National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

LogRhythm Integrated Solution 6.3.4

Report Number:	**CCEVS-VR-VID10645-2015**
Dated:	**December 22, 2015**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin
The Aerospace Corporation

Meredith Hennan
The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos Inc. (formerly SAIC, Inc.)
Columbia, MD

Table of Contents

1 Executive Summary 1
1.1 Interpretations 1
1.2 Threats....2
2 Identification 3
3 Security Policy 4
3.1 Security Audit 4
3.2 Cryptographic Support 4
3.3 Identification and Authentication 4
3.4 Security Management 4
3.5 Protection of the TSF 4
3.6 TOE Access 5
3.7 Trusted Path/Channel 5
4 Assumptions and Clarification of Scope 6
4.1 Assumptions 6
4.2 Clarification of Scope 6
5 Architectural Information 7
5.1 TOE Introduction 7
5.2 Physical Boundaries 9
6 Documentation 13
7 IT Product Testing 14
7.1 Developer Testing 14
7.2 Evaluation Team Independent Testing 14
7.3 Penetration Testing 14
8 Evaluated Configuration 15
9 Results of the Evaluation 16
10 Validator Comments/Recommendations 17
11 Annexes....18
12 Security Target 19
13 Abbreviations and Acronyms 20
14 Bibliography 21

List of Tables

Table 1: Evaluation Details.... 3
Table 2: Evaluated Assurance Requirements 16

1 Executive Summary

This report is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the LogRhythm Integrated Solution 6.3.4 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation of the LogRhythm Integrated Solution 6.3.4 was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in September 2015. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, and assurance activities specified in *Protection Profile for Network Devices*, Version 1.1, 8 June 2012 (NDPP) as amended by Errata #3. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The focus of this evaluation was on the auditing, identification/authentication, management, and cryptographic functionality of the TOE. The TOE encrypts all information that flows between itself and its trusted channels and paths. The LogRhythm Site Log Forwarder, Log Manager(s), AI Engine Server(s), Event Manager, Console(s) appliances, with the LogRhythm software, running Windows Server 2008 R2 and SQL Server 2008 software constitute the TOE.

The Leidos evaluation team determined that the TOE is conformant to *Protection Profile for Network Devices*, Version 1.1, 8 June 2012 (NDPP) as amended by Errata #3. The TOE, when configured as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in *LogRhythm Integrated Solution 6.3.4 Security Target*, Version 1.2, December 18, 2015. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test reports produced by the Leidos evaluation team.

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test reports. The validation team found that the evaluation showed that the TOE satisfies all of the security functional and assurance requirements stated in the Security Target (ST). The evaluation also showed that the TOE is conformant to Protection Profile, and that the assurance activities specified in the Protection Profile had been performed appropriately. Therefore, the validation team concludes that the testing laboratory’s findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the Evaluation Technical Report are consistent with the evidence produced.

1.1 Interpretations

Not applicable.

1.2 Threats

The TOE ST includes, by reference, the Security Problem Definition (composed of organizational policies, threat statements, and assumptions) from the NDPP. In general, the NDPP has presented a Security Problem Definition appropriate for network infrastructure devices, and as such is applicable to the LogRhythm TOE.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Details

Evaluated Product:	LogRhythm Integrated Solution 6.3.4
Sponsor:	LogRhythm Inc. 4780 Pearl East Circle Boulder, CO 80301
Developer:	LogRhythm Inc. 4780 Pearl East Circle Boulder, CO 80301
CCTL:	Leidos (formerly Science Applications International Corporation) 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	26 June 2015
Completion Date:	21 December 2015
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 4, September 2012.
Evaluation Class:	None
PP:	*Protection Profile for Network Devices*, Version 1.1, 8 June 2012 (NDPP) as amended by Errata #3 dated 3 November 2014
Evaluation Personnel:	Leidos (formerly Science Applications International Corporation): Catherine Sykes Anthony Apted Kevin Micciche Zalman Kuperman
Validation Body:	National Information Assurance Partnership CCEVS
CCEVS Validators:	Daniel Faigin, The Aerospace Corporation Meredith Hennan, The Aerospace Corporation

3 Security Policy

The TOE enforces the following security policies as described in the ST.

