CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

C010 Certification Report
Log Radar v3.2.15 with modules Console, Collector and Archiver

File name: ISCB-5-RPT-C010-CR-v1a
Version: v1a
Date of document: 13 February 2013
Document classification: PUBLIC

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

C010 Certification Report

Log Radar v3.2.15 with modules Console, Collector and Archiver

13 February 2013

ISCB Department

CyberSecurity Malaysia

Level 8, Block A, Mines Waterfront Business Park,

No 3 Jalan Tasik, The Mines Resort City

43300 Seri Kembangan, Selangor, Malaysia

Tel: +603 8946 0999 Fax: +603 8946 0888

http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C010 Certification Report – Log Radar v3.2.15 with modules Console, Collector and Archiver
DOCUMENT REFERENCE:	ISCB-5-RPT-C010-CR-v1a
ISSUE:	v1a
DATE:	13 February 2013

DISTRIBUTION:	UNCONTROLLED COPY – FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 8, Block A,

Mines Waterfront Business Park,

No 3 JalanTasik, The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Forward

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 13 February 2013, 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 at www.commoncriteriaportal.org).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate 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 3 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 3 (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
v1	23 January 2013	All	Final Released.
v1a	13 February 2013	Page iv	Add the date of the certificate.

Executive Summary

Log Radar v3.2.15 with modules Console, Collector and Archiver (hereafter referred as Log Radar) from TecForte Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL2) evaluation.

Log Radar is a software system used on enterprise data networks to centralise the storage and interpretation of logs, or events, generated by other devices or applications. Its primary function is to act as an aggregator to various disparate network devices of varying vendor origins within any given network infrastructure. Its key aims are to collect, normalise process and manage such information (logs) from a real time context.

The TOE comprises of multiple components as follows:

a) Collector - acts as the primary point of contact between the TOE and any input from devices. Its core function is to collect streams of data as and when they occur and process these device specific logs into a common and normalised form.

b) Console - acts as the interfacing point between user and TOE. This is the point in which authentication, auditing, systems security management and any other operation requiring user involvement occurs.

c) Archiver - functions as a backup daemon. Part of the utilities extended by TOE as its log management features include the ability for a user to specify the amount of active data that is to be kept on server. Since sensitive security centric data should never be permanently deleted, the Archiver functions as a backup mechanism which will automatically archive data that surpasses set configuration to a separate location.

The security functions of the TOE that are within the scope of evaluation are identification and authentication, security audit, granular access control, password management, session management, secure socket layer, import and export of configuration data, automated archive, and real time syslog collection.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for 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 EAL2. The report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by the CyberSecurity Malaysia MySEF and was completed on 15 January 2012.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangement on the Recognition of Common Criteria certificates and the product will be listed on the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that the Log Radar meets their requirements. It is recommended that a potential user of the Log Radar to 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

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), Log Radar v3.2.15 with modules Console, Collector and Archiver (hereafter referred as LogRadar), is an automated software system used on enterprise data networks to centralise the storage and interpretation of logs, or events, generated by other devices or applications. Its key aims are to collect, normalise process and manage such information (logs) from a real time context.

2 LogRadar provides a centralised security management console to track security events throughout the enterprise security infrastructure. Its normalisation and correlation engine are able to process security information generated by security devices such as Firewall, VPN and others into a clear and easy to understand report. This allows administrator to produce readable high-level management reports and construct rules based on the asset and its location.

3 The TOE component comprises of:

a) Collector – acts as the primary point of contact between the TOE and any input from devices. Its core function is to collect streams of data as and when they occur and process these device specific logs into a common and normalised form.

b) Console – acts as the interfacing point between user and TOE. This is the point in which authentication, auditing, systems security management and any other operation requiring user involvement occurs.

c) Archiver – functions as a backup daemon. Part of the utilities extended by TOE as its log management features include the ability for a user to specify the amount of active data that is to be kept on server. Since sensitive security centric data should never be permanently deleted, the Archiver functions as a backup mechanism which will automatically archive data that surpasses set configuration to a separate location.

