Trustwave SIEM Enterprise Security Target

Version 2.7

April 11, 2016

Trustwave
70 West Madison Street
Suite 1050
Chicago, IL 60602

DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

Trustwave
70 West Madison Street
Suite 1050
Chicago, IL 60602
http://www.trustwave.com

REVISION HISTORY

Rev	Description
1.0	October 30, 2014, Initial release
1.1	January 26, 2015, Addressed lab ORs
1.2	February 3, 2015, Addressed additional lab ORs
2.0	February 23, 2015, Converted to SIEM Enterprise only
2.1	March 13, 2015, Added FPT_STM.1 and O.TIME; SFR adjustments since no longer complying with PP; addressed certifier ORs
2.2	March 20, 2015, Addressed lab comments
2.3	April 11, 2015, Consistency updates for ADV
2.4	May 26, 2015, Upgrade TOE version to 2.3
2.5	June 18, 2015, Modified deployment options for DA components
2.6	March 27, 2016, Updated TOE version
2.7	April 11, 2016, Added guidance documents

TABLE OF CONTENTS

1. SECURITY TARGET INTRODUCTION 7
1.1 Security Target Reference 7
1.2 TOE Reference 7
1.3 Evaluation Assurance Level 7
1.4 TOE Overview 7
1.4.1 Usage and Major Security Features 7
1.4.2 TOE Type 9
1.4.3 Required Non-TOE Hardware/Software/Firmware 9
1.5 TOE Description 10
1.5.1 Physical Boundary 11
1.5.2 Logical Boundary 13
1.5.2.1 Audit 13
1.5.2.2 Management 13
1.5.2.3 Security Information and Event Management (SIEM) 13
1.5.2.4 I&A 13
1.5.3 TOE Data 13
1.6 Evaluated Configuration 15
1.7 Functionality Excluded from the Evaluation 15

2. CONFORMANCE CLAIMS 17
2.1 Common Criteria Conformance 17
2.2 Security Requirement Package Conformance 17
2.3 Protection Profile Conformance 17

3. SECURITY PROBLEM DEFINITION 18
3.1 Introduction 18
3.2 Assumptions 18
3.3 Threats 18
3.4 Organisational Security Policies 19

4. SECURITY OBJECTIVES 20
4.1 Security Objectives for the TOE 20
4.2 Security Objectives for the Operational Environment 20

5. EXTENDED COMPONENTS DEFINITION 22
5.1 Extended Security Functional Components 22
5.1.1 Class IDS: Intrusion Detection 22
5.1.1.1 IDS_ANL Analyser Analysis 22
5.1.1.2 IDS_RCT Analyser React 23
5.1.1.3 IDS_RDR Restricted Data Review 24
5.1.1.4 IDS_STG Analyser Data Storage 25
5.2 Extended Security Assurance Components 26

6. SECURITY REQUIREMENTS 27
6.1 TOE Security Functional Requirements 27
6.1.1 Security Audit (FAU) 27
6.1.1.1 FAU_GEN.1 Audit Data Generation 27
6.1.1.2 FAU_SAR.1 Audit Review 28

6.1.1.3 FAU_SAR.2 Restricted Audit Review 28
6.1.1.4 FAU_SAR.3 Selectable Audit Review 28
6.1.1.5 FAU_STG.2 Guarantees of Audit Data Availability 28
6.1.1.6 FAU_STG.4 Prevention of Audit Data Loss 29
6.1.2 Identification and Authentication (FIA) 29
6.1.2.1 FIA_AFL.1 Authentication Failure Handling 29
6.1.2.2 FIA_ATD.1 User Attribute Definition 29
6.1.2.3 FIA_UAU.1 Timing of Authentication 29
6.1.2.4 FIA_UID.1 Timing of Identification 29
6.1.3 Security Management (FMT) 29
6.1.3.1 FMT_MOF.1 Management of Security Functions Behaviour 29
6.1.3.2 FMT_MTD.1 Management of TSF Data 30
6.1.3.3 FMT_SMF.1 Specification of Management Functions 30
6.1.3.4 FMT_SMR.1 Security Roles 31
6.1.4 Protection of the TSF (FPT) 31
6.1.4.1 FPT_STM.1 Reliable Time Stamps 31
6.1.5 Intrusion Detection (IDS) 31
6.1.5.1 IDS_ANL.1 Analyser Analysis 31
6.1.5.2 IDS_RCT.1 Analyser React 31
6.1.5.3 IDS_RDR.1 Restricted Data Review 31
6.1.5.4 IDS_STG.1 Guarantee of Analyser Data Availability 32
6.1.5.5 IDS_STG.2 Prevention of Analyser data loss 32
6.2 TOE Security Assurance Requirements 32
6.3 CC Component Hierarchies and Dependencies 32

7. TOE SUMMARY SPECIFICATION 34
7.1 FAU_GEN.1, FPT_STM.1 34
7.2 FAU_SAR.1, FAU_SAR.2, FAU_SAR.3 34
7.3 FAU_STG.2, FAU_STG.4 34
7.4 FIA_AFL.1 34
7.5 FIA_ATD.1 34
7.6 FIA_UAU.1, FIA_UID.1 35
7.7 FMT_MOF.1 35
7.8 FMT_MTD.1 35
7.9 FMT_SMF.1 35
7.10 FMT_SMR.1 35
7.11 IDS_ANL.1, IDS_RCT.1 35
7.12 IDS_RDR.1 35
7.13 IDS_STG.1, IDS_STG.2 36

8. PROTECTION PROFILE CLAIMS 37

9. RATIONALE 38
9.1 Rationale for IT Security Objectives 38
9.2 Security Requirements Rationale 40
9.2.1 Rationale for Security Requirements of the TOE Objectives 40
9.2.2 Security Assurance Requirements Rationale 43

LIST OF FIGURES

Figure 1 - Representative TOE Deployment 8
Figure 2 - Typical TOE Deployment 11
Figure 3 - Physical Boundary 11

LIST OF TABLES

Table 1 - SE Minimum Hardware Requirements 9
Table 2 - SE Administration Console Minimum Hardware/Software Requirements 9
Table 3 - SIEM SE Appliances 12
Table 4 - Pre-installed Software 12
Table 5 - TOE Data Descriptions 13
Table 6 - Assumptions 18
Table 7 - Threats 18
Table 8 - Organisational Security Policies 19
Table 9 - Security Objectives for the TOE 20
Table 10 - Security Objectives of the Operational Environment 20
Table 11 - Auditable Events 27
Table 12 - TSF Data Access Details 30
Table 13 - EAL2+ Assurance Requirements 32
Table 14 - TOE SFR Dependency Rationale 32
Table 15 - Security Objectives Mapping 38
Table 16 - Rationale For Security Objectives Mappings 39
Table 17 - SFRs to Security Objectives Mapping 41
Table 18 - Security Objectives to SFR Rationale 41

