 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialist expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation.

74 The penetration tests focused on:

a) Unnecessary Open Ports

b) Common Vulnerability Scan

c) Broken Authentication Attack

d) SQL Injection

e) Insecure Communication

75 The results of the penetration testing demonstrate that the TOE is resistant to an attacker possessing a basic attack potential. However, it is important to ensure that the TOE is used

only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref [6]).

Vulnerability	AVA Reference	Test/Justification	Results
Unnecessary Open Ports	TEST-VA-001	To scan the TOE components for vulnerabilities associated with open ports and running services.	PASS
Common Vulnerability Scan	TEST-VA-002-WEB	To ensure that no common vulnerabilities are present on the LogRhythm Web Console.	PASS
Broken Authentication Attack	TEST-VA-003-WEB	To determine if the LogRhythm Web Console is resistant to broken authentication attacks	PASS
	TEST-VA-003-CLIENT	To determine if the LogRhythm Client Console is resistant to broken authentication attacks.	N/A
SQL Injection	TEST-VA-004-WEB	To test if the LogRhythm Web Console properly validates input and data coming from the user or from the environment, and verify if the TOE is resistant to major vulnerabilities in web applications such as SQL injection attacks.	N/A
	TEST-VA-004-CLIENT	To test if the LogRhythm Client Console properly validates input and data coming from the user or from the environment, and verify if the TOE is resistant to major vulnerabilities in client applications such as SQL injection attacks.	N/A
Insecure Communication	TEST-VA-005	To determine if the communication path between the different components of the TOE is secure	PASS

76 TEST-VA-003-CLIENT and TEST-VA-004-CLIENT were omitted as it was found that the TOE uses a custom communication protocol. The protocol employed by the TOE requires the randomisation of ports used for communication. Due to this, network traffic from the LogRhythm Client could not be proxied via the localhost and intercepted by Burp Suite. TEST-VA-004-WEB was omitted as well as it was found that the TOE uses WebSockets for

its text/search field, deterring the Burp Suite to inject malicious codes to the text/search field. It would take an attacker of greater than Basic attack potential to successfully exploit vulnerabilities associated with the above configuration.

2.1.4.4 Testing Results

77 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target (Ref [6]) and its functional specification. In addition, the documentation supplied as evidence for the EAL2 Augmented (ALC_FLR.2) Common Criteria evaluation of the TOE was analysed to identify possible vulnerabilities.

3 Result of the Evaluation

78 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 LogRhythm Integrated Solution v7.3 with Microsoft SQL Server 2016 SP1 Standard Edition performed by BAE Systems Applied Intelligence MySEF.

79 BAE Systems Applied Intelligence MySEF found that LogRhythm Integrated Solution v7.3 with Microsoft SQL Server 2016 SP1 Standard upholds the claims made in the Security Target (Ref [6]) and supporting documentation and has met the requirements of the Common Criteria (CC) assurance Level 2 (EAL2) Augmented (ALC_FLR.2).

80 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

81 EAL 2 Augmented (ALC_FLR.2) provides assurance by a full Security Target and analysis of the SFRs in that Security Target (Ref [6]), using functional and interface specifications, guidance documentation and a basic description of the design and architecture of the TOE, to understand the security behaviours of the TOE.

82 The analysis is supported by an independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to an attacker possessing a Basic attack potential.

83 EAL 2 Augmented (ALC_FLR.2) also provides assurance through use of a configuration management system and, evidence of secure delivery procedures.

3.2 Recommendation

84 The following recommendations are made:

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

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

Annex A References

A.1 References

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

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

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

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

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

[6] LogRhythm Integrated Solution v7.3 with Microsoft SQL Server 2016 Sp1 Standard Edition Security Target, Version 0.93, 16 January 2019

[7] EAU000631.01-S034-ETR, Evaluation Technical Report, Version 0.2, 11 February 2019

A.2 Terminology

A.2.1 Acronyms

Table 2: List of Acronyms

Acronym	Expanded Term
AIE	LogRhythm Advanced Intelligence Engine
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CLI	Command Line Interface
CCRA	Common Criteria Recognition Arrangement
CMDB	Case Management Database
DP	LogRhythm Data Processor
DX	LogRhythm Data Indexer
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
LDAP	Lightweight Directory Access Protocol

Acronym	Expanded Term
MPS	Messages per Second
MPD	Messages per Day
MPE	Message Processing Engine
MS-TDS	Microsoft Tabular Data Stream Protocol
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
NTP	Network Time Protocol
PM	LogRhythm Platform Manager
SA	System Administrator
SDEE	Security Device Event Exchange
SIEM	Security information and event management
SFR	Security Functional Requirement
ST	Security Target
TLS	Transfer Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface

A.2.2 Glossary of Terms

Table 3: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.

Term	Definition and Source
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
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 ---