National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

LogRhythm v6.0.4 with Microsoft SQL Server 2008 R2 Enterprise Edition

Report Number: CCEVS-VR-VID10389-2012
Dated: 30 November 2012
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

Mario Tinto

The Aerospace Corporation

Jandria Alexander

The Aerospace Corporation

Common Criteria Testing Laboratory

SAIC, Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the LogRhythm Integrated Solution product was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in March 2012. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The SAIC evaluation team determined that the product is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 2 augmented with ALC_FLR.2. The ST and TOE are also conformant to the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007 augmented with FIA_UID.2, FIA_UAU.2 and FMT_SMF.1. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

LogRhythm 6.0.4 with Microsoft SQL Server 2008 R2 Enterprise Edition 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 capabilities, anomaly and insider threat detection, turnkey appliance configuration, and a console management interface. The TOE is dependent on the correct operation of the environment and on its underlying OS, neither of which are included within the scope of the evaluation.

A deployment of the LogRhythm consists of: one Event Manager; zero or more Advanced Intelligence Engine (AI Engine) Server(s); one or more Log Manager(s); one or more System Monitor Agent(s) with Trace File Converter; one or more Console(s); and one or more SQL Server instances.

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the LogRhythm Integrated Solution Security Target (ST).

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	LogRhythm, v6.0.4
Sponsor:	LogRhythm, Inc. 4780 Pearl East Circle Boulder, CO 80301

VALIDATION REPORT
LogRhythm v6.0.4

Developer:	LogRhythm, Inc. 4780 Pearl East Circle Boulder, CO 80301
CCTL:	Science Applications International Corporation 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	2 December 2009
Completion Date:	30 March 2012
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007.
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1, Revision 2, September 2007.
Evaluation Class:	EAL 2 augmented with ALC_FLR.2
Description:	LogRhythm 6.0.4 with Microsoft SQL Server 2008 R2 Enterprise Edition is an Intrusion Detection System (IDS) consisting of several components that coordinate with one another to collect and analyze information from multiple log sources (such as Windows events, syslog, flat file, NetFlow, sFlow, databases or applications) and provides tools to view and analyze IDS results and to issue alerts of significant events.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the LogRhythm v6.0.4 product by any agency of the U.S. Government and no warranty of the LogRhythm product is either expressed or implied.
PP:	U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007 augmented with FIA_UID.2, FIA_UAU.2, and FMT_SMF.1
Evaluation Personnel:	Science Applications International Corporation: Anthony J. Apted Julie Cowan Chris Keenan
Validation Body:	National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
- An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
- An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
- An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
- An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
- An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
- An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
- Unauthorized attempts to access TOE data or security functions may go undetected.
- Improper security configuration settings may exist in the IT System the TOE monitors.
- Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
- Vulnerabilities may exist in the IT System the TOE monitors.
- The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
- The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
- The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
- Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
- Inadvertent activity and access may occur on an IT System the TOE monitors.
- Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

1.4 Organizational Security Policies

The ST identifies the following organizational security policies that the TOE and its operational environment are intended to fulfill:

- Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
- Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
- The TOE shall only be managed by authorized users.
- All data collected and produced by the TOE shall only be used for authorized purposes.
- Users of the TOE shall be accountable for their actions within the IDS.
- Data collected and produced by the TOE shall be protected from modification.
- The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

2 Identification

The evaluated product is **LogRhythm v6.0.4 with Microsoft SQL Server 2008 R2 Enterprise Edition**.

3 Security Policy

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

> ***Note:*** *Much of the description of the LogRhythm v6.0.4 security policy has been derived from the LogRhythm Integrated Solution ST and Final ETR.*

3.1 Security Audit

The TOE recognizes, and can generate audit records of, the following 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. 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. Other TOE components generate only operational and error logs.

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 sort 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 to, and deletion of stored audit records by minimizing the available interfaces and restricting these interfaces to the authorized authenticated administrators. In addition, the TOE prevents the loss of audit data in the event that the space available for storing audit records is exhausted.

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.

3.2 Identification and Authentication

LogRhythm requires all users to be identified and authenticated before accessing any TOE functionality through the 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.

3.3 Security Management

The console provides the capability to manage the auditing, analysis, and reaction functions. The management functions are restricted to administrative roles. The TOE comes with two pre-defined administrative roles: Global Admin and Global Analyst. The TOE supports a customer-defined Restricted Analyst role (that is, subset of the Global Analyst privileges). These roles, when assigned to users, provide varying levels of access to the TOE interfaces and functions.