ACRONYMS LIST

CC ..... **Common Criteria**
CCEVS ..... **Common Criteria Evaluation and Validation Scheme**
DA ..... **Data Acquisition**
DBMS ..... **DataBase Management System**
EAL ..... **Evaluation Assurance Level**
FTP ..... **File Transfer Protocol**
GUI ..... **Graphical User Interface**
IDS ..... **Intrusion Detection System**
IP ..... **Internet Protocol**
IPS ..... **Intrusion Prevention System**
IT ..... **Information Technology**
I&A ..... **Identification & Authentication**
JDBC ..... **Java DataBase Connectivity**
NIAP ..... **National Information Assurance Partnership**
OID ..... **Object IDentifier**
PC ..... **Personal Computer**
PP ..... **Protection Profile**
RHEL ..... **Red Hat Enterprise Linux**
SAR ..... **Security Assurance Requirement**
SCP ..... **Secure CoPy**
SDW ..... **Secure Data Warehouse**
SE ..... **SIEM Enterprise**
SFR ..... **Security Functional Requirement**
SIEM ..... **Security Information and Event Management**
SNMP ..... **Simple Network Management Protocol**
ST ..... **Security Target**
TD ..... **Threat Detector**
TE ..... **Threat Evaluator**
TOE ..... **Target of Evaluation**
TSF ..... **TOE Security Function**
UDP ..... **User Datagram protocol**
URL ..... **Uniform Resource Locator**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Trustwave SIEM Enterprise. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4*. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Trustwave SIEM Enterprise Security Target, Version 2.7, dated April 11, 2016.

1.2 TOE Reference

Trustwave SIEM Enterprise Version 2.3.3 (Build 856) and Trustwave SIEM Enterprise Administration Console Version 2.3.3 (Build 197).

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) augmented by ALC_FLR.2 from the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 4.

1.4 TOE Overview

1.4.1 Usage and Major Security Features

Trustwave Security Information and Event Management (SIEM) Enterprise (SE) is a comprehensive security information solution that monitors security information according to configured criteria. Users may:

- Monitor and investigate events generated by third party devices and alerts generated according to configured rules. These third party devices may include Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) sensors and/or scanners, firewalls, servers, or other types of systems capable of sending security information to the TOE.
- Generate and view reports
- Monitor alert information
- View alerts and their details
- Take ownership of alerts
- View raw log details
- Monitor system health
- Monitor reporting device status
- Manage rules for processing events
- Manage users and groups
- Manage devices and device groups
- Configure alert monitoring and event correlation information

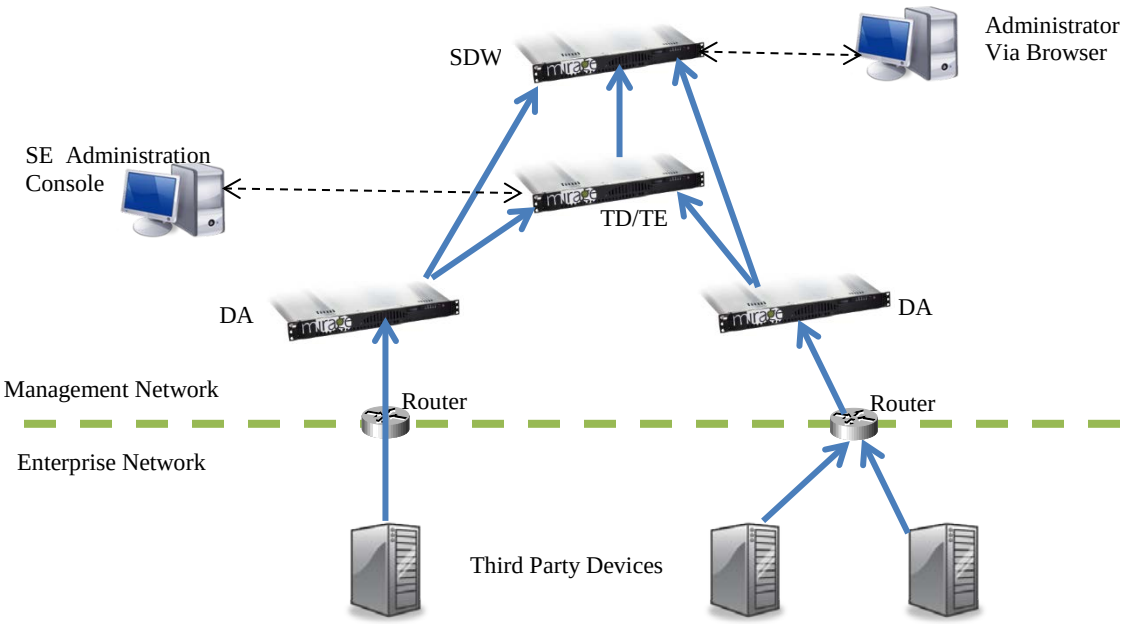
All of these tasks except the last bullet item are performed using the SE web interface. Configuration of the alert monitoring and event correlation is performed via the SE

Administration Console. Both user access mechanisms support multiple roles to limit the functionality of individual users.

A typical SE installation consists of the following components, which may execute on one platform or distributed across multiple platforms:

- One or more Data Acquisition (DA) components that receive information from third party devices
- One Security Data Warehouse (SDW) component is responsible for managing the collected and generated data for review. This component also supplies the SE web interface functionality.
- One or more combined Threat Detector (TD)/Threat Evaluator (TE) components are responsible for collecting events, applying event correlation rules to alerts, and sending them to the SDW. In environments with a high volume of security information, multiple TD/TE instances may be deployed.
- One or more SE Administration Console applications executing on Windows PCs.

Figure 1 - Representative TOE Deployment



Data Acquisition Servers

Data Acquisition (DA) components are collectors that receive information from security data sources via Syslog or SNMP. They are responsible for inbox monitoring, event filtering and output of event information.

Security Data Warehouse Server

The Security Data Warehouse (SDW) component stores the raw and processed events received from the Data Acquisition (DA) components, as well as the alerts that are generated by the Threat Detector (TD) and Threat Evaluator (TE) components, and all SE configuration.

The SE database is a MySQL database that resides on the same platform as the SDW component.

Threat Detector and Threat Evaluator Servers

The Threat Detector (TD) and Threat Evaluator (TE) components collect information from the DA components and apply correlation rules to events and alerts. The collected information is then routed to the SDW component.

SE Administration Console

SE Administration Consoles provide the user interface to configure alert generation and event correlation on TD/TE components. The SE Administration Console application can be installed on one or more Windows computers.

1.4.2 TOE Type

IDS Analyzer

1.4.3 Required Non-TOE Hardware/Software/Firmware

The TOE consists of SE distributed as a virtual appliance (VA) or physical appliance, along with the SE Administration Console application installed on a user-supplied Windows PCs.

When SE is distributed as a VA, the system hosting the VA must satisfy the following minimum requirements. These requirements apply for any combination of the SE server components (DA, SDW, TD and TE) executing on a single virtual server.