All 3 components are designed to operate independently from each other. Other components of Log Radar v3.2.15 are Aggregator and Real Time Monitor which are not included in the scope of the security evaluation.

4 In the context of the evaluation, the TOE is expected to provide the following major security features:

a) Identification and authentication – the TOE provides user identification and authentication independent from the operating system on which it operates on.

b) Security audit – the TOE records each individual user session and tracks each action within the session.

c) Granular access control – the TOE allows users access permission within the application to be dynamically and granularly assigned via users and group memberships.

d) Password management – the TOE provides a full password management function including the management of password policy rules as well as password expiry settings.

e) Sessions management – the TOE maintain session management and restricts a single login for only a single valid session.

f) Socket layer – the TOE runs on Secure Socket Layer (SSL) to protect its data when travelling thru the network.

g) Import and export of configuration data – the TOE allows import and/or export of specific configuration data for restoration or recovery purposes.

h) Automated archive – the TOE provides a mechanism where the auto archival of aggregated reports, rawlogs and syslogs will be automatically hashed with MD-5 checksum, archived with AES encryption and stored at predetermined times.

i) Real time syslog collection – the TOE provides the ability for authorised users to dynamically configure the TOE to listen to syslog streams from network devices, servers and/or any other supported applications.

1.2 TOE Identification

5 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	C010
TOE Name	Log Radar v3.2.15 with modules Console, Collector and Archiver
TOE Version	v3.2.15
Security Target Title	LogRadar Security Target
Security Target Version	v1.0R
Security Target Date	15 January 2013
Assurance Level	Evaluation Assurance Level 2 (EAL2)
Criteria	Common Criteria July 2009, Version 3.1, Revision 3
Methodology	Common Methodology for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL2

Sponsor and Developer	TecForte Sdn Bhd No 2A-13-2, Plaza Sentral-Phase II, Jalan Stesen Sentral 5, Kuala Lumpur Sentral, 50470 Kuala Lumpur, Malaysia.
Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

6 The TOE implements access control policy to restrict access to the TOE. The administrator is responsible to assign user's access based on the user's role. The user needs to provide correct username and password in order to access the TOE. The TOE will give access permission to the users based on the Access Control List (ACL) stated in Table 1 of the ST (Ref [6]).

7 In order to ensure secure and strong passwords, administrator is also responsible to setup password policy rules where the password lengths, number of expired passwords retained, and expiration period of a password can be configured.

8 The TOE also implements syslog collection policy where the authorised users are responsible to configure the TOE to listen to syslog streams from network devices, servers or any other supported applications. After the configuration, the collection process will be executed automatically as and when events occur. If the incoming logs are from unknown or unregistered devices, or the format is unrecognised, the TOE will store them in other location which will be accessed by authorised users manually.

9 The details of these security policies are described in Section 7.2 of the Security Target (Ref [6]).

1.4 TOE Architecture

10 The TOE includes both logical and physical boundaries which are described in Section 2.3 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

11 The TOE security functions comprises of the following:

a) Identification and authentication – the TOE provides this security feature to protect and prevent access from unauthorised users to the system. In addition, it will also require each user to be identified and authorised first before any access to protected functions and data is granted. Authentication and identification is performed via a username password combination that will not only identify a specific user to the system but also define the level of access permitted to that particular user account. The TOE provides the ability for login rules which would automatically disable a user account if it detects login

failures that surpasses the threshold set by administrators. On top of it, hashing is performed on user passwords during authentication or during password creations before they are saved into the database.

b) Security audit – the TOE provides auditing layer which will monitor activities and executions occurring within the system. Activities in this context are defined as operations occurring within the system that might or might not be initiated by a user. For instance a user login would be an auditable event, but in the same way an automated data synchronization transfer that is scheduled to occur periodically (and as such not subject to user initiation) qualifies also as an auditable event. Each auditable event marks the exact time the event occurs, the account associated with that action as well as parametric details that are specific to that activity.