3.4 Protection of the TOE Security Functions

All communication channels between TOE components are protected by FIPS 140-2 certified SSL. The TOE supports both self-signed certificates and user-supplied certificates for establishing SSL-protected communication. This includes the following communication channels:

- Console to Server (Event Manager or Log Manager) communications,
- System Monitor Agent to Log Manager communications,
- Log Manager to AI Engine Server communications,
- Log Manager to Event Manager communications, and
- AI Engine Server to Event Manager communications.

The integrity of LogRhythm archives is protected by SHA-1 hashing and compression. Logs received by the Log Manager are hashed and compressed by the Mediator Service before being stored in an archive, which is a file on the file system of the Log Manager. This protection is provided to inactive archived files for use in verifying integrity during archive restoration and other operations. The collected logs are formatted as ASCII text strings and can be encrypted before forwarding across untrusted networks (e.g., Internet). Modification of the archived logs can be detected by rehashing and comparing the values. Note that the SHA-1 hash values are stored in the EM database. Timestamps are provided by the operational environment. The TOE normalizes time stamps to account for time zone differences.

3.5 IDS Component requirements

The System Monitor Agents are able to collect relevant information from multiple sources. The Log Manager performs analysis on the collected information by processing the data against known signatures. The Log Manager forwards log metadata to the AI Engine Server. The AI Engine Server can analyze sets of logs for more complex signatures. For example, together the Log Manager and AI Engine Server can detect security event/violations based on integrity checks

and signature definitions. The Event Manager can take the appropriate action such as writing the event to a log file or send an alert to an administrator.

The analyzer and system logs and events can be viewed from the Console. A potential loss of logs can be prevented by the TOE's layered architecture by providing administrative interfaces to configure database sizes and automatic purging scripts.

Each log or event collected by the System Monitor Agent contains the date and time of the event (or log), subject identity, and the outcome of the event. In addition, some logs contain location, service, protocol information; source and destination addresses; and other information specific to the type of log collected. The System Monitor Agent is capable of collecting the following events: startup and shutdown; identification and authentication events; data accesses; service requests; network traffic; security configuration changes; data introduction; detected malicious code; access control configuration; service configuration; authentication configuration; accountability policy configuration; and detected known vulnerabilities. A syslog server is included in each System Monitor Agent. However, the operational environment may be required to provide additional syslog servers to support additional log sources.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- The TOE has access to all the IT System data it needs to perform its functions.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- The TOE is appropriately scalable to the IT System the TOE monitors.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The TOE can only be accessed by authorized users.