Table 1 - SE Minimum Hardware Requirements

Item	Requirements
Processors	Two CPUs
Memory	8GB
Hard Disk Free Space	50GB for the operating system 500GB for data
Network Interfaces	2
Hypervisor	VMware vSphere 5.5

SE Administration Consoles must be installed on Windows PCs meeting the minimum requirements in the following table. Any number of SE Administration Consoles may be installed, the only caveat being that at least one SE Administration Console must be installed in order to manage the TDs/TEs.

Table 2 - SE Administration Console Minimum Hardware/Software Requirements

Item	Requirements
Operating System	Windows 7
Processors	3GHz CPU Intel Pentium 4 or AMD Athlon XP
Memory	2GB
Hard Disk Free Space	1GB
Other Hardware	Display driver capable of 24 bit color at 1024x768

Item	Requirements
Browser	Internet Explorer 6.0 or higher, or Mozilla Firefox 2 or higher with pop-up blocker tools disabled and the following functionality enabled: • Cookies • Java • JavaScript • ActiveX

The TOE components communicate with one another via a segregated management network to prevent disclosure or modification of the data exchanged between TOE components. It is the responsibility of the operational environment to protect the traffic on the management network from other (non-TOE) devices.

Two or more physical interfaces are supported on the physical appliances. One interface may be used to receive management information and communicate with other TOE components, while the others may be used to receive security information from third-party devices.

Third party devices supply security information to TOE components; this information may be sent to SE Data Acquisition (DA) components. The traffic to DA components is limited to one-way UDP traffic from the third party devices to those TOE components. At least one router must interconnect the management network with the Enterprise Network. Any routers performing this function must be configured so that one-way UDP security information from the third party devices is permitted to flow from the Enterprise Network to the SE DA interfaces on the management network. No other traffic between devices connected to the management network and devices in the Enterprise Network is required by the TOE and should be blocked by the router.

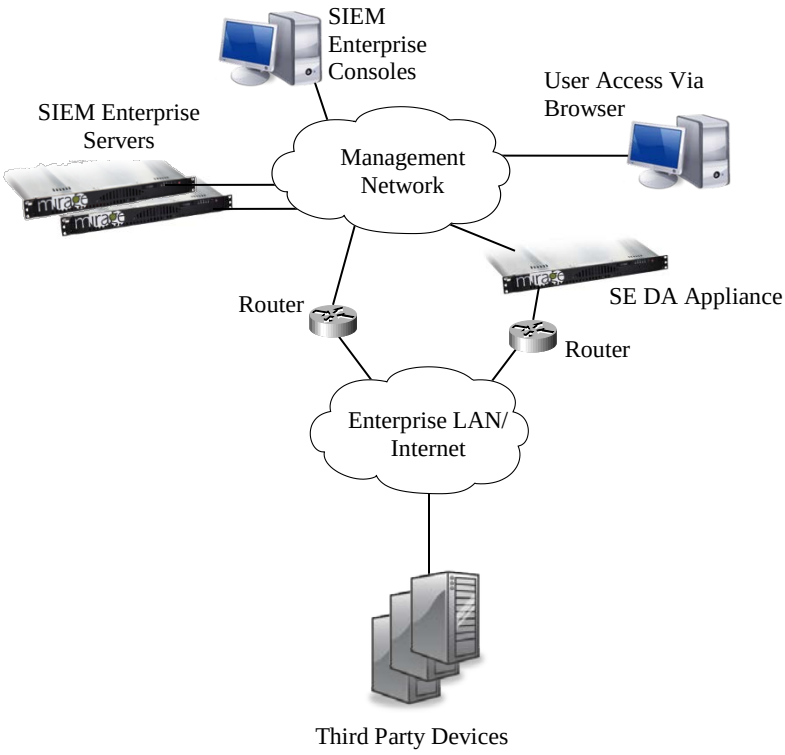
1.5 TOE Description

The TOE provides Security Information and Event Management (SIEM) functionality to normalize and correlate security information received from third party security devices and generate alerts for configured conditions. These third party security devices may include Trustwave SIEM LME appliances, IDS/IPS sensors and/or scanners, firewalls, servers, or other types of systems capable of sending security information to the TOE.

SE components execute on one or more dedicated appliances running TrustOS, a hardened Linux kernel; SE Administration Consoles are installed on one or more Windows systems. During installation of each SE physical or virtual appliance, the user may specify which components are to execute on the instance.

A typical deployment for these components is shown in the following diagram.

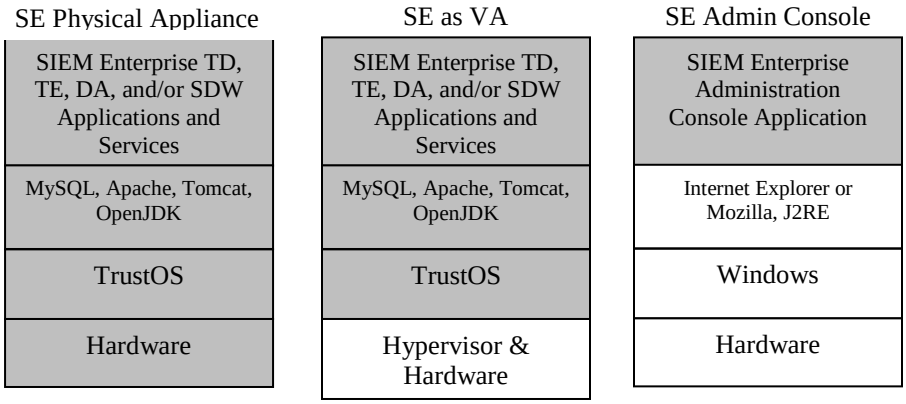
Figure 2 - Typical TOE Deployment



1.5.1 Physical Boundary

The physical boundary of the TOE is depicted in the following diagram (shaded items are within the TOE boundary).

Figure 3 - Physical Boundary



Each installed SE instance may be configured to be any combination of the SE components. Distribution of the components across multiple platforms provides higher performance and processing power for large installations, but the security functionality is equivalent for any installation scenario.

The following appliance choices are supported for SE.

Table 3 - SIEM SE Appliances

Model HW Item	LME2	LME3
CPU(s)	Intel Quad-core E5440 2.83GHz	Intel Hexa-core Xeon X5650, 2.66Ghz
RAM	12GB	16GB
Disk	2T / RAID 5	4T / RAID 5
RAID with battery backup	PERC 6/i with 256MB battery-backed cache	
NIC	Two dual-port embedded Broadcom® NetXtreme IITM 5709c Gigabit Ethernet NIC with failover and load balancing	
Software	The following software is pre-installed on the appliance by the vendor: TrustOS, MySQL, Apache, Tomcat, OpenJDK.	
Model HW Item	**LME2**	**LME3**
CPU(s)	Intel Quad-core E5440 2.83GHz	Intel Hexa-core Xeon X5650, 2.66Ghz
RAM	12GB	16GB
Disk	2T / RAID 5	4T / RAID 5
RAID with battery backup	PERC 6/i with 256MB battery-backed cache	
NIC	Two dual-port embedded Broadcom® NetXtreme IITM 5709c Gigabit Ethernet NIC with failover and load balancing	
Software	The following software is pre-installed on the appliance by the vendor: TrustOS, MySQL, Apache, Tomcat, OpenJDK.	