3.1 Security Audit

The TOE is designed to be able to generate logs for a wide range of security relevant events including the events specified in the NDPP. The TOE can be configured to store the logs locally so they can be accessed by an administrator.

The TOE operates as a log collector, receiving log events transmitted to it from a range of log sources. The TOE receives the logs over a trusted channel using IPsec, TLS, or TLS/HTTPS.

3.2 Cryptographic Support

The TOE is operated in FIPS mode and includes NIST-validated cryptographic algorithm implementations for asymmetric key generation, symmetric encryption and decryption, cryptographic signature services, cryptographic hashing services, keyed-hash message authentication services, deterministic random bit generation seeded from a suitable entropy source and key zeroization. The cryptographic algorithm implementations support cryptographic protocols used for secure communication—IPsec, TLS and HTTPS.

3.3 Identification and Authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE provides both local and remote administrative access. Local access is via a direct console connection. Remote access is via a thick client (the LogRhythm Client Console) secured by TLS or web-based graphical user interface (the Web Console) secured by TLS/HTTPS.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. Additionally, the TOE can be configured to use Active Directory to support, for example, centralized user administration.

3.4 Security Management

The TOE provides a thick client (Client Console) and a web-based client (Web Console) as mechanisms to access its security management functions. Security management commands are limited to administrators and are available only after they have provided acceptable user identification and authentication data to the TOE.

3.5 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. The TOE ensures that reliable time information is available (e.g., for log accountability) provided through the use of a NTP Server. The NTP server is considered part of the operational environment.

The TOE uses FIPS 140-2 certified cryptographic algorithms to protect communications between distributed TOE components.

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

3.6 TOE Access

The TOE can be configured to display an informative banner that will appear prior to an administrator being permitted to establish an interactive session. The TOE subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session will be terminated.

The TOE provides users (local and remote) the ability to terminate their own interactive sessions, by logging off of the TOE.

3.7 Trusted Path/Channel

The TOE protects interactive communication with remote administrators using HTTP over TLS or TLS. TLS ensures both integrity and disclosure protection. The TOE is configured by an administrator to receive external log records over a secure (IPsec, TLS or HTTPS protected) trusted channel.

The TOE supports external user authentication via Active Directory, over a secure IPsec communication between the TOE and Active Directory.

The TOE provides an interface to the Knowledge Base server and can be configured to automatically check for Knowledge Base updates. Communications with the Knowledge Base server are protected using TLS/HTTPS.

4 Assumptions and Clarification of Scope

4.1 Assumptions

This security target includes by reference the Security Problem Definition (composed of organizational policies, threat statements, and assumptions) from the NDPP. In general, the NDPP has presented a Security Problem Definition appropriate for network infrastructure devices, and as such is applicable to the LogRhythm TOE.

4.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in *Protection Profile for Network Devices*, Version 1.1, 8 June 2012 (NDPP) as amended by Errata #3 dated 3 November 2014 and performed by the evaluation team).
2. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in *LogRhythm Integrated Solution 6.3.4 Security Target*, Version 1.2, December 18, 2015. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
5. The TOE is a network device consisting of several components that coordinate with one another to provide automated centralization of log collection and event management. The TOE collects information from multiple log sources (such as syslog, snmp, netflow and sflow devices, Windows events, flat file, databases or applications). The product also provides File Integrity Monitoring and Machine Analytics, with Host and Network Forensics, in a unified Security Intelligence Platform. It analyzes collected data and provides tools to view and analyze IDS results and to issue alerts of significant events; however this functionality is outside the scope of the evaluation. The only capabilities covered by the evaluation are those in the NDPP; all other capabilities are not covered.
6. The TOE must be configured as described in Common Criteria Supplemental Guidance document, to be in the evaluated configuration.

5 Architectural Information

5.1 TOE Introduction

The LogRhythm Site Log Forwarder (SLF), Log Manager(s) (LM), AI Engine Server(s), Event Manager (EM), Console appliances, with the LogRhythm software, running Windows Server 2008 R2 and SQL Server 2008 software constitute the TOE. The Web Server appliance includes a Nginx web server. The TOE is delivered pre-configured on dedicated appliances.

