Log Radar Security Target

Jan

2012

This document details Security Target definition for Log Radar's compliance with Commons Criteria

v 1.0R

Amendment History

Version	Date	Status	Change Description
1.0a	5th October 2009	Draft	Initial version
1.0b	7th December 2009	Draft	• Increased ST evaluation scope • Redesigned logical scope diagram • Reformatted SFR notation • Added sections 2.3.3 and 2.3.4 • Reviewed section 7.2 for correct EAL2 compliance • Added new extended components SYS_COL.1 and SYS_COL.2
1.0c	11th January 2010	Draft	• Corrected ST date marker • Corrected document convention in Section 1.1 • Added new term definitions for better clarity in Section 2.3.1 • Corrected TOE SAR in Section 7.3 • Added Section 9.2.2 for Organizational Policies – Security Objective mapping
1.0d	18th January 2010	Draft	• Corrected ST version in Section 2.1 • Included notes for functions not included in TOE scope in Section 2.3.2 for better clarity • Corrected misc format and component issues in Section 7.2 • Reworked TOE Summary Specification in Section 8.1 • Corrected dependency inaccuracies in Section 9.3.2
1.0e	29th January 2010	Draft	• Corrected dependency declaration error in Section 7.2.13 • Corrected typo error in Section 7.3 • Added new items into Section 8.1 to cover all declared SFRs • Added FMT_MSA.1 and FMT_MSA.3 previously missing from Section 8.2 • Corrected mapping inaccuracies and inconsistencies in Section 9.2 • Corrected mapping errors in Section 9.3
1.0f	3rd February 2010	Draft	• Corrected mapping error for A.REM_OPER in Section 9.3.1
1.0g	22nd March 2010	Draft	• Edited by Drexx Laggui <Drexx@Laggui.com> • Updated with minor typographical fixes • Updated descriptions of TOE Type, as well as physical and logical scope of TOE • Deleted O.TMSTMP, correction on OE.TMSTMP, and added A.TIME, to satisfy FPT_STM.1 • Deleted O.SECRMT • Completed the mapping of O.EXPORT to (new) T.DLOSS, and to relevant SFRs
1.0h	1st April 2010	Draft	• Edited by Drexx Laggui Drexx@Laggui.com • Updated with minor typographical fixes • Updated descriptions of TOE Type, as well as

			physical and logical scope of TOE • Deleted O.TMSTMP, correction on OE.TMSTMP, and added A.TIME, to satisfy FPT_STM.1 • Deleted O.SECRMT • Completed the mapping of O.EXPORT to (new) T.DLOSS, and to relevant SFRs
1.0i	2nd April 2010	Draft	• Edited by Drexx Laggui Drexx@Laggui.com • Added mapping for A.TIME in Section 9.3.1
1.0j	01st Jul 2010	Draft	• Corrected titles for sections 5.2.1 and 5.2.2. • Reformatted mapping in section 9.3.1. • Added "Authorized users" in Terminology section.
1.0k	06th Jul 2010	Draft	• Changed ST authorship to Drexx Laggui <Drexx@Laggui.com> • Replaced extended components SYS_COL.1 & SYS_COL.2, and replaced with FDP_IFF & FDP_IFC, thus editing related or dependency statements
1.0L	23rd Aug 2010	Draft	• Edited by Leong Wei Khuan wkhuan@tecforte.com • Refinement assignment of section 7.2.1.a • Added application notes for FAU_SAR.1 (section 7.2.3). • In sections 7.2.6 for FPT_ETC.2.4, and 7.2.9 for FPT_ITC.2.5, changed "no additional rules" to "none." • Set "[1-10]" for FIA_AFL.1 in section 7.2.10. • Clarified the assignment of authorized user roles for FMT_MOF.1.1 and FMT_SMR.1.1.
1.0m	12th Oct 2010	Draft	• Edited by Leong Wei Khuan wkhuan@tecforte.com • In section 7.2.1a, replaced “Start up and shutdown of the audit functions” to “none”. • Refined assignment to refer to Table1 in Appendix (section 7.2.5) • Minor changes to FPT_ETC 2.1 & FPT_ITC.2 (section 7.2.6 & 7.2.9) • Added in range 1-10 into FIA_AFL 1.1 (section 7.2.10) • Referred assignment of functions of FMT_MOF1.1 to Table 1 in Appendix (7.2.14) • Edited FMT_MSA 1.1 to refer to Table 1 in Appendix (section 7.2.15) • Replaced the authorised identified roles with “Administrator and User Defined roles”. • Refined assignment of section 7.2.17 and added application notes for FMT_REV. • Listed the security management functions in FMT_SMT 1.1 (section 7.2.19). • Clarified the assignment of authorized user roles for FMT_SMR1.1 (section 7.2.20). • Removed FPT_TDC from the whole document. • Added application notes for FDP_ACF.1 (section

			7.2.23) • Added in "The roles they are assigned into," into FDP_ACF 1.1 (section 7.2.23) • Added application notes for FRU_SRA.1 (section 7.2.24). • Updated with minor formatting issues • Added Access Control List by Roles table & Security Attributes List by Roles table into Appendix
1.0n	30th Nov 2010	Draft	• Edited by Leong Wei Khuan wkhuan@tecforte.com • Added Cryptography AES, MD-5 and SHA-1 as Security Functions • Rearranged Security Functions • Added Security Objectives Rationale relating to SFRs table (section 9.2.2) • Fixed formatting • Changed FDP_ITC & FPT_ETC to FPT_ITC & FPT_ETC • Amend FPT_FMT and mapping accordingly
1.0p	31 July 2012	Draft	• Edited by Leong Wei Khuan • Incorporated comments from MyCB
1.0q	25 Sept 2012	Final	• The harmonisation issue where most of the CCES members said that this should be recognize as extended SFR not refinement.
1.0r	15 Jan 2013	Final	• The relocation of FCS_COP.1(3)

Table of Contents

Log Radar Security Target

This document details Security Target definition for Log Radar's compliance with Commons Criteria

1.0 Document introduction

1.1 Document Conventions

The following conventions have been applied in this document:

Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, and iteration.

1. The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold underline text**.

2. The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by italicized text in square brackets, [*selection value*].

3. The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment value].

4. The iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration number).

1.2 Terminology

Acronym	Meaning
ACL	Access Control List
Authorized 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.
CC	Common Criteria
DOS	Denial of Service
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
JVM	JAVA Virtual Machine
LR	Log Radar
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirements
SFR	Security Functional Requirements

ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
TSS	TOE Summary Specification
TSC	TSF Scope of Control
RTM	Real Time Monitor

1.3 References

- Common Criteria Part 1 Version 3.1 Revision 3
- Common Criteria Part 2 Version 3.1 Revision 3
- Common Criteria Part 3 Version 3.1 Revision 3
- Common Methodology for Information Technology Security Evaluation (CEM) version 3.1 Revision 3

1.4 Document Organization

This ST contains:

- TOE Description: Provides an overview of the TOE security functions and describes the physical and logical scope for the TOE
- TOE Security Problem Definition: Describes the threats, organizational security policies, and assumptions that pertain to the TOE and the TOE environment.
- TOE Security Objectives: Identifies the security objectives that are satisfied by the TOE and the TOE environment.
- TOE Security Functional Requirements: Presents the Security Functional Requirements (SFRs) met by the TOE
- TOE Security Assurance Requirement: Presents the Security Assurance Requirements (SARs) met by the TOE
- TOE Summary Specification: Describes the security functions provided by the TOE to satisfy the security requirements and objectives
- Rationale: Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability

2.0 Introduction

2.1 ST and TOE Reference

ST Title	Log Radar Security Target
ST Version	1.0R
TOE Identification	Log Radar v3.2.15, with modules Console, Collector and Archiver
CC Identification	Common Criteria v3.1 Revision 3
Assurance Level	EAL2
ST Author	Leong Wei Khuan
Keyword	SIEM

2.2 TOE Overview

Log Radar is a tool used in the arena of Security Information and Event Management (SIEM). 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, normalize, process and manage such information from a real time context. Log Radar uniquely provides real-time monitoring of system changes and user activity, detection of threats and intrusions, security information management and correlation and log management -all with a single, integrated and scalable system. The following image illustrates the scenario:

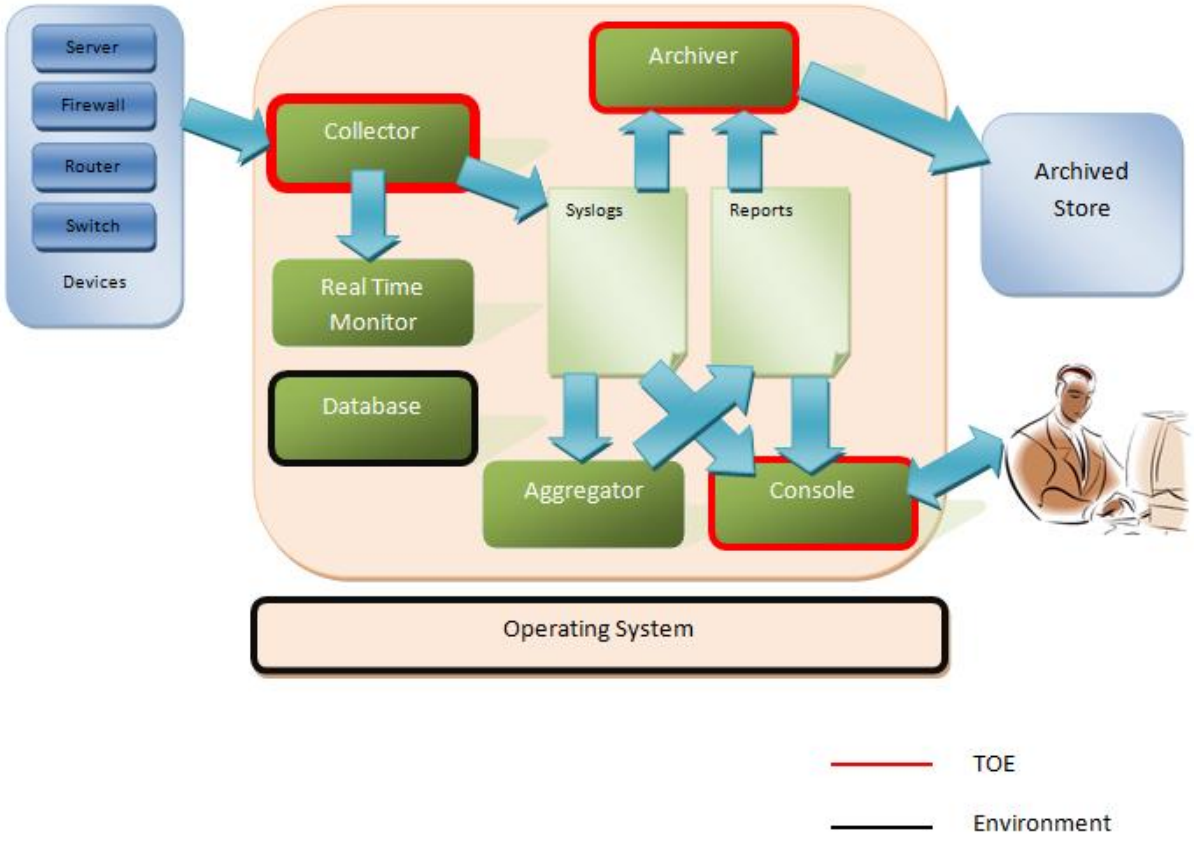

Fig 1

The TOE provides a centralized security management console to track security events throughout the enterprise security infrastructure. Its robust normalization and correlation engines are able to process massive amounts of security information and cryptic codes - generated by wide array of disparate security devices (Firewall, VPN, IDS& IPS, Anti-Virus Server, Anti-Spam Server, Web Filter and UTM Appliance) - into a clear, easy-to-understand report. The TOE is able to classify each security event in real-time and instantly pinpoint the physical location of an asset or business processes it secures. This allows administrator to produce “readable” high-level management reports and construct rules based on the asset and its location.

The TOE is specific and confined to the context of Log Radar’s web console which acts as the primary interface to the end user, as well as its Collector and Archiver modules which acts as the primary elements within LogRadar’s log management operation. As the module central to all user interactions, the web console has an inherent link to most other modules within the Log Radar suite. These points of interface occur in various forms and according to functions. Items pertinent to the context of this document will be defined in later sections. On the flip side, the Collector and Archiver has almost no direct user interaction and acts as background daemons that will process the necessary data based on user specifications and settings collected by the Console from the user.

2.2.1 TOE Type

The TOE is an automated tool used on enterprise data networks to centralize the storage and interpretation of logs, or events, generated by other devices or applications.

The TOE belongs to the "**Detection Devices and Systems**" category.

While Log Radar maintains its recommended and minimum hardware requirements, the context of this TOE should be evaluated as a software product. Log Radar’s console is types as a web application and can be accessed thru supported web browsers. The Collectors and Archiver as deployed as windows services which will execute and operate based on parameters and configurational settings as specified by the user thru the use of the LR Console.

2.2.2 Required non-TOE hardware, software, or firmware

The TOE is software product that is run on a host computer. The host computer must run the operating system platform on which the TOE can execute.

The minimum operating system (O/S) and hardware requirements for the host computer are:

O/S:	Microsoft XP, preferably Server 2003 64-bit, or better
CPU:	Intel Pentium Core 2 Duo 2.2 GHz, or faster
RAM:	At least 2GB, preferably 4GB
Connectivity:	TCP/IP network interfaces
Disk space for TOE:	At least 390 MB

Disk space for logs: Subject to traffic volume and log rotation policy

2.2.3 Operating Environment

This section describes the general environment in which the TOE is expected to perform. The environment of operation for the TOE is expected to be a facility that is physically secure from unauthorized intrusion. Personnel with explicit physical access to the hardware storing log data and application execution files must be authorized, trained and competent. In addition to this:

- The operational environment must include a web browser (Internet Explorer 6.0 or higher, or Mozilla Firefox 2.0 or higher) to be used by authorized administrators of the TOE as a medium of communication with the TOE's web GUI.
- The operational environment must include a Java Virtual Machine (JVM) versioned 1.6
- The operational environment must include the database MySQL 5.0.1a
- The operational environment must include either Windows 2003 or Windows 2008

At a minimum, a monitor, keyboard and mouse must be locally collected to the server machine in which the TOE is deployed or operated on.

2.3 TOE Description

2.3.1 Physical scope of the TOE

The TOE is composed of multiple software modules that run as a complete IT product on a required host computer. The host computer must run with an operating system platform on which the TOE executes. The TOE can be installed on host computers running Microsoft Windows Server 2003 (64-bit mode).

Please refer to Fig. 1 for a graphical representation of the scope and the points of interaction between the various components of the TOE.

2.3.2 Logical scope of the TOE

This section describes the logical security features of the TOE.

The TOE consists of 3 components, namely the Console, the Collector and the Archiver. All 3 components are designed to operate independently of the other, each fulfilling its own roles while contributing to LogRadar's common goal. This goes to say that each component is able to carry out its functions even in the event of a failure from any of the other 2 modules.

Collector

The 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 normalized form (termed Normalized Logs in LogRadar's context). 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 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 easily accessible to 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 to this, MD5 checksums are also generated to ensure backup integrity of the Rawlog folder. The configuration to save Rawlogs are optional and can be configured in the Console.

Console

The Console acts as the interfacing point between user and TOE. It is important to note that within the context of this TOE, the Console is the only point of interaction between user and the solution. As such, this is the point in which authentication, auditing, systems security management - and any other operation requiring user involvement – occurs. Data gathered from the user via the Console will be used by the Collector and Archiver during their respective execution cycles.

Archiver

The 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 (which is also user defined). In the process of archival, the said data goes thru both a series of compression and AES 128-bit encryption to ensure its confidentiality.

The Aggregator and Real Time Monitor functions are not included in the TOE scope for this ST. The security specific functions that would be evaluated in logical terms are:

2.3.3 Identification and Authentication

The TOE provides an identification and authentication layer independent from that of the Operating System it executes on. This security feature acts to protect and prevent access by unauthorized users to the system. In addition, it will also require each user to be identified and authorized first before any access to protected functions and data is granted. In the case of an authentication or identification failure, the TOE will disregard any request made an issue a forward redirection to the login page.

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. In addition to this, the system administrator can also manage authentication failure tolerance. 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, the password will be encrypted using SHA-1 when saved into the database.

2.3.4 Security Audit

The TOE provides for a comprehensive auditing layer which will monitor activities and executions occurring with 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 parameteric details that are specific to that activity.

As with most things within the TOE, the audit trails are secured not only to unidentified users but also unauthorized users as well. The security matrix built within the TOE will allow authorized administrators to set specific granular control to the exact groups of users who will have access to the audit trails.

2.3.5 Granular Access Control

The TOE provides a fluid and flexible security matrix which allows authorized administrators to specify security restrictions and awards that would make sense to their individual organization. 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.

In turn, each user is associated with a group and will inherit all permissions granted to that particular group. Needless to say, all restrictions imposed on the group would also apply to all users associated with that group.

2.3.6 Password Management

The TOE allows for the administrator to manage and control the implementation of user passwords. This in effect means that the system administrator is able to specify password complexity, expiration lengths as well as password generations.

Password complexity allows the administrator to set minimum password lengths while password expiration period means that the TOE will keep track of user password use and expire them when the allotted time has elapsed. Once expired, the users would be required to change their password before then can continue system use. Password generation tracking will also specify how many changes of passwords the TOE will keep track of. Users cannot reuse password that fall under the generation track. All user accounts (administrators or otherwise) are subject to these enforcements.

2.3.7 Sessions Management

The TOE allows for the management of sessions connection. Authorized administrators are granted the ability to set the idle timeout threshold after which an authorized user would be automatically logged out of his active session. Idle timeout is defined as a period of inactivity from the user.

2.3.8 Socket Layer

The Console portion of the TOE; being the sole interface of user interaction is designed to run on a Secure Socket Layer. SSL is a network protocol primarily used to secure the transmission of data between 2 remote locations; essentially providing protection for intercept when data packets are flowing “on the wire”.

2.3.9 Import and Export of Configuration Data

The TOE provides for the import and export of application specific configuration data. Such data exported can be used as a medium of restoration or recovery. In this context, the term configuration data includes:

- Application Configuration (Email, system settings, IP Classes, etc)
- User Security Information (Users, groups and permissions)
- Device Data
- Reporting Settings
- Real Time Threat rules
- Asset Discovery configuration

2.3.10 Automated Archive

The TOE allows authorized users to specify the length of period in which active data is to be kept on server. Data (defined as aggregated reports, rawlogs and syslogs) older than the span specified will then be archived, encrypted and stored automatically at predetermined times. On top of it, the files will be encrypted using AES 128-bit encryption.

On the other hand, an MD5 checksum is generated based on the daily Rawlog files. This is to ensure the integrity of the rawlogs.

2.3.11 Real Time Syslog Collection

LR provides the ability for authorized 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.

3.0 Conformance Claims

3.1 Common Criteria Claims

The following conformance claims are made for the ST:

- CCv3.1 Rev.3 conformant. The ST is Common Criteria conformant to Common Criteria version 3.1 Revision 3.
- Part 2 conformant. The ST is Common Criteria Part 2 extended.
- Part 3 conformant. The ST is Common Criteria Part 3 conformant.
- Package conformant. The ST is package conformant to the package Evaluation Assurance Level EAL2

This ST makes no conformance claims to any available PP.

4.0 TOE Security Problem Definitions

The TOE described is designed to execute in an infrastructural environment that has at least a basic level of robustness. Authorized users of the TOE are assumed to be cleared for all information and data pertaining to the network infrastructure in which the TOE monitors.

4.1 Assumption

Assumptions made for the TOE are as follows:

4.1.1 Environmental Assumptions

A.TIME The TOE operating environment will provide reliable system time

4.1.2 Physical Assumptions

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

A.PROTCT The physical hardware and software in which the TOE is deployed to will be protected from unauthorized physical modification.

4.1.3 Personnel Assumptions

A.DIRECT Only authorized administrators are granted direct connection access to the TOE within its secure physical boundary.

A.INTEGR 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.

A.MANAGE 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.

A.NOEVIL Authorized administrators are not careless, negligent, malicious or in any way harbour ill will and will adhere to procedures and guidelines specified in the TOE documentation.

A.NOTRST Only authorized personnel can access the TOE.

4.2 Threats

Threats to the TOE are as follows:

T.COMINT An unauthorized entity may compromise the integrity, correctness, and confidentiality of data that is collected, stored, aggregated or analyzed by the TOE by means of a security bypass.

T.DLOSS A malicious or accidental event, either by known or unknown attackers, could destroy sensitive security-centric data.