The following software is pre-installed with the distribution (whether it is via physical appliance or VA).

Table 4 - Pre-installed Software

Item	Requirements
Operating System	TrustOS 2.4 (hardened Linux derived from RHEL/CentOS
DBMS	MySQL 5.6.23-enterprise-commercial-advanced
Web Server	Apache Web Server 2.4.9
Application Server	Apache Tomcat 7.0.62
Java	OpenJDK 1.7.0-internal

The physical boundary includes the following guidance documentation:

1. *Trustwave SIEM Quick Start Guide - Version 2.3.1*
2. *Trustwave SIEM Enterprise Administration Guide – Version 2.3.1*
3. *Trustwave SIEM Enterprise User Guide – Version 2.3*
4. *Trustwave SIEM Enterprise TD/TE Configuration Guide - Version 2.3*
5. *Trustwave SIEM Enterprise Common Criteria Supplement*

6. *Trustwave SIEM Enterprise/Log Management Enterprise - Deploying and Resizing the Virtual Appliance*
7. *Trustwave SIEM Enterprise VM Quick Start*

1.5.2 Logical Boundary

1.5.2.1 Audit

Audit records are generated for specific actions performed by users. The audit records are saved and may be reviewed by authorized administrators.

1.5.2.2 Management

The TOE provides functionality for administrators to configure and monitor the operation of the TOE via the SE Administration Consoles and web browser sessions. The following administrator roles are supported: Managers, Analysts, Operators and Executives.

1.5.2.3 Security Information and Event Management (SIEM)

The TOE receives and normalizes security information and event messages from remote security devices. This information is received by the Data Acquisition components of SE via real-time feeds (e.g. syslog) or files. The received information is correlated by SE to determine if any alerts should be generated.

Users may review the saved information via web sessions and reports.

1.5.2.4 I&A

The TOE identifies and authenticates users of SE Administration Consoles and web sessions before they are granted access to any TSF functions or data. When valid credentials are presented, security attributes for the user are bound to the session.

Syslog feeds from remote security devices may be received without I&A.

1.5.3 TOE Data

The following table describes the TOE data for SE.

Table 5 - TOE Data Descriptions

TOE Data	Description
Alarms	Alarms are automatically generated by the TOE and indicate the occurrence of conditions potentially requiring actions by administrators (e.g. low disk space).
Alerts	Alerts are the results of analysis of the Events. Attributes include: • Type of Alert • Owner • Associated Events
Asset Groups	Define groups of Devices with similar attributes. Device Group attributes include: • Name • Description • Member Devices • Associated Zones

TOE Data	Description
Assets	Define physical resources, such as servers or workstations, which may be the subject of security information sent to the TOE. Device attributes include: • IP address • Hostname • Status (enabled/disabled) • Operational Risk • Compliance Risk • Contact • Zone • Location • Protocol Instances specifying how information is received from the device and processed
Contacts	Define contact information that is associated with Devices or Zones. Contact attributes include: • Name • Title • Phone Number • Email Address • Cell Phone Number
Data Retention Policies	Define the time for Analyser data to be retained in the system.
Events	Events are the parsed and normalized form of the security information received from remote security devices.
Networks	Define networks to assist in associating security information with a Device when IP addresses are not unique, such as MSSP environments. Network attributes include: • Name • Detector IP address or hostname • DA IP address or hostname • Acquiring IP address or hostname • Associated Devices and/or Device Groups
Notifications	Define conditions for sending an email message or SNMP Trap to an external entity based on analysis of Alerts or failure to receive information from a Device for an extended period. Attributes include: • Name • Conditions • Recipients
Report Definitions	Defines the parameters for a Report that can subsequently be generated. Attributes include: • Name • Time Range • Detectors • Zones
Reports	Published Reports that may be viewed. When created, Reports can be saved as public (able to be viewed by everyone) or private.
Rules	Define the analysis of Events for correlation and alert generation. Attributes include: • Correlation parameters • Alert triggers • Alert notifications

TOE Data	Description
System Latency Settings	Define the maximum time allowed for receipt of data from each source before an Alert is generated, and whether Alert generation for this condition is enabled.
User Accounts	Define the set of users that are authorized to use the TOE, with the following attributes: • User Name • Password • Role • Enabled • Locked • Full Name • Title • Email Address • Homepage • Description • Account Expiry Date (or Never) • User Is Allowed To Change Password • Group Account Memberships • Authorized Zones and Devices
Zones	Define a logical grouping of Networks (and through them Devices) used to implement data partitioning. Zone attributes include: • Name • Description • Associated Networks

1.6 Evaluated Configuration

The evaluated configuration of the TOE includes:

1. SDW – 1 instance
2. TD/TE – 1 or more instances
3. DA – 1 or more instances
4. SE Administration Console – 1 or more instances

The SE components may execute on a common platform or on separate platforms.

The following configuration restrictions apply to the evaluated configuration:

1. The default SE roles and their default permission sets are used to assign access permissions to users.
2. Non-Managers in SE are not permitted to change their own password.
3. Data expiry is configured and enabled on the DA and SDW components during installation.
4. The standard Event IDs are used (Event IDs are not customized).

1.7 Functionality Excluded from the Evaluation

The following functionality offered by SIEM Enterprise is excluded from the evaluation:

1. High Availability option for server redundancy
2. Incident management to automatically generate incidents in SIEM Enterprise from configured conditions and subsequently manage them.
3. Capability of SIEM Enterprise to forward log and event information it receives to additional (third party) system
4. Retrieval of security information by SE from remote systems via remote database access using JDBC or remote file retrieval using SCP or FTP (receipt via Syslog and SNMP are included in the evaluation)
5. Definitions of Syslog data formats in SE for custom devices (numerous third party devices as well as generic Syslog devices are included in the evaluation).
6. Customized actions to be associated with Alerts or Events
7. The “Local_admin” and “Self-service” user roles are predefined but are not used.
8. In addition to the LME2 and LME3, the TOE is also supported on the LME4 and LME5 appliances.

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Version 3.1 Revision 4, dated September 2012

Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 Security Requirement Package Conformance

EAL2 augmented by ALC_FLR.2

The TOE does not claim conformance to any security functional requirement packages.

2.3 Protection Profile Conformance

The TOE does not claim conformance to any protection profile.

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the Devices and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the Operational Environment.