   The audit trails are secured from unidentified or unauthorised users. The security matrix built within the TOE will allow authorised administrators to set specific granular control to the exact groups of users who will have access to the audit trails.

c) Granular access control – the TOE provides security matrix which allows authorised administrators to specify security restrictions and awards that would make sense to their individual organisation. In the TOE, security privileges are granted by way of group association. Groups are dynamic entities within the TOE which can be created, modified and removed at any time. Each individual group created would also contain the specific permissions and privileges associated and deemed necessary by the administrator.

   Each user is associated with a group and will inherit all permissions granted to that particular group. This means that all restrictions imposed on the group would also apply to all users associated with that group.

d) Password management – the TOE allows administrator to manage and control the implementation of user passwords by specifying:

   i) password complexity: set the minimum password lengths,

   ii) expiration lengths: set the password expiration period. The TOE will keep track of user password use and expired them when the allotted time has elapsed, and

   iii) password generations: specify how many password changes will be keep track by the TOE. Users cannot reuse password that fall under the generation track.

   All user accounts (administrator or otherwise) are subject to this enforcement.

e) Session management – the TOE allows authorised administrators to set the idle timeout threshold of an active session. Authorised users will be logged out automatically from their session if their session is idle for the period that had been setup by the administrator.

f) Secure socket layer – the Console is the sole interface for user interaction. It is designed to run on a Secure Socket Layer (SSL) to ensure protection of the data transmitted. SSL is a network protocol primarily used to secure the transmission of data between 2 remote locations.

g) Import and export of configuration data – The TOE provides import and export of application specific configuration data that can be used as a medium of restoration or recovery. In this context, the term configuration data includes:

   i) Application Configuration (email, system setting, IP classes, etc)

   ii) User Security Information (Users, groups and permissions)

   iii) Device Data

   iv) Reporting Settings

   v) Real Time Threat rules

   vi) Asset Discovery configuration

h) Automated archive – the TOE allows authorised users to specify the length of period in which active data (defined as aggregated reports, rawlogs and syslogs) is to be kept on server. Data older than the span specified will be archived, encrypted and stored automatically at predetermined times. The archive files will be encrypted using AES 128-bit encryption. An MD5 checksum is generated based on the daily rawlog files. This is to ensure the integrity of the rawlogs.

i) Real time syslog collection – the TOE provides the ability for authorised users to dynamically configure the application to listen to syslog streams from network devices, servers and/or any other supported applications. Such log collection is executed real time as and when events occur.

   If the TOE detects:

   i) incoming logs originate from unknown or unregistered devices, or

   ii) logs from registered devices but cannot be processed due to packet corruption, invalid firmware version, unsupported device features, etc,

   the TOE will mark these logs as unhandled and place them in raw form to a location easily accessible to the administrator thru the Web Console GUI.

1.4.2 Physical Boundaries

12 The TOE composed of multiple software modules that run on a host computer running on Microsoft Windows operating system; minimum Microsoft XP, but preferably Server 2003 (64-bit mode). Other supporting softwares required in the operational environment of the TOE are described in Section 2.2.2 and Section 2.2.3 of the Security Target (Ref [6]).