T.IMPCON Authorized or unauthorized users could jeopardize TOE functions thru means of improper or incorrect configuration settings.

T.INFLUX An unauthorized user could attempt to jeopardize TOE functions thru means of an influx of data or thru DOS attacks.

T.INSECUSE Authorized or unauthorized users administer the TOE in an unsecured manner causing disruption or discloser of data that is collected, stored, aggregated or analyzed.

T.INTEGR An unauthorized user could attempt to modify data while in transit from devices in the infrastructure to the TOE.

T.LOSSOF An unauthorized user could attempt to destroy data that is collected, stored, aggregated or analyzed by the TOE by means of a security bypass.

T.NOHALT An unauthorized user could attempt to end the execution of the TOE.

T.PRIVIL An unauthorized user could attempt to gain access data that is collected, stored, aggregated or analyzed by the TOE by means of exploiting system privileges.

T.UNATHDVCE An unauthorized device could attempt to jeopardize TOE functions thru means of an influx of data or thru DOS attacks.

4.3 Organizational Security Policies

Organizational security policies are as follows:

P.ACCACT All authorized users of the TOE must be accountable for their actions.

P.ACCESS All data collected, stored, aggregated or analyzed by the TOE should only be used for authorized purposes.

P.INTGTY All data collected, stored, aggregated or analyzed by the TOE should be protected from modification.

P.MANAGE The TOE should only be administered by authorized users.

P.PROTCT The TOE must be protected from unauthorized entries as well as disruptions of normal application execution.

5.0 TOE Security Objectives

5.1 Security Objective for the TOE

This section defines the security objectives in which the TOE and its supporting environment is designed to meet. These objectives not only illustrate the role but the contractual responsibility of the TOE in meeting these requirements.

5.1.1 Security objectives for the TOE

O.PROTCT The TOE must be capable of protecting itself from unauthorized access and authorized modification of both its functions and data.

O.EADMIN The TOE must be capable of providing feature sets that will allow for effective management of both its functions and data.

O.ACCESS The TOE must be capable of restricting authorized users to functions and/or data that is appropriate for their role or access level.

O.IDAUTH The TOE must be capable of identifying and authorizing users before any access to functions or data is granted.

O.AUDITS The TOE must be capable of auditing records of data access, and function execution for all events occurring within its scope.

O.INTEGR The TOE must be capable of ensuring the integrity of all data collected, stored, aggregated or analyzed.

O.EXPORT The TOE must be capable of exporting and importing data specific to the TOE for the purpose of backup, restoration and/or archival purposes.

5.1.2 Security objectives for the operational environment

OE.INSTAL All personnel responsible for the TOE must ensure that it is deployed, administered and operated within all guidelines of IT security.

OE.PHYCAL All personnel responsible for the TOE must ensure the threat of physical attack against parts of the TOE critical to all security policies, are sufficiently safeguarded at all times.

OE.PERSON All personnel playing the role of administrator of the TOE must be adequately trained to manage the solution.

OE.INTEGR All personnel responsible for administering the TOE must ensure that all measures required to secure the TOE's operating environment to protect the integrity of the data in transit have already been taken.

OE.OFLOWS The IT Environment must appropriately handle potential audit and defence perspective data storage overflows, through the IT Environment's interfaces

OE.TMSTMP The TOE operating environment must provide a reliable time source for the TOE to provide accurate timestamps for audit records

6.0 Extended components definition

This Security Target introduces one extended component: FAU_GEN.3 Simplified audit data generation. This component is a simplified version of FAU_GEN.1 and is therefore a suitable member of the FAU_GEN family. It was added to remove the need to log start and stop of auditing and to simplify the requirement.

6.1 FAU_GEN.3 Simplified audit data generation

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.3.1 The TSF shall be able to generate an audit record of the following auditable events:

a) [

- General: User login, logout
- Dashboard: View dashboard and event summary; downloading summary logs, statistic logs and statistics drilldown
- User administration: Change, reset or updating of passwords; viewing and searching of user lists and user details; creating, updating or deleting users; viewing, creating, updating or deleting groups; viewing or searching of audit trails and audit trail archives; downloading of audit information, deleting audit trail files
- Configuration: viewing, testing and saving systems configuration; saving and restoring system settings; view, create, update and deleting IP classifications; viewing and saving intranet settings; viewing, backup or restoring LR configuration files; searching and restoring archived files; view, update and initiating data transfer
- Device Management: viewing, searching, creating, updating and deleting devices; viewing, searching, creating, updating and deleting device groups;
- Branch Management: viewing, creating, updating and deleting braches; initiating branch data processing
- Log Analytics: viewing, searching, creating, updating, duplicating, exporting, deleting log analytics, analyzing log analytics results
- Asset Discovery: viewing asset list; viewing, creating, detecting asset information; viewing, updating asset discovery configurations; initiating and stopping asset discovery scans;
- Real Time Threats: viewing, creating, modifying, duplicating and deleting rules; viewing, creating, modifying, activating, deactivating and duplicating correlation; viewing correlation trigger list and report; exporting and deleting trigger reports; viewing, creating, modifying, deleting IP list; viewing, creating, modifying and deleting port details; viewing, creating, updating and deleting keywords
- Reporting: viewing, creating, modifying, deleting automated reports; viewing, creating,

modifying, deleting schedule; downloading and deleting generated reports; editing report filter based on date range, device ip(s) and ip classification; viewing and downloading on-demand or compliance reports

- Unhandled logs: viewing, downloading and deleting unhandled logs; blocking and unblocking devices

]

FAU_GEN.3.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no additional audit information].

7.0 IT Security Requirements

7.1 Overview

This section highlights the TOE security functional as well as assurance requirements. Additionally, all other environmental functional dependencies for the TOE will also be described.

7.2 TOE Security Functional Requirements

The security functional requirements for the TOE in reference to various components described by CC are summarized below:

No.	Component	Component Name
1.	FAU_GEN.3	Simplified audit data generation
2.	FAU_GEN.2	User identity association
3.	FAU_SAR.1	Audit review
r	FAU_SAR.2	Restricted audit review
5.	FDP_ACC.2	Complete access control
6.	FDP_ACF.1	Security attribute-based access control
7.	FPT_ETC.2	Export of user data with security attributes
8.	FDP_IFC.1	Subset information flow control
9.	FDP_IFF.1	Simple security attributes
10.	FPT_ITC.2	Import of user data with security attributes
11.	FIA_AFL.1	Authentication failure handling
12.	FIA_UAU.2	User authentication before any action
13.	FIA_UID.2	User identification before any action
14.	FIA_SOS.1	Verification of secrets
15.	FMT_MOF.1	Management of security functions behaviour
16.	FMT_REV.1	Revocation
17.	FMT_MSA.1	Management of security attributes
18.	FMT_MSA.3	Static attribute initialisation
19.	FMT_SAE.1	Time-limited authorisation
20.	FMT_SMF.1	Specification of management functions
21.	FMT_SMR.1	Security roles
22.	FTA_SSL.3	TSF-initiated termination
23.	FTP_TRP.1	Trusted path
24.	FRU_RSA.1	Maximum quotas
r	FCS_COP.1(1)	Cryptographic Operation (AES)
26.	FCS_COP.1(2)	Cryptographic Operation (MD5)
27.	FCS_COP.1(3)	Cryptographic Operation (SHA-1)

7.2.1 FAU_GEN.2 User identity association

Hierarchical to: No other components.
Dependencies: FAU_GEN.3 Simplified audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

7.2.2 FAU_SAR.1 Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.3 Simplified audit data generation

FAU_SAR.1.1 The TSF shall provide [users belonging to all roles explicitly granted with read access to the audit trail] with the capability to read [all audit information and audit information] from the audit records.

Application Note: Audit information includes the date, time, username, and actions performed by all the respective users.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

7.2.3 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

7.2.4 FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1 Subset access control
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the [Access Control List] on [Administrators and User Defined roles performing operations as defined in Table 1] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

7.2.5 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [Access Control List] to objects based on the following: [The roles they are assigned into, for modules Asset Discovery, Branch Management, Configuration, Dashboard, Device Management, License Management, Log Analytics, Real Time Threats, Reporting, Unhandled Log, User Administration].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [checks against a user role and permissions allowed].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [permissions granted to roles and roles which users play].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [should the user play roles which have insufficient permission to access with a data fragment or a TOE function].

Application note: For the complete Access Control List, refer to Appendix Table 1.

7.2.6 FPT_ETC.2 Export of user data with security attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FPT_ETC.2.1 The TSF shall enforce the [Access Control List] when exporting user data, controlled under the SFP(s), outside of the TOE.

FPT_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FPT_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FPT_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: [none].

7.2.7 FDP_IFC.1 Subset Information Flow Control

Hierarchical to: No other components

Dependencies: FDP_IFF.1 Simple Security Attributes

FDP_IFC.1.1 The TSF shall enforce the [syslog collection SFP] on

[

Subjects: Any computer or network device that generate syslog messages

Information: TCP/IP network packets that contain syslog messages

Operations: Receive information

].

7.2.8 FDP_IFF.1 Simple Security Attributes

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [syslog collection SFP] based on the following types of subject and information security attributes:

[

Subject security attribute: IP address of source computer or network device

Information security attribute: Destination transport and port number

].

FDP_IFF.1.2 The TSF shall permit an information flow between a ~~controlled~~ **source** subject and ~~controlled information~~ **destination subject** via a controlled operation if the following rules hold:

[

a) Destination IP addresses = any IP address of host computer

b) Destination protocol = UDP or TCP (Default is UDP)

c) Destination port number = 1 to 65,535 (Default is 514)

d) Source IP address = Any valid source IP address as enabled in the rules

].

FDP_IFF.1.3 The TSF shall enforce the

[

a) rule that if incoming syslog messages cannot be processed by the regular expression processor, then store syslog messages in an unprocessed log file

b) rule that if incoming syslog messages can be processed by the regular expression processor, then process the logs

].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

[

a) Source IP address = Any IP address included in the ignore list

].

Application note: This component defines the requirement for the management of syslog input and processing that takes place under TSF control. This states the method of response to anomalous situations arising from the input and processing of syslog so as to maintain data correctness and ensure TDF continuity.

7.2.9 FPT_ITC.2 Import of user data with security attributes

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FTP_TRP.1 Trusted path

FPT_ITC.2.1 The TSF shall enforce the [Access Control List] when importing user data, controlled under the SFP, from outside of the TOE.
FPT_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.
FPT_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FPT_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FPT_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [none].