4.1 Clarification of Scope

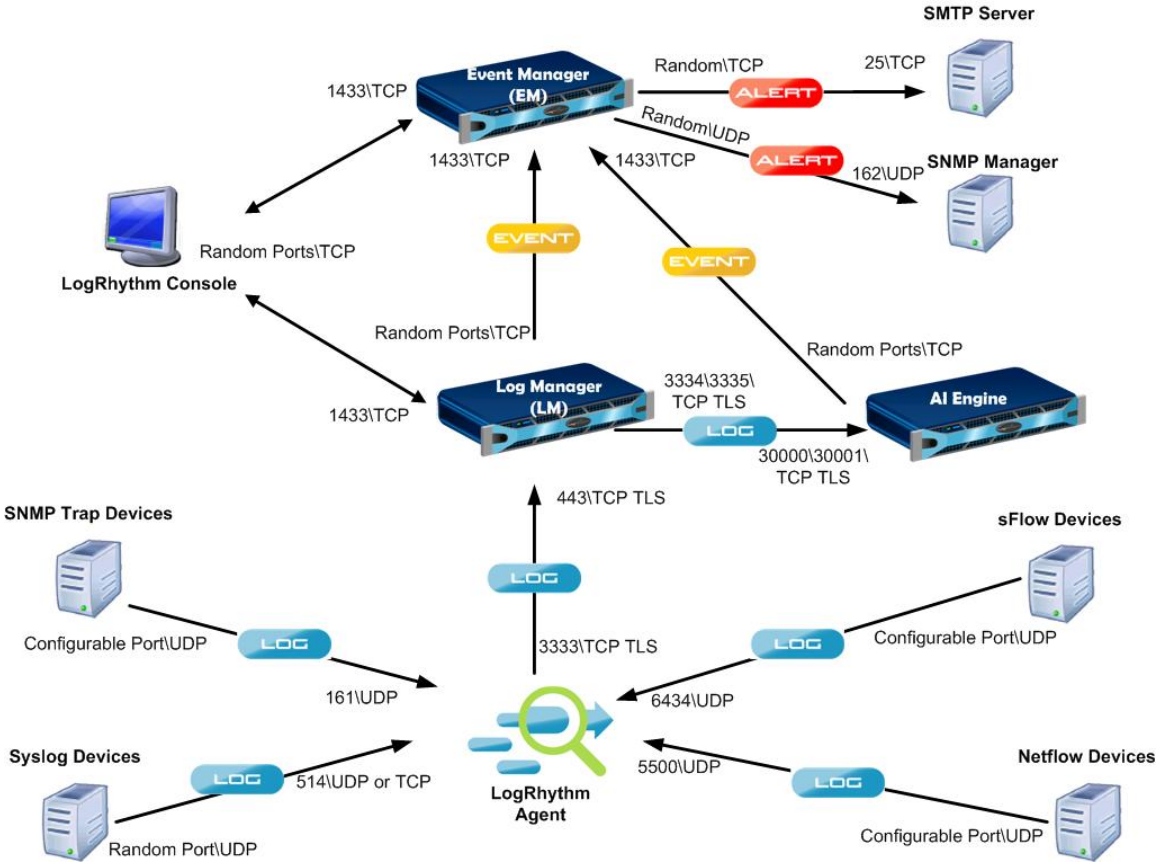
All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 augmented with ALC_FLR.2 in this case).
2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.

3. As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, 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.
4. The TOE relies on the operational environment in which it operates for the following security and other functionality:
   - The operational environment will provide the capability to protect audit information.
   - The operational environment will provide reliable timestamps to the TOE.
   - The operational environment will provide the capability to protect the confidentiality of data communicated by the administrative users to the TOE.
5. The following product capabilities described in the guidance documentation were not included within the scope of the evaluation and no claims are made regarding them:
   - The ability of the TOE to provide endpoint monitoring and control functionality, which is provided by the User Activity Monitor (UAM), the File Integrity Monitor (FIM) and the Data Loss defender (DLD). Since these capabilities are not addressed by the IDS System PP, to which the TOE claims conformance, they are outside the scope of the evaluation and are disabled by default.
   - The use of a SQL Server for user authentication. Although the product includes support for the use of a SQL Server for user authentication, it must be disabled since the evaluated configuration requires the TOE to use Windows Active Directory or the local Windows operating system for user authentication.
   - Product features supporting redundancy. Because they are not included in the scope of the evaluation, any product features supporting redundancy must not be used in the evaluated configuration.
   - The "LogRhythm Backup and Recovery Procedures", "Performance Counters" and "Log Processing Report" sections of the Administrator's Guide in the LogRhythm 6.0.4 Help document are not applicable to the evaluation according to the LogRhythm v6.0.4 Common Criteria Guide.
   - The "Network Visualization", "Save Investigation as a Report", "Reporting Center", and "Customizing Reports" sections of the User's Guide in the LogRhythm 6.0.4 Help document are not applicable to the evaluation according to the LogRhythm v6.0.4 Common Criteria Guide.
6. Third-party devices can be used in the operational environment to generate logs, but the evaluation did not address the capabilities of any specific such devices. The System Monitor Agent component of the TOE is evaluated to collect logs in the formats specified in the ST (i.e., Windows Event Logs, syslog, SNMP trap, sFlow, and NetFlow).

5 Architectural Information

The following diagram 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 diagram.



The LogRhythm System Monitor Agent(s), Log Manager(s), AI Engine Server(s), Event Manager, Console(s) and SQL Server software constitute the TOE. The TOE can be purchased as software only or pre-configured on dedicated appliances.

In general, log information flows from System Monitor Agents through Log Managers and AI Engine Servers to the Event Manager, with SQL Server used internally to store log information. System Monitor Agents collect log messages. Log Managers analyze individual log messages and identify Events. 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 Console to configure LogRhythm (for example, selecting rules that identify Events) and to view log reports and analyses.