13 Figure 1 below describes the component of Log Radar v3.2.15 that comprises the TOE.

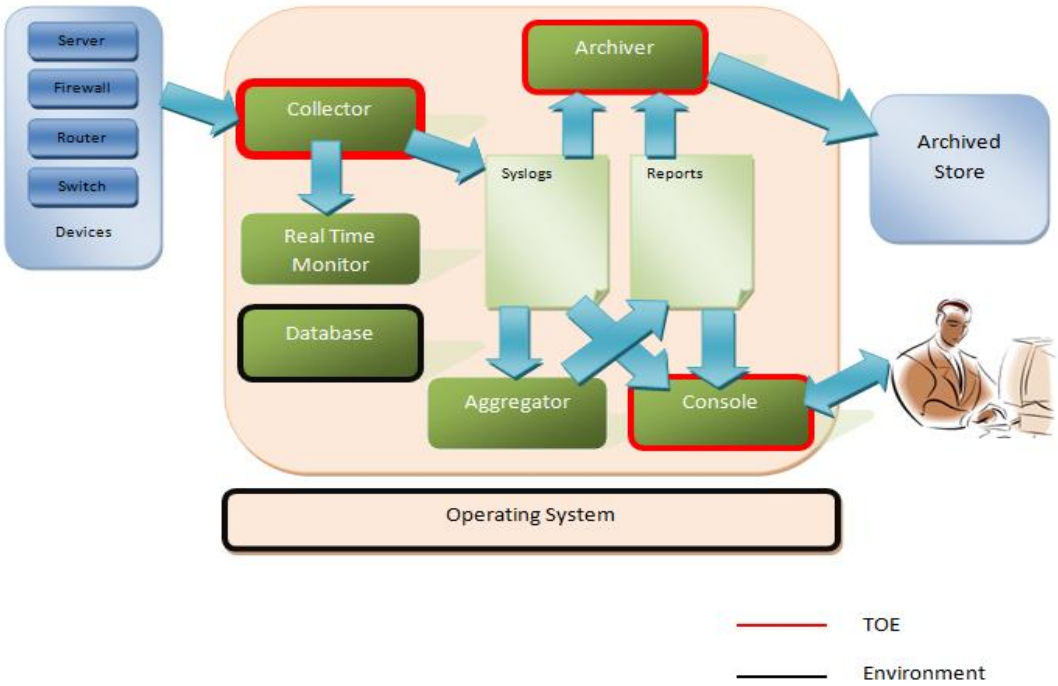

Figure 1: TOE Logical Scope

The TOE component comprises of the following:

a) **Collector** – This component act as the primary point of contact between the TOE and any input from devices. Its core function is to collect streams of data as and when they occur and process these device specific logs into a common and normalised form.

In addition to log collection and process, the Collector also determines if a data packet originates from a registered or known device. In the event the data is received from unknown or untrusted sources, the Collector would mark these logs as unhandled and place them in raw form to a location accessible by the administrator thru the Web Console GUI. In extension to this, the Collector also ensures that all data even from registered locations can be correctly understood and processed within its context. If for any reason, the data packets cannot be parsed (due to packet corruption, invalid firmware version, unsupported device features, etc), those logs are also stored in raw form in a location accessible by the administrator from the GUI.

In addition, MD5 checksums are also generated to ensure backup integrity of the rawlog folder. The configuration to save rawlogs is optional and can be configured in the Console.

b) **Console** – this component act as the interfacing point between user and TOE. This is the point in which authentication, auditing, systems security management and any other operation requiring authorised user involvement occurs. Data gathered from the user via the Console will be used by the Collector and Archiver during their respective execution cycles.

c) **Archiver** – This component function as a backup daemon. Part of the utilities extended by TOE as its log management features include the ability for a user to specify the amount of active data that is to be kept on server. Since sensitive security centric data should never be permanently deleted, the Archiver functions as a backup mechanism which will automatically archive data that surpasses set configuration to a separate location. In the process of archival, the data will be encrypted to ensure its confidentiality.

14 The Aggregator and Real Time Monitor modules are not included in the scope of the security evaluation.

15 The Security Target assumes that the host computer is to be located in a secure area that is free from physical access to unauthorised parties.

1.5 Clarification of Scope

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

17 Section 1.4 of this document described the scope of the evaluation which was limited to those claims made in the Security Target (Ref [6]). The Aggregator and Real Time Monitor modules of the LogRadar v3.2.15 are not included in the scope of the evaluation.

18 Potential consumers of the TOE are advised that some functions and services may not have been evaluated as part of the evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

19 Functions and services which are not included as part of the evaluated configuration are as follows:

a) A Hardware Server;

b) An Operating System on which the TOE is installed on;

c) A Database Software on which the TOE is dependent on as its database;

d) Other supporting software;

i) Java Virtual Machine (JVM) version 1.6.

ii) MySQL Server version 5.0.1a.

iii) Internet Browser.