7.2.10 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*an administrator configurable positive integer within the range 1-10*] unsuccessful authentication attempts occur related to [user login and authentication].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [suspend the said account from further use].

7.2.11 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.2.12 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

7.2.13 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [complexity requirements as defined in the organization's administrator guidance].

7.2.14 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behaviour of*] the functions [as defined in Appendix,Table 1. Access Control Lists by Roles] to [Administrator or User Defined roles].

7.2.15 FMT_REV.1 Revocation

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the [*User*] under the control of the TSF to [Administrator or User Defined Roles with the necessary privilege].

FMT_REV.1.2 The TSF shall enforce the rules [the enforcement of security attribute changes shall take place immediately and affects the user during the next login].

Application note: Administrator has access to revoke the access rights by default. User Defined roles can also be given this privilege to revoke access rights of other users.

7.2.16 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [Access Control List] to restrict the ability to [view or perform operations specified in the Management of Security Attributes column in Appendix, Table 1] the security attributes [as mentioned in Appendix, Table 2] to [Administrator and User Defined roles].

7.2.17 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [Access Control List] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Administrator and User Defined roles] to specify alternative initial values to override the default values when an object or information is created.

7.2.18 FMT_SAE.1 Time-limited authorisation

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FPT_STM.1 Reliable time stamps

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [user passwords] to [authorized administrative roles].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [enforce password change] after the expiration time for the indicated security attribute has passed.

7.2.19 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [-
General: User login, logout
- Dashboard: View dashboard and event summary; downloading summary logs, statistic logs and statistics drilldown
- User administration: Change, reset or updating of passwords; viewing and searching of user lists and user details; creating, updating or deleting users; viewing, creating, updating or deleting groups; viewing or searching of audit trails and audit trail archives; downloading of audit information, deleting audit trail files
- Configuration: viewing, testing and saving systems configuration; saving and restoring system settings; view, create, update and deleting IP classifications; viewing and saving intranet settings; viewing, backup or restoring LR configuration files; searching and restoring archived files; view, update and initiating data transfer
- Device Management: viewing, searching, creating, updating and deleting devices; viewing, searching, creating, updating and deleting device groups;
- Branch Management: viewing, creating, updating and deleting braches; initiating branch data processing
- Log Analytics: viewing, searching, creating, updating, duplicating, exporting, deleting log analytics, analyzing log analytics results
- Asset Discovery: viewing asset list; viewing, creating, detecting asset information; viewing, updating asset discovery configurations; initiating and stopping asset discovery scans;
- Real Time Threats: viewing, creating, modifying, duplicating and deleting rules; viewing, creating, modifying, activating, deactivating and duplicating correlation; viewing correlation trigger list and report; exporting and deleting trigger reports; viewing, creating, modifying, deleting IP list; viewing, creating, modifying and deleting port details; viewing, creating, updating and deleting keywords
- Reporting: viewing, creating, modifying, deleting automated reports; viewing, creating, modifying, deleting schedule; downloading and deleting generated reports; editing report filter based on date range, device ip(s) and ip classification; viewing and downloading on-demand or compliance reports
- Unhandled logs: viewing, downloading and deleting unhandled logs; blocking and unblocking devices].

7.2.20 FMT_SMR.1 Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [Administrator and User-Defined].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

7.2.21 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after [the administrator specified idle period has elapsed].

7.2.22 FTP_TRP.1 Trusted path

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*disclosure*].

FTP_TRP.1.2 The TSF shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [all requests made for its operation].

7.2.23 FRU_RSA.1 Maximum quotas

Hierarchical to: No other components.
Dependencies: No dependencies.

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [aggregated reports, aggregated syslogs and rawlogs] that [subjects] can use [*over a period of time as defined by the administrators of the system*].

Application note: Subjects refers to the modules/components as specified in the TOE(the collector and archiver).

7.2.24 FCS_COP.1(1) Cryptographic operation (AES)

Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_COP.1.1(1) The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [AES, Advanced Encryption Standard] and cryptographic key sizes [192 bits] that meet the following: [RFC 3268].

Application note: Encryption is performed on each archived file, and encrypted before saving into the destination. During restoration, the files will also be decrypted using the same constant key.

7.2.25 FCS_COP.1(2) Cryptographic operation (MD5)

Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_COP.1.1(2) The TSF shall perform [hashing] in accordance with a specified cryptographic algorithm [MD5, Message Digest Algorithm] and cryptographic key sizes [128 bits] that meet the following: [RFC 1321].

Application note: The rawlogs will be hashed, and the checksum will be written on a file and saved in the same location. A 3rd party Checksum calculator can be used to compare the checksums and to prove integrity of the files.

7.2.26 FCS_COP.1(3) Cryptographic operation (SHA-1)

Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_COP.1.1(3) The TSF shall perform [hashing] in accordance with a specified cryptographic algorithm [SHA-1,] and cryptographic key sizes [160 bits] that meet the following: [FIPS PUB 180-1-Secure Hash Standard].

Application note: Hashing is performed on user passwords during authentication, or during password creations.

7.4 TOE Security Assurance Requirement

The follow table illustrates the requirement component of EAL 2 for the TOE and is extracted from the Common Criteria Part 3 document. There is no refinement to any of the components listed below. For more information, please refer to the CC Part 3 document.

Assurance Class	Component ID	Component Name
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
ASE: Security target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE summary specification
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

8.0 TOE Summary Specification

8.1 TOE Security Functions

Security Function	TOE Scope Description
Identification and Authentication	LR provides user identification and authentication independent of that provided by the operating system it which it operates on.
Security Audit	LR provides a comprehensive auditing trail which records each individual user session and tracks each action within the session.
Granular Access Control List	LR allows users access permission within the application to be dynamically and granularly assigned via users and group memberships. Passwords are hashed using SHA-1.
Password Management	LR provides a full password management function including the management of password policy rules as well as password expiry settings.
Session Management	LR maintains session management and restricts a single login for only a single valid session. This is to say that should an account be used for 2 logins, the latter of the session will be invalidated and the access revoked.
Secured Socket Layer	LR runs on SSL to protect its data when travelling thru the wire.
Import and Export of configuration data	LR allows for the import and/or export of LR specific configuration data. Data exported and be later used as a medium of restoration or recovery.
Automated Archive	LR 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.
Real Time Syslog Collection	LR provides the ability for authorized users to dynamically configure the application to listen to syslog streams from network devices, servers and/or any other supported applications. Such a log collection is done real time as and when events occur.

8.1.1 Identification and Authentication

The TOE provides an identification and authentication layer independent from that of the Operating System it executes on. This security feature acts to protect and prevent access by unauthorized users to the system. In addition, it will also require each user to be identified and authorized first before any access to protected functions and data is granted. In the case of an authentication or identification failure, the TOE will disregard any request made an issue a forward redirection to the login page.

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. In addition to this, the system administrator can also manage authentication failure tolerance.

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.

Functional Requirements Satisfied:

- **FIA_UAU.2:** This component ensures that the user is authenticated before being granted access to the TOE.
- **FIA_UID.2:** This component ensures that the user is identified before being granted access to the TOE.
- **FDP_ACC.2:** This component ensures that the access control policies are enforced on all operations among subjects and objects in the SFP.
- **FIA_AFL.1:** This component ensures that the necessary measures are taken when a string of unsuccessful login attempt is detected, which frequency exceeds the tolerance threshold as specified by the system administrator.
- **FCS_COP.1(3):** This component specifies that the user account passwords are hashed using SHA-1.

8.1.2 Security Audit

The TOE provides for a comprehensive auditing layer which will monitor activities and executions occurring with 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 parameteric details that are specific to that activity.

As with most things within the TOE, the audit trails are secured not only to unidentified users but also unauthorized users as well. The security matrix built within the TOE will allow authorized administrators to set specific granular control to the exact groups of users who will have access to the audit trails.

Functional Requirements Satisfied:

- **FAU_GEN.3:** This component defines requirement to identify the auditable events for which audit records should be generated, and the information to be provided in the audit records.
- **FAU_GEN.2:** This component addresses the requirement of accountability of auditable events at the level of individual user identity. This component should be used in addition to FAU_GEN.3.
- **FAU_SAR.1:** This component will provide authorized users the capability to read audit information.

- **FAU_SAR.2:** This component specifies that all users will be denied access to audit records, except for those who have been explicitly given read access.

- **FMT_SMF.1:** This component ensures that the TOE grants authorized users the ability to manage the functions of audit trail management, user account management, role management and application security configuration.

8.1.3 Granular Access Control

The TOE provides a fluid and flexible security matrix which allows authorized administrators to specify security restrictions and awards that would make sense to their individual organization. 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.

In turn, each user is associated with a group and will inherit all permissions granted to that particular group. Needless to say, all restrictions imposed on the group would also apply to all users associated with that group.

Functional Requirements Satisfied:

- **FDP_ACF.1:** This component ensures that permissions and privileges can be granted to specific subjects and objects for different accesses.

- **FMT_MOF.1:** This component ensures that the ability to restrict access to functions based on specific user roles or groups.

- **FMT_REV.1:** This component ensures that the ability to remove access to functions based on specific user roles or groups.

- **FMT_SMR.1:** This component ensures that the users can be associated with groups.

- **FMT_SMF.1:** This component ensures that the TOE grants authorized users the ability to manage the functions of audit trail management, user account management, role management and application security configuration.

- **FMT_MSA.1:** This component ensures that the TOE will grant or restrict access to query, update and delete security roles to users with the correct access levels.

- **FMT_MSA.3:** This component ensures that the TOE permits authorized users to override default permissions and security values set.

8.1.4 Password Management

The TOE allows for the administrator to manage and control the implementation of user passwords. This in effect means that the system administrator is able to specify password complexity, expiration lengths as well as password generations.

Password complexity allows the administrator to set minimum password lengths while password expiration period means that the TOE will keep track of user password use and expire them when the allotted time has elapsed. Once expired, the users would be required to change their password before then can continue system use. Password generation tracking will also specify how many changes of passwords the TOE will keep track of. Users cannot reuse password that fall under the generation track. All user accounts (administrators or otherwise) are subject to these enforcements.

Functional Requirements Satisfied:

- **FIA_SOS.1:** This component ensures the necessary mechanism to specify rules for secrets management is made available.

8.1.5 Sessions Management

The TOE allows for the management of sessions connection. Authorized administrators are granted the ability to set the idle timeout threshold after which an authorized user would be automatically logged out of his active session. Idle timeout is defined as a period of inactivity from the user.