The Figure 1 shown below depicts the TOE components within their environment and shows communications among the components and operational environment devices. SQL Server is an internal component of Log Managers and Event Manager and is not shown in the figure. The figure depicts examples of collection sources including syslog, snmp, netflow and sflow devices but the TOE can also collect Windows events, flat file, databases or applications.

In general, remote log information flows to the SLF. The SLF in turn passes information to the Log Managers and AI Engine Servers to the Event Manager where a SQL Server is used internally to store log information. Log Managers analyze individual log messages and identify Events. The SLFs collect logs that were stored in various locations, e.g., Windows Event Log, SQL Server trace files and converts collected logs to ASCII text strings, which can be encrypted before forwarding across untrusted networks (e.g. Internet). An Event is a log message or collection of log messages that LogRhythm determines to be important or interesting. AI Engine Servers analyze log metadata gleaned from sets of log messages to identify more complex Events. The Event Manager processes Events and raises alarms as appropriate. Administrators use the Client Console to configure LogRhythm (for example, selecting rules that identify Events) and to view log reports and analyses. The alarms may be viewed by the Web Console or Client Console. Optionally the alarms may be sent to an external SMTP Server or SNMP Server in the operational environment. Alarms are not in the scope of evaluation and were not tested.

Each SLF forwards logs to the LM that is configured to receive them, where they are analyzed against defined Knowledge Base rules, written to a centralized database in the LM, and also archived on a file system. SLF communications with LM(s) are authenticated and encrypted via FIPS 140-2 certified TLS. Each LM consists of a SQL Server 2008 R2 instance and a LogRhythm Mediator Server. The Mediator Server takes in log messages (collected and forwarded by SLF and processes them against Knowledge Base rules that identify and categorize the log messages. The applied Knowledge Base rules determine whether the Mediator Server forwards log metadata to an AI Engine or forwards the log message to the EM as an Event or both. The Mediator Server is also responsible for writing incoming logs to an active archive, which is a file on the file system of the LM Host. Once that active archive file reaches a certain size or age (administrative configurable), the active archive is converted to an inactive archive file. During that conversion, the contents are SHA-1 hashed and then compressed. The SHA-1 hash value is stored in a database table within the LogRhythm Event Manager. If there is a restore request of the logs contained within the inactive archives, the SHA-1 hash is verified to ensure that the file has not been altered since being sealed. Communications between LM and AI Engine Server and between LM and EM are protected by FIPS 140-2 certified TLS. Updates to the Knowledge Base rules can be obtained by licensed customers at the LogRhythm’s website. Though the Knowledge Base server and Knowledge Base Rules themselves have not been subject to evaluation; the communications with the Knowledge Base server is protected using TLS/HTTPS and this has been tested. The Knowledge Base Server communicates with the EM. The EM, via the Client Console or Job Manager, contacts the Knowledge Base server and the Knowledge base updates are downloaded directly to the EM database.

An AI Engine Server consists of two services: AI Engine Communication Manager service and AI Engine service. The AI Engine Communication Manager receives log metadata from one or more Log Managers. It marshals the data for the AI Engine to process. Also, it maintains TLS connections with Log Managers.

An AI Engine processes the data by applying AI rules to the set of log metadata collected over time. An AI rule can correlate multiple log messages to identify an Event, which the AI Engine sends to the EM.

The EM consists of two services: the LogRhythm Alarming and Response Manager (ARM) service and the Job Manager service together with a SQL Server instance. There is only one EM per deployment. The EM receives and maintains log information from the LMs that have been analyzed against the Knowledge Base rules and have been identified as Events. The EM receives Events corresponding to complex conditions from the AI Engine Server. The ARM service evaluates Alarm Rules to determine if an Event (or series of Events) should be alarmed on and, if so, what the response should be (e.g., sending e-mails to people on a notification list, sending SNMP traps, or perform a remediation action).

The Web Console is a component that comprises a single service on the LogRhythm Web Services appliance. To support the most common end-user activities, the user interface provides easy access to analytical tools, alarms, and customized dashboards. The Web Console includes graphic visualizations and guided workflows for both trained security analysts and non-technical users. The Web Console communication is protected by FIPS 140-2 certified TLS/HTTPS.