Table 6 - Assumptions

A.Type	Description
A.ACCESS	The TOE has access to all the IT System resources necessary to perform its functions.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.MGMTNETWORK	The TOE components will be interconnected by a segregated management network that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users, and limits traffic from the enterprise network entering the management network to security information from third party security devices being sent via UDP to the DA components of the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

3.3 Threats

The threats identified in the following table are addressed by the TOE and the Operational Environment.

Table 7 - Threats

T.Type	Description
T.COMDIS	An unauthorized person may attempt to disclose the data analyzed and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.Type	Description
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of potential intrusion data received from all data sources.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.IMPCON	The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.LOSSOF	An unauthorized person may attempt to remove or destroy data analyzed and produced by the TOE.
T.NOHALT	An unauthorized person may attempt to compromise the continuity of the TOE's analysis functionality by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

3.4 Organisational Security Policies

The Organisational Security Policies identified in the following table are addressed by the TOE and the Operational Environment.

Table 8 - Organisational Security Policies

P.Type	Description
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.ACCESS	All data analyzed and generated by the TOE shall only be used for authorized purposes.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to potential intrusion data and appropriate response actions taken.
P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System must be collected.
P.INTGTY	Data analyzed and generated by the TOE shall be protected from modification.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of analysis and response activities.

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 9 - Security Objectives for the TOE

O.Type	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDACTS	The TOE must accept potential intrusion data from external data sources and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.
O.INTEGR	The TOE must ensure the integrity of all audit and Analyzer data.
O.OFLOWS	The TOE must appropriately handle potential audit and Analyzer data storage overflows.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.TIME	The TOE will provide reliable timestamps.

4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives.

Table 10 - Security Objectives of the Operational Environment

OE.Type	Description
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.INTROP	The TOE is interoperable with external data sources that supply data to the TOE.
OE.MGMTNETWORK	The operational environment will provide a segregated management network interconnecting the TOE components that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users, and limits traffic from the enterprise network entering the management network to security information from third party security devices being sent via UDP to the DA components of the TOE.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.

OE.Type	Description
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

5. Extended Components Definition

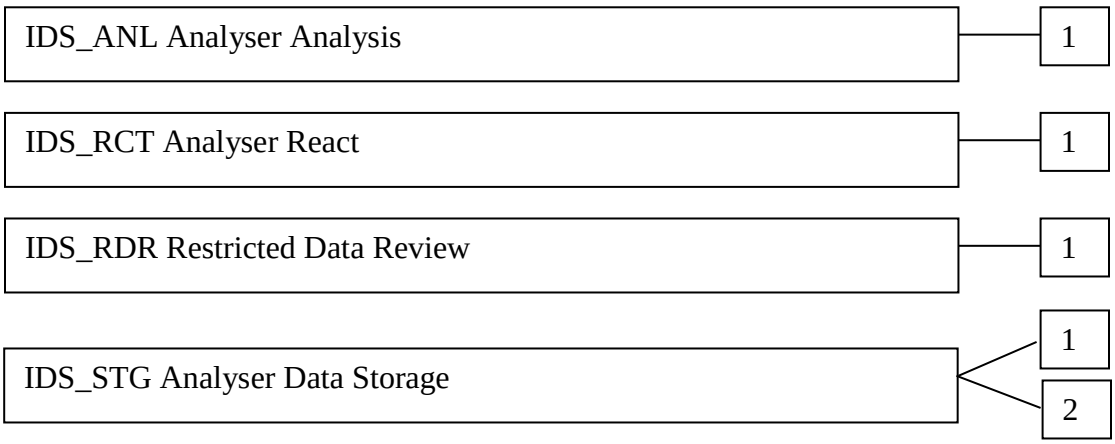
5.1 Extended Security Functional Components

5.1.1 Class IDS: Intrusion Detection

All of the components in this section are taken directly from the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments.

This class of requirements is taken from the IDS Analyzer PP to specifically address the data analysed by an IDS analyzer. The audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of analyser data and provide for requirements about analyzing, reviewing and managing the data.

Application Note: The PP does not provide hierarchy and dependency information for the extended SFRs defined in the PP. This information has been derived from the model SFRs referenced by the PP.

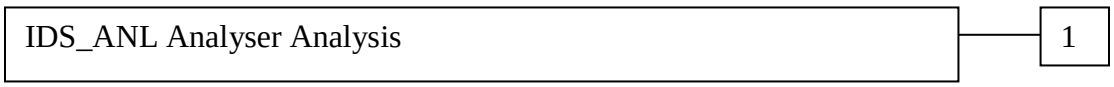


5.1.1.1 IDS_ANL Analyser Analysis

Family Behaviour:

This family defines the requirements for the TOE regarding analysis of information related to security events received from remote IT systems.

Component Levelling:



IDS_ANL.1 Analyser Analysis provides for the functionality to require TSF controlled analysis of data received from remote IT systems regarding information related to security events.

Management:

The following actions could be considered for the management functions in FMT:

a) Configuration of the analysis to be performed.

Audit:

There are no auditable events foreseen.

IDS_ANL.1 Analyser Analysis

Hierarchical to: No other components.

Dependencies: None

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all potential intrusion data received:

a) **[selection: *statistical, signature, integrity*]; and**

b) **[assignment: *other analytical functions*].**

Application Note: Statistical analysis involves identifying deviations from normal patterns of behaviour. For example, it may involve mean frequencies and measures of variability to identify abnormal usage. Signature analysis involves the use of patterns corresponding to known attacks or misuses of a system. For example, patterns of system settings and user activity can be compared against a database of known attacks. Integrity analysis involves comparing system settings or user activity at some point in time with those of another point in time to detect differences.

IDS_ANL.1.2 The TSF shall record within each analytical result at least the following information:

a) **Date and time of the result, type of result, identification of data source; and**

b) **[assignment: *other security relevant information about the result*].**

Application Note: The analytical conclusions drawn by the analyser should both describe the conclusion and identify the information used to reach the conclusion.

5.1.1.2 IDS_RCT Analyser React

Family Behaviour:

This family defines the requirements for the TOE regarding reactions to the analysis of information related to security events received from remote IT systems when an intrusion is detected.

Component Levelling:

IDS_RCT Analyser React	1

IDS_RCT.1 Analyser React provides for the functionality to require TSF controlled reaction to the analysis of data received from remote IT systems regarding information related to security events when an intrusion is detected.

Management:

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of actions.

Audit:

There are no auditable events foreseen.

IDS_RCT.1 Analyser React

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 Analyser Analysis

IDS_RCT.1.1 The TSF shall send an alarm to [assignment: *alarm destination*] and take [assignment: *appropriate actions*] when an intrusion is detected.

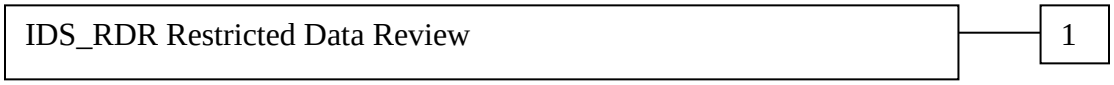
Application Note: There must be an alarm, though the ST should refine the nature of the alarm and define its target (e.g., audit log). The TSF may optionally perform other actions when intrusions are detected; these actions should be defined in the ST. An intrusion in this requirement applies to any conclusions reached by the analyser related to past, present, and future intrusions or intrusion potential.