The System Monitor Agents are capable of collecting logs from most sources, including Windows events (local and remote), syslog, flat file, NetFlow, databases, or applications. The System Monitor Agent converts collected logs to ASCII text strings, which can be encrypted before forwarding across untrusted networks (e.g. Internet). Trace File Converter is a support service, which converts binary SQL Server log data to UTF-8 text suitable for collection by a System Monitor Agent

Each System Monitor Agent 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. System Monitor Agent communications with LM(s) are

authenticated and encrypted via FIPS 140-2 certified SSL[1]. Each LM consists of an SQL Server 2008 R2 instance and a LogRhythm Mediator Server. The Mediator Server takes in log messages (collected and forwarded by LogRhythm System Monitor Agents) 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 (administrator 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 SSL. Updates to the Knowledge Base rules can be obtained by licensed customers at the vendor's website.

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 as well as maintaining SSL connections. 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, which has been analyzed against the Knowledge Base rules, in the form of 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 performing a remediation action).

The Console provides the user interface into a LogRhythm deployment. The Console is a Windows .NET-based client application. Authenticated users can view logs, Events, alarms and reports. The Console also provides real-time monitoring, incident management, and interfaces for TOE configuration and user management. The Console tools also provide interfaces to the administrator to configure the pruning and aging scripts which are designed to automatically manage the LM and EM databases. All communications between the Console and LogRhythm servers (EM and LMs) are protected by FIPS 140-2 certified SSL. An AI Engine Server obtains its configuration from the Console indirectly via the EM.

Every TOE deployment will have one EM component, at least one LM component, and at least one System Monitor Agent component. An AI Engine Server is optional in a TOE deployment. Each appliance configuration includes agent software and, in the case where a software-only purchase is made, the agent software must also be installed. The System Monitor Agent is the only component responsible for collecting the logs. The System Monitor Agent collects the logs and forwards them to an LM. LogRhythm has the capability to perform "agent-based" or "agent-less" monitoring, dependent on the source of log data. Typically, monitoring flat files requires a System Monitor Agent be installed on the system where the log resides. This is an example of

[1] SSL is used as a generic term here. The TOE implements TLS 1.0. FIPS certificate numbers: 1051, 1111, 1337, 1805, 1807, 1808 and 1817.

agent-based monitoring (i.e., any deployment where a System Monitor Agent must be installed where the log data resides). "Agent-less monitoring" refers to any log source that a System Monitor Agent accesses remotely via network resources (for example Windows Event logs via API or ASCII flat files via network storage shares) or any log source that pushes log messages to a System Monitor Agent (for example syslog and Checkpoint firewall logs). "Agent-less" does not mean that there is no System Monitor Agent involved, but rather the System Monitor Agent is not on the same system as the log source. Note that Windows Event Logs can be collected in an agent-based or agent-less configuration. In addition to being able to read its local Windows Event Logs, the Windows System Monitor Agent can connect to remote Windows assets and pull the Windows Event Logs, which are then forwarded to a LM. All System Monitor Agents contain an integrated syslog server. In addition, Windows System Monitor Agents include a SNMP trap receiver, Netflow servers, and sFlow Collectors, allowing for the reception of SNMP, Netflow, and sFlow data for collection.

As identified in the above discussion, the EM and each LM in a deployment includes a SQL Server instance. SQL Server is provided as part of the TOE distribution—the customer is not required to have an instance of SQL Server in the operational environment prior to installation. This means LogRhythm is able to configure SQL Server for maximum security as part of the TOE installation (this is discussed in "LogRhythm Software Solution 6 Installation Guide").

The SQL Server Management Studio Audit interface provides user capabilities to manage and view the security audit trail. The TSF and its operational environment limit SQL Server Management Studio Audit access to authorized administrators, using database and file system permissions. SQL Server requires each user to identify and authenticate before allowing access to the stored procedures developed by LogRhythm that provide support for security audit functionality, including audit selection and audit review. SQL Server uses Windows authentication in the evaluated configuration (either local or Active Directory).

6 Documentation

6.1 Product Guidance

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- LogRhythm v6.0.4 Common Criteria Guide, Revision 4, March 30, 2012
- LogRhythm 6.0.4 Help, v001, February 1, 2012
- LogRhythm Solution Software 6 Installation Guide, Revision 4, January 21, 2011
- LogRhythm 5.1 MPE Rule Builder Cheat Sheet, July 7, 2010
- LogRhythm Components and Operating System Compatibility, Revision 1, January 23, 2012

6.2 Evaluation Evidence

The following tables identify the additional documentation submitted as evaluation evidence by the vendor. With the exception of the Security Target, these documents are proprietary and not available to the general public.