The Client Console provides the user interface into a LogRhythm deployment. The Client Console is a Windows .NET-based client application that provides authenticated users with the ability to view logs, Events, alarms and reports. The Client Console also provides real-time monitoring, incident management, and interfaces for TOE configuration and user management. All communications between the Client Console and LogRhythm servers (EM and LMs) are protected by FIPS 140-2 certified TLS.

The product also provides a programmatic interface to maintain the integrity of shared information distributed between LogRhythm and other external data sources. This includes the ability to automate the exchange and synchronization of configuration data to enhance administrative functions as well as extend monitoring and analysis functions. The LogRhythm Web Services are intended to provide broad interoperability. They are SOAP based, WS-1 Basic Profile 1.1 compliant. A WSDL 1.1 compliant descriptor is provided which can be used to generate proxy classes in .Net, JAVA, or other languages. The Web Services API is not included in the evaluated configuration.

Site Log Forwarder (SLF) – LogRhythm’s SLF appliances contain an Agent-Less System Monitor Agent that collects log, flow, and machine data for secure transport from remote locations to LogRhythm LMs. An Agent-less collector means that an agent is not required to be installed on the log sources being collected from. SLFs additionally manage bandwidth consumption via collection scheduling and/ or compression of transmitted data.

Every TOE deployment will have one EM component, at least one LM component, AI Engine Server and at least one Site Log Forwarder (SLF) component along with the consoles.

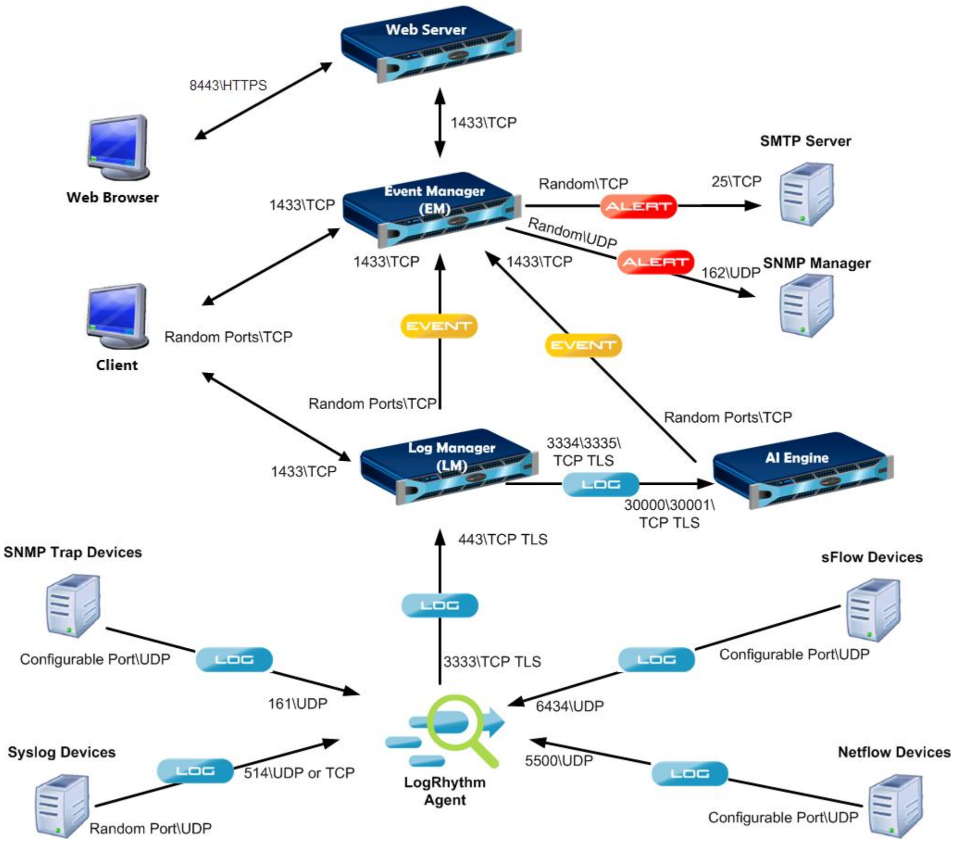

Figure 1 TOE Components

5.2 Physical Boundaries

The LogRhythm 6.3.4 TOE consists of the following hardware and software components:

The LogRhythm components operate within the context of a Windows Server 2008 R2 operating system and require a SQL server database. For the purposes of evaluation against the NDPP, the Windows operating system and SQL database are included with the LogRhythm components in the TOE boundary, which is bounded by the physical hardware appliances on which they are installed.