5.1.1.3 IDS_RDR Restricted Data Review

Family Behaviour:

This family defines the requirements for the TOE regarding review of the analyser data collected by the TOE.

Component Levelling:



IDS_RDR.1 Restricted Data Review provides for the functionality to require TSF controlled review of the analyser data collected by the TOE.

Management:

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users with read access right to the analyser data records.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Basic: Attempts to read analyser data that are denied.

b) Detailed: Reading of information from the analyser data records.

IDS_RDR.1 Restricted Data Review

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 Analyser Analysis

IDS_RDR.1.1 The Analyser shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of Analyser data*] from the Analyser data.

Application Note: This requirement applies to authorised users of the Analyser. The requirement is left open for the writers of the ST to define which authorised users may access what Analyser data.

IDS_RDR.1.2 The Analyser shall provide the Analyser data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The Analyser shall prohibit all users read access to the Analyser data, except

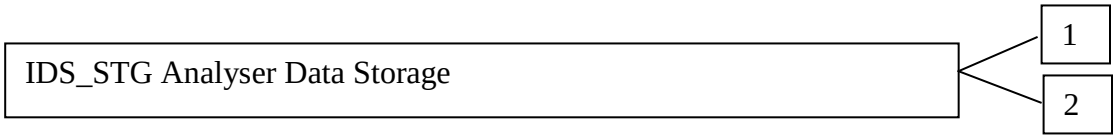
those users that have been granted explicit read-access.

5.1.1.4 IDS_STG Analyser Data Storage

Family Behaviour:

This family defines the requirements for the TOE to be able to create and maintain a secure analyser data trail.

Component Levelling:



IDS_STG.1 Guarantee of Analyser Data Availability requires that the analyser data be protected from unauthorised deletion and/or modification and defines the behaviour when specific conditions occur.

IDS_STG.2 Prevention of Analyser Data Loss defines the actions to be taken if the analyser data storage capacity has been reached.

Management: IDS_STG.1

The following actions could be considered for the management functions in FMT:

a) maintenance of the parameters that control the analyser data storage capability.

Management: IDS_STG.2

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of actions to be taken in case analyser data storage capacity has been reached.

Audit: IDS_STG.1

There are no auditable events foreseen.

Audit: IDS_STG.2

There are no auditable events foreseen.

IDS_STG.1 Guarantee of Analyser Data Availability

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 Analyser Analysis

IDS_STG.1.1 The Analyser shall protect the stored Analyser data from unauthorised deletion.

IDS_ STG.1.2 The Analyser shall protect the stored Analyser data from modification.

Application Note: Authorised deletion of data is not considered a modification of Analyser data in this context. This requirement applies to the actual content of the Analyser data, which should be protected from any modifications.

IDS_ STG.1.3 **The Analyser shall ensure that [assignment: *metric for saving Analyser data*] Analyser data will be maintained when the following conditions occur: [selection: *Analyser data storage exhaustion, failure, attack*].**

Application Note: The ST needs to define the amount of Analyser data that could be lost under the identified scenarios.

IDS_STG.2 Prevention of Analyser data loss

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 Analyser Analysis

IDS_STG.2.1 **The Analyser shall [selection: *'ignore Analyser data', 'prevent Analyser data, except those taken by the authorised user with special rights', 'overwrite the oldest stored Analyser data'*] and send an alarm if the storage capacity has been reached.**

Application Note: The ST must define what actions the analyser takes if the result log becomes full. Anything that causes the Analyser to stop analysing events may not be the best solution, as this will only affect the Analyser and not the system on which it is analysing data (e.g., shutting down the Analyser).

5.2 Extended Security Assurance Components

None

6. Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

6.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation* with the exception of completed operations.

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) *The auditable events in the following table.*

Table 11 - Auditable Events

SFR	Event	Audit Record	Details
FAU_GEN.1	Start-up and shutdown of audit functions	startup.*component* shutdown.*component*	Component
FAU_SAR.1	Reading of information from the audit records	user.report.run	Name of report
FIA_UAU.1	All use of the authentication mechanism	user.login user.logoff user.timeout	Success or failure
FIA_UID.1	All use of the identification mechanism	user.login user.login.fail user.logoff user.timeout	Failure, locked, disabled
FMT_MTD.1	Modifications to the values of TSF data	admin.account.edited admin.datasource.*action* admin.notification.*action* admin.user.add	Account name Action, Data source name Action, Notification name Account name

SFR	Event	Audit Record	Details
IDS_RDR.1	Reading analyser data	user.chart.run user.eventexplorer,run user.logexplorer.run user.alertexplorer.run user.report.run	Name of chart Name of report

FAU_GEN.1.2 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, *the additional information specified in the Details column of the preceding table*.

6.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *all authorized users* with the capability to read *all audit information via Reports* from the audit records.

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

6.1.1.3 FAU_SAR.2 Restricted 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.

6.1.1.4 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to apply *sorting* of audit data based on *date and time, subject identity, and type of event*.

6.1.1.5 FAU_STG.2 Guarantees of Audit Data Availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that *the most recent* stored audit records will be maintained when the following conditions occur: audit storage exhaustion.

6.1.1.6 FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1 The TSF shall overwrite the oldest stored audit records and *send an alarm* if the audit trail is full.

6.1.2 Identification and Authentication (FIA)

6.1.2.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when *6* unsuccessful authentication attempts occur related to *consecutive login failure attempts of an individual User Account*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *lock the User Account*.

6.1.2.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) User identity;

b) Authentication data;

c) Authorisations; and

d) Status (enabled or disabled).

6.1.2.3 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.2.4 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3 Security Management (FMT)

6.1.3.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behaviour of the functions *of analysis and reaction* to *Managers and Analysts*.

6.1.3.2 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, *and create* the *TSF data identified in the following table* **to** *the authorised identified roles identified in the following table*.