Design Documentation	Version	Date
LogRhythm Engineering Specification EngNote_CCArchitecture	2	30 Jan 2012

LogRhythm Engineering Specification EngNote_CCFuncSpec	3	1 Feb 2012
LogRhythm Engineering Specification EngNote_CCTOEDesign	2	30 Jan 2012
LogRhythmErrors_60 (Excel spreadsheet)		

Configuration Management Documentation	**Version**	**Date**
LogRhythm Common Criteria Configuration Management Supplement	6	30 Mar 2012
LogRhythm Database Schema Versioning and Configuration Management	2	19 Jul 2011
LogRhythm Software Build 6.0	1	6 Oct 2011
LogRhythm Software Versioning	2	19 Jul 2011

Delivery and Operation Documentation	**Version**	**Date**
LogRhythm Appliance Imaging Upgrade Process	2	13 Oct 2011
LogRhythm Common Criteria Delivery Supplement	5	12 Mar 2012
LogRhythm Software Delivery Process	3	17 Aug 2011

Flaw Remediation Documentation	**Version**	**Date**
LogRhythm Technical Support Standards and Procedures	5	3 Oct 2011
LogRhythm Defect Categorization	1	1 Apr 2012
LogRhythm QA Software Defect Process	4	1 Sept 2011

Test Documentation	**Version**	**Date**
LogRhythm v6.0.3 Common Criteria Test Case Advanced Intelligence (AI) Engine Interface		10 Feb 2012
LogRhythm v6.0.3 Common Criteria Test Case Audit Interface		10 Feb 2012
LogRhythm v6.0.3 Common Criteria Test Case Console Interface Deployment		10 Feb 2012
LogRhythm v6.0.3 Common Criteria Test Case Console Interface Management		10 Feb 2012
LogRhythm v6.0.3 Common Criteria Test Case Mediator Interface		10 Feb 2012
LogRhythm v6.0.3 Common Criteria Test Case *NIX Agent Interface		10 Feb 2012
LogRhythm v6.0.3 Common Criteria Test Case TLS TSF Interfaces		10 Feb 2012
LogRhythm v6.0.3 Common Criteria Test Case Windows Agent Interface: Netflow		10 Feb 2012
LogRhythm v6.0.3 Common Criteria Test Case Windows Agent Interface: sFlow		10 Feb 2012
LogRhythm v6.0.3 Common Criteria Test Case Windows Agent Interface: SNMP Trap Receiver		10 Feb 2012
LogRhythm v6.0.3 Common Criteria Test Case Windows Agent Interface: Syslog		19 Jan 2012
LogRhythm v6.0.3 Common Criteria Test Case System Storage Exhaustion		10 Feb 2012
TCD_LRv6.0.3_ConsInt_Manage_20120120.xls		20 Jan 2012
TCR_LRv6.0.3_AgInt_Netflow_Windows_20120110		10 Jan 2012
TCR_LRv6.0.3_AgInt_SNMPTrap_Windows_20120111.xls		11 Jan 2012
TCR_LRv6.0.3_AgInt_Syslog_Windows_20120110.xls		10 Jan 2012

TCR_LRv6.0.3_AuditInt_20120113.xls		13 Jan 2012
TCR_LRv6.0.3_TLSInt_20120122.xls		22 Jan 2012
TCR_LRv6.0.3_ConsInt_Deploy_20120112.xls		12 Jan 2012
TCR_LRv6.0.3_AgInt_sFlow_Windows_20120111.xls		11 Jan 2012
TCR_LRv6.0.3_AgInt_Syslog_NIX_20120116.xls		17 Jan 2012
TCR_LRv6.0.3_AIEInt_20120123.xls		23 Jan 2012
TCR_LRv6.0.3_StExh_20120123.xls		23 Jan 2012
TCR_LRv6.0.3_MedInt_20120210.xls		10 Feb 2012
LogRhythm Quality Assurance Test Case Management Process	1	31 Oct 2011
LogRhythm v6.0.3 Common Criteria Test Plan	5	10 Feb 2012

Security Target	Version	Date
LogRhythm Integrated Solution Security Target	1.1	30 Mar 2012

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for LogRhythm v6.0.4 with Microsoft SQL Server 2008 R2 Enterprise Edition.