Functional Requirements Satisfied:

- **FMT_SAE.1:** This component ensures the ability to set expiration limits for idle sessions.
- **FTA_SSL.3:** This component provides the ability to terminate an interactive session after the specified period of inactivity has elapsed.

8.1.6 Secured Socket Layer

The Console portion of the TOE; being the sole interface of user interaction is designed to run on a Secure Socket Layer. SSL is a network protocol primarily used to secure the transmission of data between 2 remote locations; essentially providing protection for intercept when data packets are flowing “on the wire”.

Functional Requirements Satisfied:

- **FTP_TRP.1:** This component ensures that the communication path between itself and remote users are provided and sufficiently protected.

8.1.7 Import and Export of Configuration Data

The TOE provides for the import and export of application specific configuration data. Such data exported can be used as a medium of restoration or recovery. In this context, the term configuration data includes:

- Application Configuration (Email, system settings, IP Classes, etc)
- User Security Information (Users, groups and permissions)
- Device Data
- Reporting Settings
- Real Time Threat rules
- Asset Discovery configuration

Functional Requirements Satisfied:

- **FPT_ETC.2:** This component ensures that any export from the TOE will be authenticated and that only authorized users would be allowed access to such functions.
- **FPT_ITC.2:** This component ensures that any import to the TOE will be authenticated and that only authorized users would be allowed access to such functions.

8.1.8 Automated Archive

The TOE allows authorized users to specify the length of period in which active data is to be kept on server. Data (defined as aggregated reports, rawlogs and syslogs) older than the span specified will then be archived, encrypted and stored automatically at predetermined times.

Functional Requirements Satisfied:

- **FRU_RSA.1:** This component ensures that the TOE provides an avenue in which authorized users can specify the maximum quota of active data that should be kept on server at any time.
- **FCS_COP.1(1):** This component ensures that the TOE encrypts archived data to prevent from being read by unauthorized TOE users.
- **FCS_COP.1(2):** This component ensures that the TOE hashes the rawlogs and with the generated checksum, users can prove integrity of the files using 3rd party checksum calculators.

8.1.9 Real Time Syslog Collection

LR provides the ability for authorized users to dynamically configure the application to listen to syslog streams from network devices, servers or any other supported applications. Such log collection is executed real time as and when events occur.

Functional Requirements Satisfied:

- **FDP_IFF.1:** This component states that the TOE can receive syslog messages from remote computer or network devices.
- **FDP_IFC.1:** This component states that the TOE will detect when incoming logs originate from unknown or unregistered devices and then store them apart so the overall statistics and the accuracy of aggregated data would not be compromised. This component also provides for the eventuality that a log from registered devices cannot be processed or that the format is unrecognized. Such occurrences would be dealt with gracefully and stored in locations readily available to users with the appropriate access levels.

8.2 SFR Rationale Summary

The following section delves into each individual SFR and exactly how the TOE meets it:

Component	Component Name	Rationale
FAU_GEN.3	Simplified audit data generation	The TOE generates audit data for all functions which require user authentication. All audit trails is saved into database and accessible via web GUI. This component traces back to and aids in meeting the following security function: **Security Audit.**
FAU_GEN.2	User identity association	All audit data are grouped into specific sessions to ease the tracking of what a user executes for every unique session. Accessing the audit trail would clearly display each individual session, the user involved as well the every single event, it informative parameters and the corresponding timestamp. This component traces back to and aids in meeting the following security function: **Security Audit.**
FAU_SAR.1	Audit data review	The TOE provides a web interface to review all audit logs. Audit records can be viewed and filtered using either by specific users, specific actions or by

		specific dates. This component traces back to and aids in meeting the following security function: **Security Audit.**
FAU_SAR.2	Restricted audit review	Only users that are authenticated and have the correct access control permissions would be able to view audit trail logs. This component traces back to and aids in meeting the following security function: **Security Audit.**
FDP_ACC.2	Complete access control	Any action or function access in the TOE is controlled by its access control list (ACL) which is user defined and configured from within the TOE's security settings. As such, every action that requires user authentication will validate a user's roles and privileges against what is required for a specific function call. This component traces back to and aids in meeting the following security function: **Identification and Authentication.**
FDP_ACF.1	Security based access control	The TSF will allow each individual function to be explicitly assigned permission to a specific subject. This component traces back to and aids in meeting the following security function: **Granular Access Control.**
FPT_ETC.2	Export of user data with security attributes	The TOE provides for the export of user and security specific information. This function is termed as "Exporting Configuration" within the TOE. Among other elements, exported configuration will contain user data as well as the set security matrix of group permissions and membership. "Trusted IT products" in this context is defined as the TOE itself or any other installations of the TOE of a similar version. This component traces back to and aids in meeting the following security function: **Import and Export of Configuration Data.**
FDP_IFC.1	Subset information flow control	The TOE should have the facility to receive syslog messages from any computer or network device.

		This component traces back to and aids in meeting the following security function: **Real Time Syslog Collection.**
FDP_IFF.1	Simple security attributes	In the course of the TOE's data collection cycle, should data packets from known and registered device be unprocessable for any reason, those logs will be stored, filed and labelled "unparsable". Administrators will have access to all unparsable logs via the web GUI console. While these logs are saved to disk, they are not considered valid data and hence will not be aggregated or considered for statistical analysis. This component traces back to and aids in meeting the following security function: **Real Time Syslog Collection.**
FPT_ITC.2	Import of user data with security attributes	The TOE provides for the import of user and security specific information. This function is termed as "Import Configuration" within the TOE. Among other data elements, importing configuration will populate the TOE with user data as well as the set security matrix of group permissions and membership which exists within the exported data set. "Trusted IT products" in this context is defined as the TOE itself or any other installations of the TOE of a similar version. This component traces back to and aids in meeting the following security function: **Import and Export of Configuration Data.**
FIA_AFL.1	Authentication failure handling	TOE administrators can set threshold within the administration sections to determine how many times a failed login would be tolerated. This component traces back to and aids in meeting the following security function: **Identification and Authentication.**
FIA_UAU.2	User authentication before any action	Most of the TOE functions require the user to be authenticated and identified. These function calls would check and verify that the action session belongs to a valid user account before granting access. Invalid sessions or unauthenticated users will be redirected to the login page.

		This component traces back to and aids in meeting the following security function: **Identification and Authentication.**
FIA_UID.2	User identification before any action	Most of the TOE functions require the user to be authenticated and identified. These function calls would check and verify that the action session belongs to a valid user account before granting access. Invalid sessions or unauthenticated users will be redirected to the login page. This component traces back to and aids in meeting the following security function: **Identification and Authentication.**
FIA_SOS.1	Verification of secrets	The TOE allows for users with the appropriate access levels/permissions to specify minimum password lengths within the TOE. Such a setting would impose a global affect to any passwords set or updated within the TOE. This component traces back to and aids in meeting the following security function: **Password Management.**
FMT_MOF.1	Management of security functions behaviour	The TOE maintains a fluid and dynamic ACL which can be configured and reconfigured by authorized users in real time. The ACL will grant/restrict access to specific users based to the roles they play and the permissions that have been assigned. This component traces back to and aids in meeting the following security function: **Granular Access Control.**
FMT_REV.1	Revocation	As described in the compliance of FMT_MOF.1, the ACL grants/revokes access to all functions within the TOE. Any users with the necessary clearance level will be able to revoke access for any given role. This component traces back to and aids in meeting the following security function: **Granular Access Control.**
FMT_MSA.1	Management of security	The TOE enforces the access control matrix to all

	attributes	operations which require user verification. Included in such enforcement are the ability to query, modify or delete permission settings and access rights. This component traces back to and aids in meeting the following security function: **Granular Access Control.**
FMT_MSA.3	Static attribute initialisation	The TOE allows the user to maintain its own list of permissions settings and user groups. Groups are elements that are dynamically created and its associated permissions settings also fluid and definable in accordance to user preference and application. This component traces back to and aids in meeting the following security function: **Granular Access Control.**
FMT_SAE.1	Time-limited authorisation	The TOE will time out sessions that have been idle for a configured period of time. Timed out sessions are essentially invalidate and will no longer be considered authorized users. This component traces back to and aids in meeting the following security function: **Sessions Management.**
FMT_SMF.1	Specification of management functions	The TOE the following for security management functions: • Audit trail • User account management • Roles and ACL management • Application security configuration This component traces back to and aids in meeting the following security function: **Granular Access Control.**
FMT_SMR.1	Security roles	Roles within the TOE are dynamic and created by end users themselves to best cater for individual organizational structures. Each role is created with a permission matrix set. Every user playing that role would be granted/restricted access accordingly. This component traces back to and aids in meeting the following security function:

		Granular Access Control.
FTA_SSL.3	TSF-initiated termination	The TOE will automatically initiate session invalidation if a period of configured inactivity is detected from a logged in user. Such an operation will cause a logged in user to be automatically logged out. This component traces back to and aids in meeting the following security function: **Sessions Management.**
FTP_TRP.1	Trusted path	The TOE will handle all its request response from user to TSF via SSL leveraging on the secured http protocol so that data will be encoded before being sent thru the wire. This component traces back to and aids in meeting the following security function: **Secured Socket Layer.**
FRU_RSA.1	Maximum quotas	Authorized administrators are given the ability to set the quota of live data that will be maintained by the TOE. Administrators are able to specify the number of day worth of data that should be kept as active data on server itself. The Archiver module will then periodically run to archive data which do not fall into the given range. Archived data are stored separately, are not part of the active set and can be restored at a later date if necessary. This component traces back to and aids in meeting the following security function: **Automated Archive.**
FCS_COP.1(1)	Cryptographic operations (AES)	As the quotas are decided by Administrators and User-Defined roles, data that do not fall into the given range will be archived. Without user interventions, prior to archival, the data will be compressed, and encrypted using AES 128-bit. To view these logs again, they will have to be restored and decrypted back using the TOE. This component traces back to and aids in meeting the following security function: **Automated Archive**.

FCS_COP.1(2)	Cryptographic operations (MD5)	On daily basis, the Rawlogs will compressed and an MD5 checksum will be generated based on the files. With this checksum, Administrators can prove the integrity of the files. This component traces back to and aids in meeting the following security function: **Automated Archive**.
FCS_COP.1(3)	Cryptographic operations (SHA-1)	Users have to be authenticated before they are allowed to gain access to the TOE. The passwords are hashed using SHA-1. This component traces back to and aids in meeting the following security function: **Identification and Authentication.**

9.0 Rationale

9.1 Conformance Claims Rationale

The Conformance Claim of this ST does not claim conformance to any Protection Profile. Hence, there are no elements to be covered in the conformance claim rationale.