Table 12 - TSF Data Access Details

TSF Data	Managers	Analysts	Executives	Operators
Alarms	Query and Modify	Query	Query and Modify	None
Alerts	Query and Modify	Query and Modify	Query	Query and Modify
Asset Groups	Create, Modify, Query, Delete	Create, Modify, Query, Delete	None	None
Assets	Create, Modify, Query, Delete	Create, Modify, Query, Delete	None	Query for authorized Devices
Contacts	Create, Modify, Query, Delete	Create, Modify, Query, Delete	None	None
Data Retention Policies	Query, Modify	Query, Modify	None	None
Devices	Create, Modify, Query, Delete	Create, Modify, Query, Delete	None	None
Events	Query for authorized Zones and Devices	Query for authorized Zones and Devices	Query for authorized Zones and Devices	Query for authorized Zones and Devices
Networks	Create, Modify, Query, Delete	Create, Modify, Query, Delete	None	None
Notifications	Create, Modify, Query, Delete	Create, Modify, Query, Delete	None	None
Report Definitions	Create, Modify, Query, Delete any	Create, Modify, Query; Delete owned	None	Create, Modify, Query; Delete owned
Reports	Query, Create, Delete owned, shared or private	Query, Create, Delete owned or shared	Query shared	Query, Create, Delete owned or shared
Rules	Create, Modify, Query, Delete	Create, Modify, Query, Delete	None	None
System Latency Settings	Query, Modify	None	None	None
User Accounts	Create, Modify, Query	Query	None	None
Zones	Create, Modify, Query, Delete	Create, Modify, Query, Delete	None	None

6.1.3.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

a) User management;

b) Group management;

c) Device management;

d) Alert management.

6.1.3.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles *Managers, Analysts, Operators, and Executives*.

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

6.1.4 Protection of the TSF (FPT)

6.1.4.1 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time-stamps.

6.1.5 Intrusion Detection (IDS)

6.1.5.1 IDS_ANL.1 Analyser Analysis

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all potential intrusion data received:

a) statistical, signature and

b) *no other analytical functions*.

IDS_ANL.1.2 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) *associated Events*.

6.1.5.2 IDS_RCT.1 Analyser React

IDS_RCT.1.1 The TSF shall send an alarm to *the configured notification destinations for an Alert* and take *the action to generate an Alert* when an intrusion is detected.

6.1.5.3 IDS_RDR.1 Restricted Data Review

IDS_RDR.1.1 The Analyser shall provide *authorised users* with the capability to read *Alert and Event information for the Zones and Devices they are authorized to view* from the Analyser data.

IDS_RDR.1.2 The Analyser shall provide the Analyser data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The Analyser shall prohibit all users read access to the Analyser data, except those users that have been granted explicit read-access.

6.1.5.4 IDS_STG.1 Guarantee of Analyser Data Availability

IDS_STG.1.1 The Analyser shall protect the stored Analyser data from unauthorised deletion.

IDS_ STG.1.2 The Analyser shall protect the stored Analyser data from modification.

IDS_ STG.1.3 The Analyser shall ensure that *the most recent data* Analyser data will be maintained when the following conditions occur: Analyser data storage exhaustion.

6.1.5.5 IDS_STG.2 Prevention of Analyser data loss

IDS_STG.2.1 The Analyser shall overwrite the oldest stored Analyser data and send an alarm if the storage capacity has been reached.

6.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2 augmented by ALC_FLR.2. These requirements are summarised in the following table.

Table 13 - EAL2+ Assurance Requirements

Assurance Class	Component ID	Component Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
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
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 14 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components.	FAU_SAR.1	Satisfied
FAU_SAR.3	No other components.	FAU_SAR.1	Satisfied
FAU_STG.2	FAU_STG.1	FAU_GEN.1	Satisfied

SFR	Hierarchical To	Dependency	Rationale
FAU_STG.4	FAU_STG.3	FAU_STG.1	Satisfied by FAU_STG.2
FIA_AFL.1	No other components.	FIA_UAU.1	Satisfied
FIA_ATD.1	No other components.	None	n/a
FIA_UAU.1	No other components.	FIA_UID.1	Satisfied
FIA_UID.1	No other components.	None	n/a
FMT_MOF.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied
FPT_STM.1	No other components.	None	n/a
IDS_ANL.1	No other components.	None	n/a
IDS_RCT.1	No other components.	IDS_ANL.1	Satisfied
IDS_RDR.1	No other components.	IDS_ANL.1	Satisfied
IDS_STG.1	No other components.	IDS_ANL.1	Satisfied
IDS_STG.2	No other components.	IDS_ANL.1	Satisfied

7. TOE Summary Specification

7.1 FAU_GEN.1, FPT_STM.1

SE generates audits for the events specified in the table included with the FAU_GEN.1. Startup and shutdown of the audit function is equivalent to startup and shutdown of the TOE server components. The following information is included in all audit records:

- Data and time of the event,
- Type of event,
- Subject identity (if applicable),
- Outcome (success or failure) of the event (if it is not apparent from the Event type),
- Associated TOE server component,
- IP address of the associated SE Administration Console, and
- Additional information specified in the Details column of the table included with the SFR.

The TOE provides reliable time stamps for the audit records.

7.2 FAU_SAR.1, FAU_SAR.2, FAU_SAR.3

SE provides authorized users with the ability to review audit records in a human readable form via Reports. Only authorized users have access to any audit record information.

The information available via Reports may include any of the records in the audit trail. The information displayed may include any information from those audit records. The Report configuration may specify filters to select the information included in the Report.

7.3 FAU_STG.2, FAU_STG.4

Audit trails are maintained for SE.

The user access functionality of the TOE does not provide any mechanism to modify audit records. Audit records may be indirectly deleted by authorized users configuring audit retention parameters. If no space is available in the database when the TOE attempts to insert a new audit record, the oldest audit record is deleted and the new record is inserted. An alarm is generated when the audit storage space is exhausted.

Users with the Manager role may delete audit records.

7.4 FIA_AFL.1

SE tracks consecutive login failures for each defined user account. If six consecutive failures occur for any user account (for any user access TSFI), the user account is automatically disabled. After 10 minutes the account is automatically re-enabled.

7.5 FIA_ATD.1

SE maintains the following information for each user account:

- User identity;
- Authentication data (Password, number of consecutive authentication failures);

- Authorisations (User Groups, Zone associations, Device permissions); and
- Status (enabled or disabled, locked).

7.6 FIA_UAU.1, FIA_UID.1

SE requires all users to successfully identify and authenticate themselves before access is granted to any TSF data or functions.

7.7 FMT_MOF.1

SE Administration Consoles permit users that are Managers or Analysts to configure Rules, which determine what analysis is performed and what reactions are taken upon detection of configured conditions.

7.8 FMT_MTD.1

SE Administration Consoles and/or the web interface grant access to TSF data according to the roles and permissions specified in the table included with FMT_MTD.1. SE Administration Consoles may only be used by authorized users that are Managers or Analysts. Access to TSF data other than that specified in the table is prevented.

7.9 FMT_SMF.1

SE provides functionality for authorized users to manage the following items:

- Users;
- Groups;
- Devices (including Device Groups, Zones, Networks, and Contacts); and
- Alerts (including Rules).

7.10 FMT_SMR.1

All interactive users of SE are required to successfully complete I&A, at which time the role configured for the user account is associated with the user session. Per the evaluated configuration of the TOE, only the default roles are used.

7.11 IDS_ANL.1, IDS_RCT.1

As security information is received from third party security devices, the TOE normalizes the information into Events and performs statistical and signature analysis against the Events to detect configured conditions.

Analysis is performed in real time. Rules specify the analysis to be performed and Alerts are generated as the result of the analysis. Each Alert includes references to the Events that triggered the Alert. The Alert may specify that a Notification be sent to a configured destination.