Evaluation team testing was conducted at the vendor's development site March 19 through March 23, 2012.

7.1 Developer Testing

The vendor's approach to testing for LogRhythm is based on manual testing of the LogRhythm features and security functions. LogRhythm is tested using a number of manual test suites organized by interface, with varying numbers of test cases, which are separately documented in individual Microsoft Word test case documents.

The Microsoft Word test case documents are separated by interface to address the specific interface tested, but also provide a mapping to show the security functions covered in the testing of the given interface. For LogRhythm, test cases were provided for all of the interfaces (Syslog Server, NetFlow Server, SNMP Manager, sFlow Collector, Mediator, Console, SQL Server Management Studio, TLS, and AIE Server), which provided coverage for all of the security functions, including Security Audit, Identification and Authentication, Security Management, Protection of the TOE Security Functions, and IDS Component requirements.

The vendor ran the TOE test suites in various configurations, consistent with the test environment described in the testing documentation, and provided the evaluation team with the actual results. The test configurations were representative of the operating systems supported and the application environment. All tests passed.

7.2 Evaluation Team Independent Testing

The evaluation team chose a subset of the vendor tests to run, based on the following criteria: coverage of TSFI described in the FSP; coverage of security functions described in the TSS; coverage of SFRs specified in the ST; at least 20% of the vendor test suite (the final sample size actually comprised 40% of the developer's test suite). Since the vendor's test documentation was organized according to the defined TSFI, coverage of TSFI was achieved by ensuring at least one

test case from each test document was included in the sample. The evaluation team used the results from the test coverage analysis to identify tests for each security function and SFR.

The test sample selected by the evaluation team covered the following TOE security functionality:

- Configuration and management of security auditing
- Generation and review of audit records, including: capabilities for sorting audit records; selecting the auditable events in the set of audited events, based on event type; and restrictions on the roles able to read the audit records in the audit trail
- Configuration and management of user accounts
- User identification and authentication
- Security management functions and restrictions on which roles can perform specific security management functions
- Configuration and management of the IDS capabilities, including: collection of logs from various sources (syslog, Windows Event Log, NetFlow, sflow, and SNMP traps); analysis; alerts; and notifications
- Review of IDS results
- Protection of communication between distributed TOE components
- Behavior when IDS data storage is exhausted.

The evaluation team executed the selected sample of the vendor test suite for LogRhythm v6.0.4 per the evaluated configuration as described in the developer's test documentation. This documentation describes the testing environment for LogRhythm as follows:

TOE Software:

- Event Manager
- AI Engine Server
- Log Manager
- System Monitor Agent
- Console

Operating System:

- Microsoft Windows Server 2008 R2

Database (for storing TOE data):

- Microsoft SQL Server 2008 R2 Enterprise Edition

Supported operating systems for the System Monitor Agents:

- Windows XP, 7, Server 2003, Server 2008, and Server 2008 R2
- RedHat Linux 2.4 and 2.6
- Debian, Ubuntu, and CentOS
- Solaris 8, 9, and 10, and Solaris 10x86
- HP-UX 11.11
- AIX 5.2, 5.3, and 6.1

The evaluation team devised and performed the following additional functional tests:

- **Testing Security Audit**—the evaluation team added additional testing to supplement the vendor's testing of the Security Audit function to confirm the following requirements: in addition to the vendor coverage on sorting, the evaluation team wanted to ensure that the audit logs can be sorted based on the type of event and the outcome of an event (success or failure); the evaluation team wanted to verify that when an event was included or excluded from the auditable events, the expected audit was/was not recorded; finally, the evaluation team wanted to verify that audit records are protected from unauthorized deletion.
- **Testing Identification and Authentication**—the evaluation team added additional testing to supplement the vendor's testing of the Identification and Authentication function, to determine that in the event of an unsuccessful login attempt, an error message would not provide specific details as to whether it was the login username and/or password that was incorrect. In testing this, the evaluation team found that since FIPS mode requires the Windows credentials be used for login, there is no opportunity for a user to enter incorrect credentials if the Windows login was successful.
- **Testing Security Management**—the evaluation team complemented the developer's testing of the Security Management security function by confirming that the role restrictions between the Global Admin and Global Analyst are exactly as described in the Security Target.
- **Testing the Protection of the TSF**—the evaluation team complemented the developer's testing of the Protection of the TSF security function by confirming that the communication sessions between the AI Engine Server and the Log Manager are encrypted and hashed.
- **Testing the IDS component requirements**—the evaluation team complemented the developer's testing of the IDS component requirements security function by confirming that a customized Restricted Analyst Administrator cannot view any system data if it is not granted to the user by the Global Admin.