9.2 Security Objectives Rationale

The section details each individual security threat and where/how the TOE manages and/or counters them.

9.2.1 Security Objectives for the TOE

Threat	How threat is met
T.COMINT	The threat of a malicious person who may tamper with the integrity and secrecy of data that the TOE collects, is reduced by implementing: • **O.ACCESS** The TOE must be capable of restricting authorized users to functions or data that is appropriate for their role or access level. • **O.IDAUTH** The TOE must must identify and verify its users, before the execution of any TOE function or data is granted. • **O.PROTCT** Access Control Lists are required to limit authorized users to an access level sufficient for a specific function or data. • **OE.INTEGR** All personnel responsible for administering the TOE must ensure that all measures required to secure the TOE's operating environment to protect the integrity of the data in transit have already been taken.
T.DLOSS	The probability of a malicious or accident security event, either by known or unknown entities, may destroy protected TOE data. This threat is mitigated by: • **O.EXPORT** The TOE must be capable of exporting and importing data specific to the TOE for the purpose of backup, restoration or archival purposes, thus assuring the maintenance of the integrity and availability of TOE data.
T.IMPCON	The threat of the TOE's security being jeopardized either through a malicious configuration set by unauthorized entities, or accidentally having incorrect

	configuration settings set by authorized users, are mitigated by: • **O.ACCESS** The TOE must be capable of restricting authorized users to functions or data that is appropriate for their role or access level. • **O.EADMIN** The TOE must contain all necessary management functions to administer all security aspects of the TOE. • **O.IDAUTH** The TOE must must identify and verify its users, before the execution of any TOE function or data is granted. • **OE.INSTAL** All personnel responsible for the TOE must ensure that it is deployed, administered, and operated within all guidelines of IT security.
T.INFLUX	There exists a possibility that unauthorized entities may attempt to jeopardize TOE functions through means of an influx of data, or DoS (denial-of-service) attacks. This threat is reduced by: • **OE.OFLOWS** The IT environment must manage the potential problem of data storage overflow.
T.INSECUSE	There exists a possibility that either authorized or unauthorized users who are managing the TOE, may accidentally or maliciously cause disruption to the TOE, or disclose data that are collected, stored, aggregated, or analyzed. This threat is mitigated by: • **O.ACCESS** The TOE must be capable of restricting authorized users to functions or data that is appropriate for their role or access level. • **O.IDAUTH** The TOE must must identify and verify its users, before the execution of any TOE function or data is granted. • **O. PROTCT** Access Control Lists (ACLs) are required to limit authorized users to an access level sufficient for a specific function or data. • **OE.INSTAL** All personnel responsible for the TOE must ensure that it is deployed, administered, and operated within all guidelines of IT security. • **OE.PERSON** All personnel with the role of TOE administrator must be adequately trainied to manage the situation.
T.INTEGR	The threat is that an unauthorized user may attempt to modify data while in transit from devices in the infrastructure to the TOE. This threat is reduced by:

	• **OE.INTEGR** All personnel responsible for administering the TOE must ensure that all measures required to secure the TOE's operating environment to protect the integrity of the data in transit have already been taken.
T.LOSSOF	The threat of an unauthorized user attempting to destroy data that are collected, stored, aggregated, or analyzed by the TOE by means of a security bypass, is reduced by: • **O.ACCESS** The TOE must be capable of restricting authorized users to functions or data that is appropriate for their role or access level. • **O.IDAUTH** The TOE must must identify and verify its users, before the execution of any TOE function or data is granted. • **O. PROTCT** Access Control Lists (ACLs) are required to limit authorized users to an access level sufficient for a specific function or data.
T.NOHALT	The threat of an unauthorized user attempting to end the execution of the TOE by forcibly ending the service or process run, is reduced by: • **O.ACCESS** The TOE must be capable of restricting authorized users to functions or data that is appropriate for their role or access level. • **O.IDAUTH** The TOE must must identify and verify its users, before the execution of any TOE function or data is granted. • **O.PROTCT** Access Control Lists (ACLs) are required to limit authorized users to an access level sufficient for a specific function or data.
T.PRIVIL	The threat is that an unauthorized user may attempt to gain access to data that are collected, stored, aggregated, or analyzed by the TOE, through means of exploitation of system privileges, are mitigated by: • **O.ACCESS** The TOE must be capable of restricting authorized users to functions or data that is appropriate for their role or access level. • **O.IDAUTH** The TOE must must identify and verify its users, before the execution of any TOE function or data is granted. • **O.PROTCT** The TOE must be capable of restricting authorized users to functions or data that is appropriate for their role or access level.

T.UNATHDVCE	The threat of an unauthorized device attempting to jeopardize the TOE function through means of a massive influx of data (otherwise known as DoS (denial-of-service) attacks), is mitigated by: • **OE.OFLOWS** The IT environment must manage the potential problem of data storage overflow.

9.2.2 Organizational Policies for the TOE

Policies	How policies are supported
P.ACCACT	The organizational policy states that all users of the TOE must be accountable for their actions. This is implemented by: • **O.AUDITS** The TOE must provide the means to collect, store and maintain all records of function and data access within its scope. • **O.IDAUTH** The TOE must must identify and verify its users, before the execution of any TOE function or data is granted.
P.ACCESS	The organizational policy states that all collected, stored, aggregated, or analyzed data by the TOE should only be used for authorized purposes. This is implemented by: • **O.ACCESS** The TOE must be capable of restricting authorized users to functions or data that is appropriate for their role or access level. • **O.IDAUTH** The TOE must must identify and verify its users, before the execution of any TOE function or data is granted. • **O.PROTCT** Access Control Lists (ACLs) are required to limit authorized users to an access level sufficient for a specific function or data.
P.INTGTY	The organizational policy states that all collected, stored, aggregated, or analyzed data by the TOE should be protected from modification. This is implemented by: • **OE.INTEGR** All personnel responsible for administering the TOE must ensure that all measures required to secure the TOE's operating environment to protect the integrity of the data in transit have already been taken. • **O.INTEGR** The TOE must manage its defined anomalous circumstances gracefully, to

	ensure that the integrity of all collected data and generated statistics.
P.MANAGE	The organizational policy states that the TOE should only be administered by authorized users. This is implemented by: • **O.ACCESS** The TOE must be capable of restricting authorized users to functions or data that is appropriate for their role or access level. • **O.EADMIN** The TOE must contain all necessary management functions to administer all security aspects of the TOE. • **O.IDAUTH** The TOE must must identify and verify its users, before the execution of any TOE function or data is granted. • **O.PROTCT** Access Control Lists (ACLs) are required to limit authorized users to an access level sufficient for a specific function or data.
P.PROTCT	The organizational policy states that the TOE must be protected from unauthorized entries, as well as disruptions of normal application execution. This is implemented by: • **OE.OFLOWS** The IT environment must manage the potential problem of data storage overflow.

9.2.3 Security objectives for the environment

Assumption	How assumption traced back to objective for environment
A.TIME	• **OE.TMSTMP** The objective ensures the IT environment provides a reliable time source for the TOE to provide an accurate timestamp for all audit records.
A.DIRECT	• **OE.PHYCAL** This objective provides that the parts of the TOE which are crucial to all security policies are protected from physical threats at all times.
A.LOCATE	• **OE.PHYCAL** This objective provides that the parts of the TOE which are crucial to all security policies are protected from physical threats at all times.
A.PROTCT	• **OE.PHYCAL** This objective provides that the parts of the TOE which are crucial to all security policies are protected from physical threats at all times.
A.INTEGR	• **OE.PHYCAL** This objective provides that the parts of the TOE which are crucial to all security policies are protected from physical threats at all times. • **OE.INTEGR** This objective provides all assigned administrators must ensure the correctness and integrity of the data in transit from its source to the TOE.
A.MANAGE	• **OE.PERSON** This objective provides that all assigned administrators must be competent and adequately trained to correctly manage and administer the TOE.
A.NOEVIL	• **OE.PERSON** This objective provides that all assigned administrators must be competent and adequately trained to correctly manage and administer the TOE.
A.NOTRST	• **OE.PHYCAL** This objective provides that the parts of the TOE which are crucial to all security policies are protected from physical threats at all times. • **OE.PERSON** This objective provides that all assigned administrators must be competent and adequately trained to correctly manage and administer the TOE.

9.2.4 Security functional requirements of the TOE

SFR	How the requirement is met
FAU_GEN.3	• **O.AUDITS** This objective provides that the TOE will diligently collect, store and maintain

	all records of function and data access within its scope.
FAU_GEN.2	• **O.AUDITS** This objective provides that the TOE will diligently collect, store and maintain all records of function and data access within its scope.
FAU_SAR.1	• **O.EADMIN** This objective ensures that the TOE contains all necessary management functions to administer all security aspects of the TOE.
FAU_SAR.2	• **O.ACCESS** This objective is an extension from O.IDAUTH which grants access only to authorized users to access the TOE data. • **O.IDAUTH** This objective provides for the verification of users before the execution of any TOE function which requires user authentication. • **O. PROTCT** This objective provides for the necessary ACL to restrict/block even authorized users should their access level be insufficient for a specific function or data.
FDP_ACC.2	• **O.EADMIN** This objective ensures that the TOE contains all necessary management functions to administer all security aspects of the TOE.
FDP_ACF.1	• **O.EADMIN** This objective ensures that the TOE contains all necessary management functions to administer all security aspects of the TOE.
FPT_ETC.2	• **O.EXPORT** This objective ensures that the TOE provides the ability to import and export data for the purpose of either backup, restore or archival.
FDP_IFC.1	• **O.INTEGR** This objective provides for the integrity of all collected data and generated statistics by ensuring the TOE manages defined anomalous circumstances gracefully.
FDP_IFF.1	• **O.INTEGR** This objective provides for the integrity of all collected data and generated statistics by ensuring the TOE manages defined anomalous circumstances gracefully.
FPT_ITC.2	• **O.EXPORT** This objective ensures that the TOE provides the ability to import and export data for the purpose of either backup, restore or archival.