Other than the specific software component installed on a given appliance, the only differences among the appliance models relate to speed, performance and capacity (as described in the tables below) and do not affect any of the claimed security functions. Each appliance has Windows Server 2008 R2 with SQL Server 2008 installed on the Log Manager and the Event Manager.

All-in-one (XM) - LogRhythm XM appliances provide all the capabilities of the EM and LM appliance on the same platform. Many deployments begin with an XM configuration providing a high performance solution in a single appliance.

Appliance Series	Appliance Model	Description
LR-XM4300	LR-XM4310 LR-XM4330 LR-XM4350 (combined EM/LM	Max Processing – 1,000 MPS CPU – 6 core Memory - 64 GB

Appliance Series	Appliance Model	Description
	server)	Storage - (Useable -1TB) (Raw 2 TB) Ethernet – Broadcom 5720 (2 x 1 GB)
LR-XM6300	LR-XM6310 LR-XM6330 LR-XM6350 (combined EM/LM server)	Max Processing – 5,000 MPS CPU – 12 core Memory - 128 GB Storage - (Useable -2TB)) (Raw 4 TB) Ethernet – Broadcom 5720 (4 x 1 GB)

Event Manager - The LogRhythm Event Manager server is a Windows Server system. There is one Event Manager per deployment. The Event Manager provides centralized event management, incident management, analysis, reporting, and configuration across a LogRhythm deployment.

Appliance Line	Description
LR-EM3350	Max Processing – N/A CPU – 6 core Memory - 64 GB Storage - (Useable -1TB) (Raw 2 TB) Ethernet – Broadcom 5720 (2 x 1 GB)
LR-EM5350 (dedicated EM server)	Max Processing – N/A CPU – 12 core Memory - 128 GB Storage - (Useable -2TB)) (Raw 4 TB) Ethernet – Broadcom 5720 (4 x 1 GB)
LR-EM7350 (dedicated EM server)	Max Processing – N/A CPU – 16 core Memory - 128 GB (Expandable 256 GB) Storage - (Useable -2TB)) (Raw 4 TB) Ethernet – Broadcom 5720 (4 x 1 GB)

Log Manager (LM) - LogRhythm LM appliances provide high performance, distributed and redundant log collection and management. Each LogRhythm deployment has at least one Log Manager.

Appliance Series	Appliance Models	Description
LR-LM3300	LR-LM3310 LR-LM3350	Max Processing – 2,500 MPS CPU – 6 core Memory - 64 GB Storage - (Useable -1TB) (Raw 2 TB) Ethernet – Broadcom 5720 (2 x 1 GB)
LR-LM5300	LR-LM5310 LR-LM5350	Max Processing – 5,000 MPS CPU – 12 core Memory - 128 GB Storage - (Useable -2TB)) (Raw 4 TB) Ethernet – Broadcom 5720 (4 x 1 GB)

Appliance Series	Appliance Models	Description
LR-LM7300	LR-LM7310 LR-LM7311 LR-LM7312 LR-LM7313 LR-LM7350 LR-LM7351 LR-LM7352 LR-LM7353 (dedicated LM servers)	Max Processing – 15,000 MPS CPU – 16 core Memory - 128 GB (Expandable 256 GB) Storage - (Useable -2TB)) (Raw 4 TB) Ethernet – Broadcom 5720 (4 x 1 GB) Note: The models are all the same system, but with different numbers of DAS attached and different LR licensing levels. The number of DAS for each model is the last number of model number. For example model number LR-LM7353 has 3 DAS.