1.6 Assumptions

20 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the TOE as defined in subsequent sections and in the Security Target.

1.6.1 Environment assumptions

21 Assumptions for the TOE environment listed in the Security Target are:

a) The TOE operating environment will provide reliable system time.

1.6.2 Physical assumptions

22 Assumptions for the TOE physical environment listed in the Security Target are:

a) The resources responsible for the execution process of the TOE will be located in a controlled facility; and protected from unauthorised physical access.

b) The physical hardware and software in which the TOE is deployed to will be protected from unauthorised physical modification.

1.6.3 Personnel assumptions

23 Assumptions for the TOE personnel listed in the Security Target are:

a) Only authorised administrators are granted direct connection access to the TOE within its secure physical boundary.

b) Logs in transit from the source to the TOE are secured by any means necessary. This may include, but are not limited to, trusted system administrators copying the logs from one storage media to another, or transmitted through the Internet but protected using the host computer's encryption facilities.

c) There will be an assignment of at least one single competent administrator to manage the TOE and the security of the information that it maintains.

d) Authorised administrators are not careless, negligent and malicious or in any way will adhere to procedures and guidelines specified in the TOE documentation.

e) Only authorised personnel can access the TOE.

1.7 Evaluated Configuration

24 The TOE is a software product that is installed on a host computer, in combination with an operating system (OS) and third party software applications, as described in Section 2.2.2 and 2.2.3 of the ST (Ref [6]). The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented preparative user guidance (Ref 31b)).

1.8 Delivery Procedures

25 Log Radar is delivered to the user using the procedure described in the Delivery Procedure (Ref 31c)) which ensures that Log Radar is securely transferred from development environment into the responsibility of the user. The delivery procedures are outlined below.

26 The LogRadar is copied from the development machines of TecForte by trusted TecForte personnel, and stored on read-only CD media. The CD media is placed in a sealed and marked envelope, and is then passed to the trusted TecForte personnel for delivery.

27 The LogRadar is stored only on read-only Compact Discs (CD) media by trusted TecForte personnel, and is not made accessible to anyone else without proper authorisation.

28 LogRadar will be delivered from TecForte office to the end-user site in a physically secure manner, by having only trusted and authorised TecForte employees carry the TOE.

29 The LogRadar is then installed by either TecForte personnel, or the end-user. Upon completion of the installation, a User Acceptance Test is provided.

1.9 Documentation

30 To ensure continued secure usage of the product, it is important that the Log Radar is used in accordance with guidance documentation.

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

a) Log Radar v3.2.15 (with modules Console, Collector and Archiver) Operational User Guidance EAL2, version 1.0, 11 August 2010

b) Log Radar v3.2.15 (with modules Console, Collector and Archiver) Preparative Procedures EAL2, version 1.0, 11 August 2010

c) Log Radar v3.2.15 (with modules Console, Collector and Archiver) Delivery Procedures EAL2, version 1.1, 12 November 2010

2 Evaluation

32 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 (EAL2). The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

34 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

35 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

36 The evaluators analysed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces (TSFIs), and how the TSF implements the security functional requirements (SFRs).

37 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

38 The evaluators examined the TOE security architecture description; they 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.

2.1.3 Guidance documents

39 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

2.1.4 IT Product Testing

40 Testing at EAL2 consists of assessing developer tests, perform independent function test, and perform penetration tests. The TOE testing was conducted at CyberSecurity Malaysia MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of Developer Tests

41 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).

42 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

43 Independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a sample of the developer's test plan, and creating test cases that augmented the developer tests.