FIA_AFL.1	• **O.IDAUTH** This objective provides for the verification of users before the execution of any TOE function which requires user authentication.
FIA_UAU.2	• **O.ACCESS** This objective is an extension from O.IDAUTH which grants access only to authorized users to access the TOE data. • **O.IDAUTH** This objective provides for the verification of users before the execution of any TOE function which requires user authentication. • **O. PROTCT** This objective provides for the necessary ACL to restrict/block even authorized users should their access level be insufficient for a specific function or data.
FIA_UID.2	• **O.ACCESS** This objective is an extension from O.IDAUTH which grants access only to authorized users to access the TOE data. • **O.IDAUTH** This objective provides for the verification of users before the execution of any TOE function which requires user authentication.
FIA_SOS.1	• **O.ACCESS** This objective is an extension from O.IDAUTH which grants access only to authorized users to access the TOE data. • **O.IDAUTH** This objective provides for the verification of users before the execution of any TOE function which requires user authentication.
FMT_MOF.1	• **O.ACCESS** This objective is an extension from O.IDAUTH which grants access only to authorized users to access the TOE data. • **O.IDAUTH** This objective provides for the verification of users before the execution of any TOE function which requires user authentication. • **O. PROTCT** This objective provides for the necessary ACL to restrict/block even authorized users should their access level be insufficient for a specific function or data.
FMT_REV.1	• **O.ACCESS** This objective is an extension from O.IDAUTH which grants access only to authorized users to access the TOE data. • **O.IDAUTH** This objective provides for the verification of users before the execution of any TOE function which requires user authentication. • **O. PROTCT**

	This objective provides for the necessary ACL to restrict/block even authorized users should their access level be insufficient for a specific function or data.
FMT_MSA.1	• **O.EADMIN** This objective ensures that the TOE contains all necessary management functions to administer all security aspects of the TOE.
FMT_MSA.3	• **O.EADMIN** This objective ensures that the TOE contains all necessary management functions to administer all security aspects of the TOE.
FMT_SAE.1	• **O.EADMIN** This objective ensures that the TOE contains all necessary management functions to administer all security aspects of the TOE.
FMT_SMF.1	• **O.EADMIN** This objective ensures that the TOE contains all necessary management functions to administer all security aspects of the TOE.
FMT_SMR.1	• **O.IDAUTH** This objective provides for the verification of users before the execution of any TOE function which requires user authentication.
FTA_SSL.3	• **O.ACCESS** This objective is an extension from O.IDAUTH which grants access only to authorized users to access the TOE data. • **O.IDAUTH** This objective provides for the verification of users before the execution of any TOE function which requires user authentication. • **O. PROTCT** This objective provides for the necessary ACL to restrict/block even authorized users should their access level be insufficient for a specific function or data.
FTP_TRP.1	• **O. INTEGR** This objective provides for the integrity all TOE data.
FRU_RSA.1	• **O.EXPORT** This objective ensures that the TOE provides the ability to import and export data for the purpose of either backup, restore or archival.
FCS_COP.1 (1) AES	• **O. INTEGR** This objective provides for the integrity all TOE data.

FCS_COP.1 (2) MD5	• **O. INTEGR** This objective provides for the integrity all TOE data.
FCS_COP.1 (3) SHA1	• **O.IDAUTH** This objective provides for the verification of users before the execution of any TOE function which requires user authentication.

9.3 Security Requirements Rationale

9.3.1 Tracing of SFR to security objectives

The functional and assurance requirements presented in this ST are mutually supportive and their combinations meet the stated security objectives. The security requirements were derived according to the general model presented in Part 1 of the Common Criteria. The table below illustrates the mapping between security requirements, assumptions, threats, and the security objectives:

Map 1: SFRs to Security Objective for the environment

	O.PROTCT	O.EADMIN	O.ACCESS	O.IDAUTH	O.AUDITS	O.INTEGR	O.EXPORT	OE.INSTAL	OE.PHYCAL	OE.PERSON	OE.INTEGR	OE.TMSTMP	OE.OFLOWS
FAU_GEN.3					X								
FAU_GEN.2					X								
FAU_SAR.1		X											
FAU_SAR.2	X		X	X									
FDP_ACC.2		X											
FDP_ACF.1		X											
FPT_ETC.2							X						
FDP_IFC.2						X							
FDP_IFF.1						X							
FPT_ITC.2							X						
FIA_AFL.1				X									
FIA_UAU.2	X		X	X									
FIA_UID.2			X	X									
FIA_SOS.1			X	X									
FMT_MOF.1	X		X	X									
FMT_REV.1	X		X	X									
FMT_MSA.1		X											
FMT_MSA.3		X											
FMT_SAE.1		X											
FMT_SMF.1		X											
FMT_SMR.1				X									
FTA_SSL.3	X		X	X									
FTP_TRP.1						X							
FRU_RSA.1							X						
FCS_COP.1(1)						X							
FCS_COP.1(2)						X							
FCS_COP.1(3)				X									

Map 2: Security Objectives to Threats and OSPs

	T.COMINT	T.DLOSS	T.IMPCON	T.INFLUX	T.INSECUSE	T.INTEGR	T.LOSSOF	T.NOHALT	T.PRIVIL	T.UNATHDVCE	P.ACCACT	P.ACCESS	P.INTGTY	P.MANAGE	P.PROTCT
O.PROTCT	X				X		X	X	X		X			X	
O.EADMIN			X											X	
O.ACCESS	X		X		X		X	X	X		X	X		X	
O.IDAUTH	X		X		X		X	X	X		X	X		X	
O.AUDITS											X				
O.INTEGR													X		
O.EXPORT		X													

Map 3: Security Objectives for non-IT environment to Assumptions, Threats, and Organizational Security Policies

	A.TIME	A.DIRECT	A.LOCATE	A.PROTCT	A.INTEGR	A.MANAGE	A.NOEVIL	A.NOTRST	T.COMINT	T.DLOSS	T.IMPCON	T.INFLUX	T.INSECUSE	T.INTEGR	T.LOSSOF	T.NOHALT	T.PRIVIL	T.UNATHDVCE	P.ACCACT	P.ACCESS	P.INTGTY	P.MANAGE	P.PROTCT
OE.INSTALL											X		X										
OE.PHYCAL		X	X	X	X			X															
OE.PERSON						X	X	X					X										
OE.INTEGR										X				X							X		
OE.TMSTMP	X																						
OE.OFLOWS												X						X					X

9.3.2 Security Objectives Rationale relating to SFRs

Security Objective	SFR	Rationale
O.PROTCT The TOE shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. The user must be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. Users shall be able to execute the functions based on the Access Control bound to the User's role. At the same time, Administrators or User Defined Roles with the necessary privilege has the authority to revoke the attributes assigned to the other Users. After a specific idle period, the interactive session will be terminated.	FAU_SAR.2 FIA_UAU.2 FMT_MOF.1 FMT_REV.1 FTA_SSL.3	The TOE must be capable of protecting itself from unauthorized access. Only Administrators and Users with the necessary privilege is allowed to gain access and execute the specific functions. Privileges assigned earlier can also be revoked by Administrators or User Defined Roles with the revoking privilege. After a specific idle time, the session will be terminated to prevent from unauthorized users gaining access to the TOE, e.g on a shared PC.
O.EADMIN Only Administrators and User Defined roles who have granted access to read the audit trail information will be allowed to do so. Access to all the functions in the TOE is restricted by the Access Control List. Before the User is allowed to access to any page and perform any functions including the Security Attributes, the User's privilege is checked against the Access Control List. By default, some values will already have been set for the Security Attributes, however Administrators and User Defined roles with the granted privilege is able to override the values. The TSF shall be able to enforce password change after a specific period.	FAU_SAR.1 FDP_ACC.2 FDP_ACF.1 FMT_MSA.1 FMT_SMF.1 FMT_MSA.3 FMT_SAE.1	This objective ensures that the TOE contains all necessary management functions to administer all security aspects of the TOE. All privileges will be determined in the Access Control List. Before any User can perform any function in the TOE, their privilege will be checked against the Access Control List. However, their privilege can also be override for modifications of roles. These is also a password expiration period which can be enforced, and the expiration period can be modified.
O.ACCESS Only Administrators and User Defined roles who have granted access to read the audit trail information will be allowed to do so.	FAU_SAR.2	The TOE must be capable of restricting authorized users to functions or data that is appropriate for their role or access level. All Users must be

All users must be successfully authenticated and identified before they are allowed to gain access to the TOE and perform any actions on it. They will have to authenticate using valid username and password before they are allowed to gain access to the TOE. Upon successful authentication, the User will be allowed to perform functions as defined in the Access Control List. However, the User privileges can also be revoked as determined by Administrators or User Defined Roles with the necessary privileges. After a specified period of idleness, the Web session will be terminated.	FIA_UAU.2 FIA_UID.2 FIA_SOS.1 FMT_MOF.1 FMT_REV.1 FTA_SSL.3	successfully authenticated and identified by using valid Username and Passwords before they are allowed to gain access to the TOE. Upon successful authentication, all the authorised functions for the User will be as defined in the Access Control List. The privileges can also be revoked as deemed appropriate by the Administrators or User Defined Roles. However, if the Web Session is inactive after a period of time, it will be terminated to prevent from unauthorized users from gaining access to the TOE, e.g. on a Shared PC.
O.IDAUTH Users without the access to necessary permission to read the audit trail will not be allowed to do so. If a User failed the Username and Password authentication more than [1-10] times, their account will be suspended from further use. All users must be successfully authenticated and identified before they are allowed to gain access to the TOE and perform any actions on it. They will have to authenticate using valid username and password before they are allowed to gain access to the TOE. Upon successful authentication, the User will be allowed to perform functions as defined in the Access Control List. However, the User privileges can also be revoked as determined by Administrators or User Defined Roles with the necessary privileges. All user accounts will be associated to a predefined role, where it can be the Administrator role, or other User Defined roles.	FAU_SAR.2 FIA_AFL.1 FIA_UAU.2 FIA_UID.2 FIA_SOS.1 FMT_MOF.1 FMT_REV.1 FMT_SMR.1 FTA_SSL.3 FCS_COP.1 (3)	This objective provides for the verification of users before the execution of any TOE function which requires user authentication.. All Users must be successfully authenticated and identified by using valid Username and Passwords before they are allowed to gain access to the TOE. If the User failed the authentication more than a specific number of times, the account will be suspended immediately. The authentication trial can be modified and set between 1-10. Passwords are hashed using SHA-1 to prevent from illegal modifications. Upon successful authentication, all the authorised functions for the User will be as defined in the Access Control List. The privileges can also be revoked as deemed appropriate by the Administrators or User Defined Roles. All user accounts will be associated to the predefined roles, ie. the default