7.12 IDS_RDR.1

SE provides authorized users with the ability to read Alert and Event information in a human readable form via the web interface. Access to information is limited to the Zones and Devices each user is authorized to access.

7.13 IDS_STG.1, IDS_STG.2

The user access functionality of the TOE does not provide any mechanism to modify Event records in SE. Events may only be indirectly deleted by authorized users configuring data retention parameters.

SE does not permit Alert types or associated Events to be modified, although the owner of the Alert may be assigned. Alerts may only be indirectly deleted by authorized users configuring data retention parameters.

If no space is available in the database when the TOE attempts to insert new Event or Alert information, the oldest information is deleted and the new information is inserted. When audit storage space is exhausted, an alarm is generated.

8. Protection Profile Claims

The TOE does not claim conformance to any protection profile.

9. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

9.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each organizational security policy, threat and assumption, the security objective(s) that address it.

Table 15 - Security Objectives Mapping

	O.ACCESS	O.AUDITS	O.EADMIN	O.IDACTS	O.IDAUTH	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	O.TIME	OE.CREDEN	OE.INSTAL	OE.INTROP	OE.MGMTNETWORK	OE.PERSON	OE.PHYCAL
A.ACCESS													X			
A.LOCATE																X
A.MANAGE															X	
A.MGMTNETWORK														X		
A.NOEVIL											X	X				X
A.NOTRST											X					X
A.PROTCT																X
T.COMDIS	X				X			X								
T.COMINT	X				X	X		X								
T.FALACT									X							
T.FALASC				X												
T.FALREC				X												
T.IMPCON	X		X		X							X				
T.INFLUX							X									
T.LOSSOF	X				X	X		X								
T.NOHALT	X			X	X											
T.PRIVIL	X				X			X								
P.ACCACT		X			X					X						
P.ACCESS	X				X			X								
P.ANALYZ				X												
P.DETECT		X		X												
P.INTGTY						X										
P.MANAGE	X		X		X			X			X	X			X	
P.PROTCT			X													X

The following table describes the rationale for the security objectives mappings.

Table 16 - Rationale For Security Objectives Mappings

*.TYPE	Security Objectives Rationale
A.ACCESS	The OE.INTROP objective ensures the TOE has the needed access.
A.LOCATE	The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.MGMTNETWORK	The OE.MGMTNETWORK objective ensures that a segregated network will protect the intra-TOE traffic and limit the traffic entering the segregated network from the general enterprise network.
A.NOEVIL	The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.NOTRST	The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.PROTCT	The OE.PHYCAL provides for the physical protection of the TOE hardware and software.
T.COMDIS	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.COMINT	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.FALACT	The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.
T.FALASC	The O.IDACTS objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.
T.FALREC	The O.IDACTS objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.
T.IMPCON	The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.INFLUX	The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.
T.LOSSOF	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.NOHALT	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDACTS objective addresses this threat by requiring the TOE to collect all events, including those attempts to halt the TOE.

*.TYPE	Security Objectives Rationale
T.PRIVIL	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.
P.ACCACT	The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. O.TIME will provided a time stamp for each audit.
P.ACCESS	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective provides for TOE self-protection.
P.ANALYZ	The O.IDACTS objective requires analytical processes be applied to data collected from Sensors and Scanners.
P.DETECT	The O.AUDITS and O.IDACTS objectives address this policy by requiring collection of audit and Scanner data.
P.INTGTY	The O.INTEGR objective ensures the protection of data from modification.
P.MANAGE	The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective provides for TOE self-protection.
P.PROTCT	The O.EADMIN objective requires the TOE allow for effective management of TOE data. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

9.2 Security Requirements Rationale

9.2.1 Rationale for Security Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements and/or Security Assurance Requirements demonstrating that the SFRs/SARs are suitable to address the security objectives.

The following table identifies for each TOE security objective and the SFR(s) that address it.

Table 17 - SFRs to Security Objectives Mapping

	O.ACCESS	O.AUDITS	O.EADMIN	O.IDACTS	O.IDAUTH	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	O.TIME
FAU_GEN.1		X								
FAU_SAR.1			X							
FAU_SAR.2	X				X					
FAU_SAR.3			X							
FAU_STG.2	X				X	X	X	X		
FAU_STG.4		X					X			
FIA_AFL.1	X				X					
FIA_ATD.1					X					
FIA_UAU.1	X				X					
FIA_UID.1	X				X					
FMT_MOF.1	X				X			X		
FMT_MTD.1	X				X	X		X		
FMT_SMF.1			X							
FMT_SMR.1					X					
FPT_STM.1										X
IDS_ANL.1				X						
IDS_RCT.1									X	
IDS_RDR.1	X		X		X					
IDS_STG.1	X				X	X	X	X		
IDS_STG.2							X			

The following table provides the detail of TOE security objective(s).

Table 18 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.ACCESS	The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE is required to restrict the review of Analyzer data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The Analyser is required to protect the Analyzer data from any modification and unauthorized deletion [IDS_STG.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. This process is supported by defined actions when repeated invalid credentials are supplied [FIA_AFL.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the TOE may query and add Analyzer and audit data, and authorized administrators of the TOE may query

Security Objective	SFR and Rationale
	and modify all other TOE data [FMT_MTD.1].
O.AUDITS	Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. The TOE must prevent the loss of collected data in the event the its audit trail is full [FAU_STG.4].
O.EADMIN	The TOE must provide the ability to review the audit trail of the TOE [FAU_SAR.1, FAU_SAR.3]. The TOE must provide the ability for authorized administrators to effectively manage the TOE [FMT_SMF.1]. The TOE must provide the ability for authorized administrators to view the Analyzer data [IDS_RDR.1].
O.IDACTS	The TOE is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].
O.IDAUTH	The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE is required to restrict the review of collected Analyzer data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2]. The TOE is required to protect the Analyzer data from unauthorized deletion as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The process includes defined actions when repeated invalid credentials are supplied [FIA_AFL.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the TOE may query and add Analyzer and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1].
O.INTEGR	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE is required to protect the Analyzer data from any modification and unauthorized deletion [IDS_STG.1]. Only authorized administrators of the TOE may query or add audit and Analyzer data [FMT_MTD.1].
O.OFLOWS	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE must prevent the loss of audit data in the event the its audit trail is full [FAU_STG.4]. The TOE is required to protect the Analyzer data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The TOE must prevent the loss of audit data in the event the its audit trail is full [IDS_STG.2].

Security Objective	SFR and Rationale
O.PROTCT	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE is required to protect the Analyzer data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the TOE may query and Analyzer and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1].
O.RESPON	The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1].
O.TIME	The TOE is required to provide reliable time stamps [FPT_STM.1].

9.2.2 Security Assurance Requirements Rationale

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 augmented by ALC_FLR.2 from part 3 of the Common Criteria.