Advanced Intelligence (AI) Engine - The AI Engine is a Windows Server system. It is LogRhythm's advanced analysis platform that performs correlation, pattern recognition, and behavioral analysis. It receives logs from the Log Manager Mediator's AI Engine Data Provider and sends events to the Event Manager. There are no databases for the AI Engine. It communicates with the Log Manager. It consists of the following services: AI Engine Communication Manager and AI Engine Server.

Appliance Line	Description
LR-AIE5310	Max Processing – 15,000 MPS CPU – 6 core Memory - 64 GB / (Expandable 128 GB) Storage - 550 GB Ethernet – Broadcom 5720 (4 x 1 GB)
LR-AIE7310	Max Processing – 30,000 MPS CPU – 16 core Memory - 128 GB / (Expandable 256 GB) Storage - 1 TB Ethernet – Broadcom 5720 (4 x 1 GB)
LR-AIE9310	Max Processing – 75,000 MPS CPU – 32 core Memory - 256 GB / (Expandable 512 GB) Storage - 1 TB Ethernet – Broadcom 5720 (4 x 1 GB)
MPS = Messages Per Second	

Site Log Forwarder (SLF) - The Site Log Forwarder is an appliance containing an Agent-Less System Monitor Agent. An Agent-less collector means that an agent is not required to be installed on the log sources being collected from. The System Monitor Agent, also just called Agent, provides local and remote log data collection across various operating systems including Windows, Linux, AIX, HPUX, and Solaris. It serves as a central log data collector, collecting logs from many devices, servers, databases, and applications, performing host activity monitoring and forwarding logs, via authenticated TCP connections, to the Log Manager. The communications channel with the various log sources are protected using IPsec, TLS or HTTPS. The communication channel from the SLF to the LM component is protected using TLS.

Appliance	Description
SLF3310	A System Monitor Agent: Max Collection Rate: 10,000 CPU – 6 core Memory - 16 GB RAM Ethernet – (2 x 1 GB) Physical Disk: 2 x 300 GB 10K RPM SAS RAID 1 278 GB usable Logical Volume: C Drive (200 GB) D Drive (78 GB)

The SLF collects audit data from the monitored sources. As such the operating environment includes devices being monitored by the TOE.

LogRhythm Console – In the evaluated configuration the Client Console is installed on one of the appliances (either the EM or XM) and communicates with both the LM and the EM and provides local administration. The Console provides interfaces for TOE configuration and user management. Identification, Authentication and administrative activity are audited to hold users accountable for their actions. The audit records are protected from unauthorized modification and deletion. All administrators must be identified and authenticated (authentication is performed either by the local Windows OS or by Active Directory in the operational environment).

Web Services Host[1] – The Web Services appliance is a component that hosts the LogRhythm Web Console that supports most common end-user activities, and provides a user interface for easy access to analytical tools, alarms, and customized dashboards.

Appliance	Description
WS3310	Max Processing – 1,000 MPS CPU – 6 core Memory - 32 GB Storage - (Useable -1TB) (Raw 2 TB) Ethernet – Broadcom 5720 (2 x 1 GB)

[1] The Web Console/ Web Services Host component is referred to as the Web Server in Figure 1.

6 Documentation

LogRhythm offers a number of guidance documents along with a CC-specific supplemental document describing the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features.

- LogRhythm Help
- LogRhythm Web Console Installation Guide Version 6.3.4
- LogRhythm Web Console User Guide Version 6.3.4
- LogRhythm Compliance Overview AGD Supplement Guide
- LogRhythm Solution Software (LRSS) Installation Guide v6.3

Additional guidance documentation is provided by LogRhythm on purchase of their network device or through their website.

These guidance documents contain security-related guidance material for this evaluation and must be referenced to place the product within the Common Criteria evaluated configuration. The guidance documents are applicable the version of LogRhythm claimed by this evaluation.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following, which is not publically available:

- LogRhythm Integrated Solution 6.3.4 Common Criteria Test Report and Procedures, Version 3.0, December, 2015

7.1 Developer Testing

The assurance activities in *Protection Profile for Network Devices* do not specify any requirement for developer testing of the TOE.

7.2 Evaluation Team Independent Testing

The evaluation team devised a test plan based on the Test Assurance Activities specified in *Protection Profile for Network Devices*. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test report identified above.