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 vulnerabilities applicable to the TOE in its evaluated configuration. In addition, the developer performed an Nmap scan of the TOE in its test environment and provided an analysis of the results to the evaluation team. The list of open ports shows that the services running are minimal, and do not belong to the TOE process. This signifies that the TOE does not expose a network interface that opens it up for network-based attacks.

8 Evaluated Configuration

The evaluated version of the TOE is LogRhythm v6.0.4 with Microsoft SQL Server 2008 R2 Enterprise Edition.

The TOE 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 capabilities, anomaly and insider threat detection, turnkey appliance configuration, and a console management interface.

A deployment of the TOE consists of the following software components: one Event Manager; zero or more AI Engine Server(s); one or more Log Manager(s); one or more System Monitor Agent(s); one or more Console(s); one or more SQL Server instances.

The Event Manager and Log Manager can reside on the same server for low-volume deployments, or on dedicated servers for high volume deployments. Each AI Engine Server runs on a dedicated system. The System Monitor Agents can be deployed on Windows, Linux, Solaris, HP-UX or AIX systems.

The Event Manager, AI Engine Server, Log Manager, and System Monitor Agent software can be pre-installed on vendor-supplied appliance(s) or can be installed directly on a system by the customer. Each appliance solution consists of LogRhythm software (EM, AI Engine Server, LM, System Monitor Agent, or Console), hardened Windows Operating System (Windows Server 2008 R2 with .NET framework) and hardened SQL Server 2008 R2 Enterprise Edition. Windows Server, .NET Framework, and the appliance hardware (if purchased in this configuration) are not part of the TOE. Each System Monitor Agent includes a syslog server. Additional syslog servers may be required to support additional log sources in the operational environment. SMTP servers are required to support the TOE.

The Console software can be installed on the following operating systems:

- Windows Server 2000;
- Windows Server 2003 32- and 64-bit;
- Windows XP 32-bit;
- Windows Vista 32-bit;
- Windows Server 2008 32-bit;
- Windows 7 32/64-bit; and
- Windows Server 2008 R2 64-bit.

All releases of the operating systems listed are supported. One or more of these operating systems is required for all configurations; one for each Console desired. Also required for notifications in all configurations is at least one SMTP or one SNMP server. A full-featured LogRhythm deployment would include servers for both types of notifications.

The integrated solution can be delivered in a single appliance called the XM appliance or through a combination of integrated Log Manager, AI Engine Server, and Event Manager appliances (called LM, AI Engine Server, and EM appliances, respectively). An XM appliance includes Log Manager and Event Manager, but not AI Engine Server. A deployment can contain XM, LM, AI Engine Server, and EM appliances and SLF (System Monitor Agent-only log collection) although only one Event Manager is active in a deployment.

An SLF (a stand-alone appliance that includes System Monitor Agent software) is not required for a typical deployment, as agents are generally installed directly on the customer's IT infrastructure. SLF's are generally indicated when change control prohibits installation of foreign software on customer systems.

LogRhythm appliances are available in two families: LRX, which comprises LM, EM and XM appliances; and AIE, which comprises AI Engine Server appliances. There are five different LRX hardware configurations: LRX1; LRX1-2; LRX2; LRX3; and LRX3-2. There are two different AIE hardware configurations: AIE1; and AIE2. Within each family, there are no

security functional differences between the hardware configurations. The only differences are in performance and storage capacity.

For each LRX hardware configuration, three software configurations are available: EM appliance (Event Manager on one box), LM appliance (Log Manager on one box) or XM appliance (EM and LM on one box). In all three cases, a SQL Server and System Monitor Agent are included on the appliance. The appliances designated -2 indicate the appliance provides twice the storage of the original model; i.e. LRX1-2 provides twice the storage of the LRX1. The LRX1 provides 12 GB RAM and 272 GB storage capacity. The LRX2 provides twice the RAM of the LRX1 and 834 GB storage capacity. The LRX3 provides 32GB RAM and 1.25 TB storage capacity.