44 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 developed and performed by the evaluators to verify the TOE functionality as follows:

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
Test Group A comprises a series of test cases on TOE security functions of web based for **audit records generation and**	Security Audit	1) Audit Trail Page 2) IP Classes Page	**PASS**. Result as expected.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
time stamp for relevant authentication and management events.			
Test Group B comprises a series of test cases on TOE security functions of identification and authentication. Password encryption using SHA-1 when saved into the database.	Identification and Authentication	**User Administrator TSFI** 1) Login Page 2) User Page 3) Add New User Page 4) Settings Page	**PASS**. Result as expected.
Test Group C comprises a series of test cases on TOE security functions of how the TOE control access and privilege for each user, manage and control the implementation of user passwords	Granular Access Control List Password Management	**User Administrator TSFI** 1) Add New User Group Page 2) Edit User Group Page **User Administrator TSFI** 1) Change Password Page 2) Email Page 3) Settings Page	**PASS**. Result as expected.
Test Group D comprises a series of test cases on TOE security functions of **monitoring user session** in web portal.	Sessions Management	**Configuration TSFI** 1) Settings Page	**PASS.** Result as expected.
Test Group E comprises a series of test cases on TOE security function to - Automatically archive the aggregated reports, rawlogs, syslogs and encrypted using AES 128-bit encryption. - MD5 checksum is generated based on the daily Rawlog files. - Secure	Automated Archive Secured Socket Layer	**User Administrator TSFI And Syslog TSFI** 1) Login Page 2) Change Password Page 3) Change Password Page 4) User Page 5) Add New User Page	**PASS.** Result as expected.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
communication between TOE and remote user		6) Edit User Page 7) Add New User Group Page 8) Edit User Group Page 9) Audit Trail Page 10) Email Page 11) Settings Page 12) IP Classes Page 13) Intranet Page 14) Backup Configuration Page 15) Data Backup Page 16) Data Transfer Page 17) Device Page 18) Add New Device Page 19) Edit Device Page 20) Device Group Page 21) Add New Device Group Page 22) Edit Device Group Page 23) Add New Branch Page 24) Edit Branch Page 25) Unhandled Logs Page 26) SSL API	
Test Group F comprises a series of test cases on TOE security functions to **dynamically configure**	Real Time Syslog Collection	**Configuration TSFI** 1) Backup Configuration Page	**PASS**. Result as expected.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
Real Time Syslog Collection.		2) Data Backup Page **Syslog TSFI** 1) Intranet Page 2) Data Transfer Page 3) Device Page 4) Add New Device Page 5) Edit Device Page 6) Device Group Page 7) Add New Device Group Page 8) Edit Device Group Page 9) Add New Branch Page 10) Edit Branch Page 11) Unhandled Logs Page	

45 All tests performed by the evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration Testing

46 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, TOE design, and security architecture description.

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

48 The penetration tests focused on:

a) Generic vulnerabilities;

b) Bypassing;

c) Tampering; and

d) Direct attacks.

49 The results of the penetration testing note that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment.

2.1.4.4 Testing Results

50 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

3 Results of the Evaluation

51 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 Log Radar performed by the CyberSecurity Malaysia MySEF.

52 The CyberSecurity Malaysia MySEF found that Log Radar 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 EAL2.

53 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. This risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

54 EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

55 The analysis is supported by 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 penetration attackers with a basic attack potential.

56 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

57 In addition to ensure secure usage of the product, below are additional recommendations for Log Radar consumers:

a) Manage the password securely by ensure the complexity of the password and frequently change the password;

b) Use the product only in its evaluated configuration; and

c) Ensure strict adherence to the delivery procedures.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[4] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1, December 2009.

[6] LogRadar Security Target, Version 1.0R, 15 January 2013

[7] Evaluation Technical Report Log Radar v3.2.15, Version 1.4, 14 January 2013

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
ACL	Access Control List
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
GUI	Graphical User Interface
IEC	International Electrotechnical Commission
ISCB	Information Security Certification Body
ISO	International Standards Organisation
JVM	JAVA Virtual Machine
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

Acronym	Expanded Term
RTM	Real Time Monitor
ST	Security Target
TOE	Target of Evaluation
TSFI	TOE Security Functions Interface

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
Authorised user	A term used to describe all users that interact with the TOE that have a unique identifier. This includes the non-privileged set of users and all others within the administrator groups.
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.
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.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.

Term	Definition and Source
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.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User data	Data created by and for the user that does not affect the operation of the TSF.

--- END OF DOCUMENT ---