As documented in Figure 1 shown in Section 5.1, the following hardware and software components were included in the evaluated configuration during testing:

- TOE Software
  - LogRhythm 6.3.4
- TOE Software Platform
  - Windows Server 2008 R2
- Test Environment Components
  - Logging Components
  - Web Browser (IE/Firefox/Chrome)
  - Net Internals (via Chrome)
  - Power Shell (via Windows)
  - LogRhythm Log Generator (Test Tool)
  - Wireshark

As can be seen above, the configuration used during testing of the TOE matches the configuration specified in the ST.

Evaluation testing took place at the LogRhythm facility in Boulder, Colorado in April 2015.

Subsequently, the evaluators exercised all the test cases. The tests were selected in order to ensure that each of the test assertions specified in *Protection Profile for Network Devices* were covered. All tests passed. A summary of the testing performed by the evaluation team is provided in *LogRhythm Integrated Solution 6.3.4 Common Criteria Assurance Activities Report*.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any obvious vulnerabilities applicable to the TOE in its evaluated configuration.

8 Evaluated Configuration

The TOE is LogRhythm Integrated Solution 6.3.4 running in EM/LM configuration or in XM configuration, which is installed and configured according to *LogRhythm Compliance Overview document, 9 December 2015*. The TOE in its evaluated configuration is delivered on a hardware appliance running Windows Server 2008 R2. The TOE is configured to operate in FIPS mode.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Protection Profile for Network Devices, Version 1.1, 8 June 2012 (NDPP) as amended by Errata #3 dated 3 November 2014*, in conjunction with Version 3.1, Revision 4 of the CC and CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the PP, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Final ETR, which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: Evaluated Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

Please note the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the LogRhythm Compliance Overview (AGD Supplement) document.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

The ST for this product’s evaluation is LogRhythm Integrated Solution 6.3.4 Security Target, Version 1.2, 18 December 2015

13 Abbreviations and Acronyms

AAR	Assurance Activities Report
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
EM	Event Manager
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
IKE	Internet Key Exchange—a protocol used to set up a security association (SA) in the IPsec protocol suite
IP	Internet Protocol—communications protocol for relaying datagrams across network boundaries
IPsec	Internet Protocol Security—a protocol suite for securing IP communications
IT	Information Technology
LM	Log Manager
MB	Megabyte
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol—a means of synchronizing clocks over a computer network
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
PIN	Personal Identification Number—a password used to access a secured system (e.g., USB token)
RFC	Request for Comments—an Internet Engineering Task Force memorandum on Internet standards and protocols
SLF	Site Log Forwarder
SSH	Secure Shell—a network protocol for secure data communication and remote command execution
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
URL	Uniform Resource Locator—typically a web address
VR	Validation Report
XM	All-in-one LogRhythm appliance

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012. Part 1: Introduction and general model. CCMB-2009-07-001.

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012Part 2: Security functional components. CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012. Part 3: Security assurance components. CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012. Evaluation methodology. CCMB-2009-07-004.

[5] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[6] Protection Profile for Network Devices, Version 1.1, 8 June 2012 (NDPP) as amended by Errata #3 dated 3 November 2014.

[7] LogRhythm Integrated Solution 6.3.4 Security Target, Version 1.2, 18 December 2015.

[8] LogRhythm Integrated Solution 6.3.4 Common Criteria Assurance Activities Report, Version 0.5, 21 December 2015.

[9] Evaluation Technical Report for LogRhythm Integrated Solution 6.3.4 Part 1 (Non-Proprietary), Version 1.1, 21 December 2015.

[10] Security Target Evaluation Technical Report for LogRhythm Integrated Solution 6.3.4 (Proprietary), Version 0.4, 21 December 2015.

[2][11] LogRhythm Compliance Overview, 9 December 2015.

[12] Installation Guide: LogRhythm Solution Software (LRSS) v6.3, 12 March 2015.

[13] LogRhythm Help, 10 March 2015.

[14] LogRhythm Web Console User Guide, Version 6.3.4, 11 March 2015.

[15] LogRhythm Web Console Installation Guide, Version 6.3.4, 9 March 2015.

[2] Also known as the AGD Supplement Guide