Each AI Engine Server hardware configuration supports the same AI Engine Server software, as described above. The AIE1 provides 32 GB RAM and 272 GB storage capacity. The AIE2 provides 96 GB RAM and 544 GB storage capacity.

Optional System Monitor Agent-only collection appliances (SLFs), Log Manager appliances (LMs), and AI Engine Server appliances can be added as needed. The appliances can be configured to address log volumes ranging from tens of millions to over a billion logs per day. Customers expecting more logs may require additional LM and AI Engine Server appliances.

The TOE contains no dependencies on the underlying hardware and the appliance is provided to customers at their request only as a convenient packaging bundle. Regardless of whether the customer purchases a software-only solution or an appliance, the TOE executable is the same with the exception of the agent code, which may differ based on the supported platform.

If a software only configuration is selected, the following operational environment components are required (in addition to the OS requirement for the Console identified above): one or more Windows Server 2008 R2 operating systems and the underlying hardware to host the EM, AI Engine Server, LM, and System Monitor Agent components. Note that the System Monitor Agents can additionally be installed on:

- Windows: XP 32-bit; Vista 32- and 64-bit; 7; Server 2003 32- and 64-bit; Server 2008 32- and 64-bit; Server 2008 R2 64-bit;
- Linux 2.4: Red Hat Enterprise Linux (RHEL) 9 32-bit;
- Linux 2.6: CentOS 5.1 32-bit; CentOS 5.5 64-bit; Debian 5.0.3 32-bit; Fedora 7 32-bit; RHEL 5 32- and 64-bit; RHEL 6 64-bit; SUSE Linux 9 64-bit; Ubuntu 9.10 32- and 64-bit; Ubuntu 10 32-bit;
- Solaris 8, 9, and 10 SPARC; Solaris 10 x86;
- HP-UX 11i: v1, v2, v3 PA-RISC; v2, v3 Itanium 64-bit;
- AIX: 5.2, 5.3 and 6.1 64-bit.

All versions of the specified operating systems are supported. Depending on the supporting platform, the System Monitor Agents will have different binaries, though the binaries for Linux, Solaris and AIX share the same source code base. Also required are the following:

- Active Directory
- Connections are supported for Windows Server 2008 R2 using .Net V3.5
- IP*works libraries are used for SNMP (version 8 .Net Edition which supports SNMP V1 and V2).

SMTP is provided by the OS and meets RFC821 specifications. Please see the LogRhythm Installation Guide for additional details including instructions for securing (hardening) the Windows operating system. Moreover, the TOE may be run in a virtualized environment, since the TOE has no dependencies on the underlying hardware. The security environment is the same

whether the customer installs TOE software on physical or virtual devices. Please see the LogRhythm Installation Guide for a Virtual Appliance installation of the TOE software.

Regardless of whether the customer purchases a software-only solution or an appliance, the TOE functionality is the same.

9 Results of the Evaluation

The evaluation was conducted based upon version 3.1 of the CC and the 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 agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an "EAL2 augmented with ALC_FLR.2" certificate rating be issued for LogRhythm v6.0.4 with Microsoft SQL Server 2008 R2 Enterprise Edition.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the SAIC CCTL. The security assurance requirements are listed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_ARC.1	Security architecture description
ADV_FSP.2	Security-enforcing functional specification
ADV_TDS.1	Basic design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.2	Use of a CM system
ALC_CMS.2	Parts of the TOE CM coverage
ALC_DEL.1	Delivery procedures
ALC_FLR.2	Flaw reporting procedures
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample
AVA_VAN.2	Vulnerability analysis

10 Validator Comments/Recommendations

The validators do not have any additional comments or recommendations regarding the TOE.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is **LogRhythm Integrated Solution Security Target,** Version 1.1, dated March 30, 2012.

13 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 1, September 2006, CCMB-2006-09-001.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1, Revision 2, September 2007, CCMB-2007-09-002.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1, Revision 2, September 2007, CCMB-2007-09-003.
4. Common Methodology for Information Technology Security: Evaluation Methodology, Version 3.1, Revision 2, September 2007, CCMB-2007-09-004.
5. LogRhythm Integrated Solution Security Target, Version 1.1, March 30, 2012.