After a specified period of idleness, the Web session will be terminated. User passwords will be hashed using SHA-1, 160 bits, meeting standards FIPS PUB 180-1-Secure Hash Standard.		Administrator role and User Defined role. However, if the Web Session is inactive after a period of time, it will be terminated to prevent from unauthorized users from gaining access to the TOE.
O.AUDITS All auditable events will be audited. Audit information will include the time and date of event, the type of event and identity of the user.	FAU_GEN.3 FAU_GEN.2	This objective provides that the TOE will diligently collect, store and maintain all records of function and data access within its scope. All the activities performed by the user will be recorded including the time/date, type of event and the identity of the user.
O.INTEGR The IT environment will provide reliable time stamps. The TSP will receive Syslogs sent by any computers or network devices using TCP/IP network packets, based on Source IP, Port number and Protocol. The TSF shall encrypt and decrypt data using AES 192 bits that meets RFC 3268, and hash the Rawlogs using MD5, 128 bits, meeting RFC 1321.	FDP_IFC.1 FDP_IFF.1 FCS_COP.1 (1) FCS_COP.1 (2)	This objective provides for the integrity of all collected data and generated statistics by ensuring the TOE manages defined anomalous circumstances gracefully. The server should be able to provide reliable time, so that reliable time stamp can be used on the Audit trail and Syslogs. The Syslogs are configured to receive using Source IP, Port number and Protocol. The received Syslogs will be encrypted and decrypted using AES during archival process. The Rawlogs are also hashed using MD5 128 bits to provide a mechanism to prove integrity of the logs.
O.EXPORT The TSF enforces Access Control List when importing and exporting user data and security attributes. When the data has exceeded a quota of timing, they will be archived away.	FPT_ETC.2 FPT_ITC.2 FRU_RSA.1	This objective ensures that the TOE provides the ability to import and export data for the purpose of either backup, restore or archival. Only Users with the privilege to perform this function is allowed to modify these settings. Upon completion of configuration, no user intervention is required, archival

		will run automatically on the back end. Aggregated Report, Aggregated Syslog and Rawlogs which has exceeded the archival period, will be archived to a specified storage location.

9.3.3 SFR dependency rationale

This section provides a demonstration that all of the functional requirements of the Security Functional Requirements included within the TOE have been satisfied.

SFR	Dependency	Justification
FAU_GEN.3	FPT_STM.1	See 6.0 Extended components definition
FAU_GEN.2	FAU_GEN.3 FIA_UID.1	Satisfied FAU_GEN.3 and FIA_UID.1
FAU_SAR.1	FAU_GEN.3	Satisfied FAU_GEN.3
FAU_SAR.2	FAU_SAR.1	Satisfied FAU_SAR.1
FDP_ACC.2	FDP_ACC.1 FDP_ACF.1	Satisfied FDP_ACC.1 (hierarchical) and FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Satisfied FDP_ACC.1 and FMT.MSA.3
FPT_ETC.2	FDP_ACC.1	Satisfied FDP_ACC.1
FDP_IFC.1	FDP_IFF.1	Satisfied FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Satisfied FDP_IFC.1 and FMT_MSA.3
FPT_ITC.2	FDP_ACC.1 FTP_TRP.1	Satisfied FDP_ACC.1 and FTP_TRP.1
FIA_AFL.1	FIA_UAU.1	Satisfied FIA_UAU.1
FIA_UAU.2	FIA_UAU.1 FIA_UID.1	Satisfied FIA_UAU.1(hierarchical) and FIA_UID.1
FIA_UID.2	FIA_UID.1	Satisfied FIA_UID.1 (hierarchical)
FIA_SOS.1	-	No dependencies
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Satisfied FMT_SMR.1 and FMT_SMF.1
FMT_MSA.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	Satisfied FDP_ACC.1, FMT_SMR.1 and FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Satisfied FMR_MSA.1 and FMT_SMR.1
FMT_REV.1	FMT_SMR.1	Satisfied FMT_SMR.1
FMT_SAE.1	FMT_SMR.1 FPT_STM.1	Satisfied FMR_SMR.1 See 9.3.4 “Justification for missing dependencies”
FMT_SMF.1	-	No dependencies
FMT_SMR.1	FIA_UID.1	Satisfied FIA_UID.1

FTA_SSL.3	-	No dependencies
FTP_TRP.1	-	No dependencies
FRU_RSA.1	-	No dependencies

9.3.4 Justification for missing dependencies

The functional component FAU_GEN.3 has an identified dependency on FPT_STM.1. This dependency is not satisfied by any TOE functional requirement as the functionality of reliable time stamps is provided by the TOE environment.

9.3.5 SAR justification

The TOE and this ST manuscript are drawn in tandem with the requirements for CC EAL2. This particular package was chosen to provide assurances that are in conjunction with good commercial practises and in line with standard industry design. The chosen assurance level is consistent with the claimed threat environment.

10.0 Appendix

Main Modules	Available Access Controls	Roles	
		Administrator	User Defined
Asset Discovery Module	Delete Asset Item Detect Asset Availability Save Asset Alias Save Asset Configuration Save Automated Configuration Start Asset Scan Stop Asset Scan View Asset Details View Asset List View Automated Configuration View Configuration	Yes	Optional
Branch Management Module	Add Branch Delete Branch Edit Branch Process Branch Data View Branches List	Yes	Optional
Configuration Module	Add IP Classification Delete IP Classification Edit IP Classification Restore Data Save Backup Data Configuration Save Configuration Settings Save Data Transfer Configuration Save Email Configuration Save Intranet IP Configuraiton Test Backup Restore Path Test Email Configuration View Backup Restore Configuration View Backup Restore Data View Configuration Settings View Data Transfer Configuration View Email Configuration View Intranet Configuration View IP Classifications List	Yes	Optional
Dashboard Module	Download Logs DrillDown	Yes	Optional
Device Management Module	Add Device Add Device Group Delete Device Delete Device Group Edit Device Edit Device Group View Device Groups List View Devices List	Yes	Optional
License Management Module	Registration	Yes	Optional

	Renewal		
Log Analytics Module	Add Log Analytic Delete Log Analytic Edit Log Analytic Export Log Analytic View Log Analytics List View Log Analytics Results	Yes	Optional
Real-Time Threats Management Module	Add Correlation Add Keyword Add Predefined IP Add Predefined Port Add Rule Change Correlation Statu Delete Correlation Delete Keyword Delete Predefined IP Delete Predefined Port Delete Rule Delete Triggered Report Edit Correlation Edit Keyword Edit Predefined IP Edit Predefined Port Edit Rule Export Triggered Report Triggered Report Acknowledgement View Correlations List View Keywords List View Predefined Ips List View Predefined Ports List View Rules List View Triggered List View Triggered Report	Yes	Optional
Reporting Module	Add Automated Report Compliance CSV Download Compliance PDF Download Delete Automated Report Delete Generated Report Download Automated Report Edit Automated Report Edit Report Filter On Demand CSV Download On Demand PDF Download View Automated Reports List View Compliance Reports View On Demand Reports	Yes	Optional
Unhandled Log Module	Block Unhandled Device Logs Delete Unhandled Logs File Download Unhandled Logs Email Unhandled Logs	Yes	Optional

	Unblock Unhandled Device Logs View Unhandled Logs List		
User Administration Module	Add User Add User Group Audit Trail Archive List Delete Audit Trail Archive File Delete User Delete User Group Download Audit Trail Archive File Edit User Edit User Group Reset User Password View Audit Trails View User Groups List View Users List	Yes	Optional

Table 1. Access Control List by Roles

Main Modules	Security Attributes	Management of Security Attributes	Roles	
			Administrator	User Defined
Asset Discovery Module	Asset Alias	Save	Yes	Optional
	Asset Availability	Detect		
	Asset Configuration	Save		
	Asset Details	View		
	Asset Item	Delete		
	Asset List	View		
	Asset Scan	Start Stop		
	Automated Configuration	Save View		
	Configuration	View		
Branch Management Module	Branch	Add Delete Edit	Yes	Optional
	Branch Data	Process		
	Branches List	View		
Configuration Module	Backup Data Configuration	Save	Yes	Optional
	Backup Restore Configuration	View		
	Backup Restore Data	View		
	Backup Restore Path	Test		
	Configuration Settings	Save View		
	Data	Restore		
	Data Transfer Configuration	Save View		
	Email Configuration	Save Test View		
	Intranet Configuration	View		
	Intranet IP Configuraiton	Save		
	IP Classification	Add Delete Edit		
	IP Classifications List	View		
Dashboard Module	Logs	Download DrillDown	Yes	Optional
Device Management Module	Device	Add Delete Edit	Yes	Optional
	Device Group	Add Delete Edit		
	Device Groups List	View		
	Devices List	View		
License Management Module	License	Registration Renewal	Yes	Optional

Log Analytics Module	Log Analytic	Add Delete Edit Export	Yes	Optional
	Log Analytics List	View		
	Log Analytics Results	View		
Real-Time Threats Management Module	Correlation	Add Delete Edit	Yes	Optional
	Correlation Status	Change		
	Correlations List	View		
	Keyword	Add Delete Edit		
	Keywords List	View		
	Predefined IP	Add Delete Edit		
	Predefined Ips List	View		
	Predefined Port	Add Delete Edit		
	Predefined Ports List	View		
	Rule	Add Delete Edit		
	Rules List	View		
	Triggered List	View		
	Triggered Report	Delete Export View Acknowledge		
Reporting Module	Automated Report	Add Delete Download Edit	Yes	Optional
	Automated Reports List	View		
	Compliance CSV	Download		
	Compliance PDF	Download		
	Compliance Reports	View		
	Generated Report	Delete		
	On Demand CSV	Download		
	On Demand PDF	Download		
	On Demand Reports	View		
	Report Filter	Edit		
Unhandled Log Module	Unhandled Device Logs	Block Unblock	Yes	Optional
	Unhandled Logs	Download Email		

	Unhandled Logs File	Delete		
	Unhandled Logs List	View		
User Administration Module	User	Add	Yes	Optional
	User Group	Add		
	Audit Trail Archive File	Delete Download		
	Audit Trail Archive List	View		
	Audit Trails	View		
	User	Delete Edit		
	User Group	Delete Edit		
	User Groups List	View		
	User Password	Reset		
	Users List	View		

Table 2.Security Attributes List by Roles