Security Target

McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1

Document Version 1.1

March 25, 2013

Prepared For:

McAfee, Inc.

2821 Mission College Blvd.

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1
ST Revision	1.1
ST Publication Date	March 25, 2013
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	McAfee Enterprise Security Manager 9.1.3 Build 20121030211720 with Event Receiver9.1.3 Build 20121030211720, Enterprise Log Manager 9.1.3 Build 20121030211720, Advanced Correlation Engine 9.1.3 Build 20121030211720, Application Data Monitor 9.1.3 Build 20121030211720 and Database Event Monitor 9.1.3 Build 20121030211720 (All TOE components have the same build number.)

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)

SECTION	TITLE	DESCRIPTION
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1-1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- 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 text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *italicized* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

When not embedded in a Security Functional Requirement, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table describes the acronyms used in this document:

TERM	DEFINITION
ACE	Advanced Correlation Engine
APM	Application Data Monitor
CC	Common Criteria version 3.1
DSM	Database Event Monitor
EAL	Evaluation Assurance Level
ELM	Even Log Monitor

TERM	DEFINITION
ERC	Event Receiver
ESM	Enterprise Security Manager
ESMI	Enterprise Security Manager Interface
NTP	Network Time Protocol
OSP	Organizational Security Policy
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

Table 1-2 – Acronyms Used in Security Target

1.6 TOE Overview

The TOE is suite of software components aggregated to provide a Security Information and Event Management (SIEM) solution to the enterprise. It uses a single environment to consolidate, correlate, and report on security information from heterogeneous devices. The TOE sets policies, rules, and thresholds that will generate alerts and launch mitigations. It reduces audit effort by consolidating audit and compliance activities with a single pane for continuous governance and rapid reporting.

Note: The official name of the product is: McAfee® Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1. The product name may also be abbreviated as the *TOE*.

1.7 TOE Description

1.7.1 Overview and Physical Boundary

The TOE consists of the following components:

- McAfee Enterprise Security Manager (ESM)
- McAfee Event Receiver (ERC)
- McAfee Database Event Monitor (DSM)
- McAfee Application Data Monitor (APM)
- McAfee Advanced Correlation Engine (ACE)
- McAfee Enterprise Log Manager (ELM)

All components in the TOE architecture can scale with multiple instances of the components.

The following diagram reflects the functional blocks in the configuration:

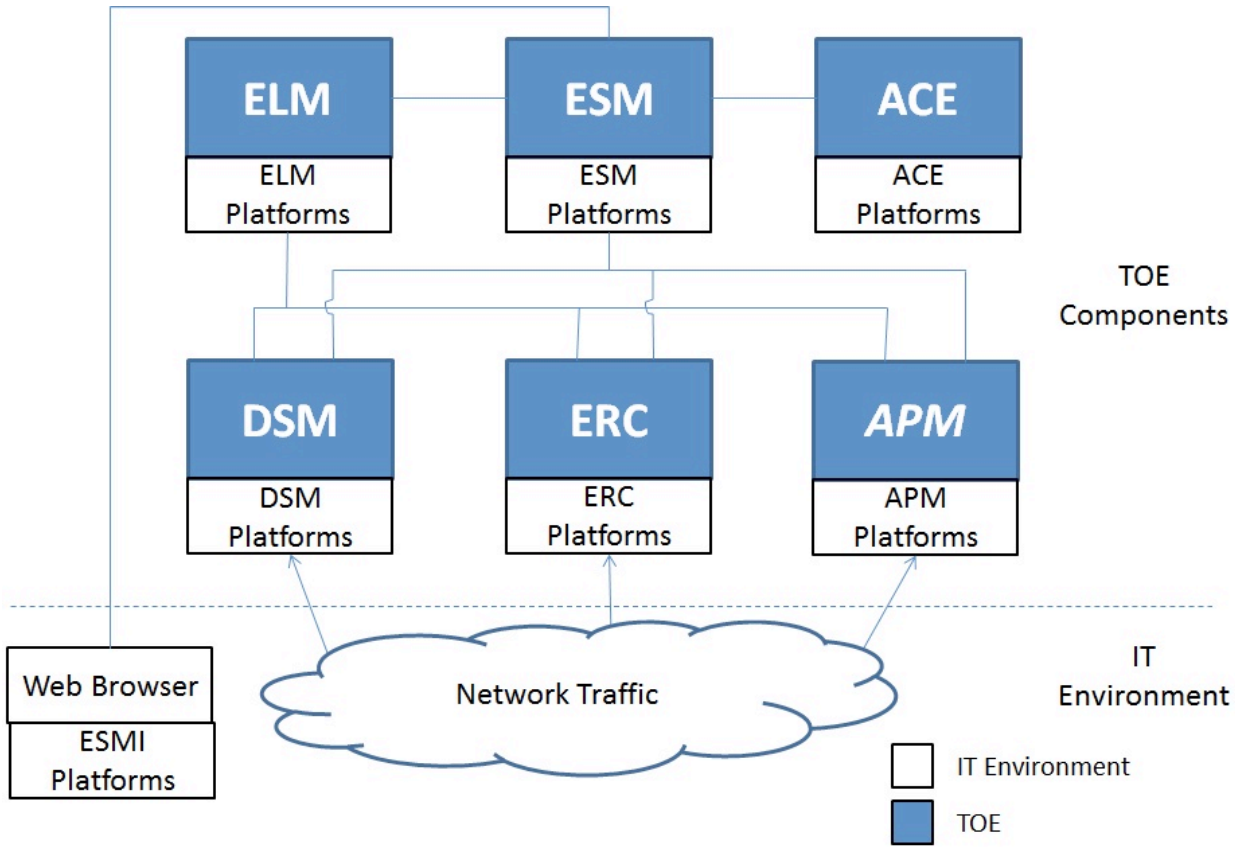


Figure 1 - TOE Boundary

The McAfee Enterprise Security Manager (ESM) system devices are intelligent network monitoring and intrusion tools to help with network forensics. McAfee Enterprise Security Manager consolidates, correlates, assesses, and prioritizes security events for both third-party and McAfee solutions. From the ELM, ESM receives the event information that the ELM has collected from the DSM, ERC and APM. It uses this data to create a real-time understanding of the threat landscape. The ESM is the management and reporting interface for the SIEM. Administrators identify and authenticate through the ESM interface. This web-based interface is known as ESMI and is presented through a web browser. It is through the ESMI that the authorized administrator has the capability to read or modify audit records. Only authorized users are permitted to access configuration, user account and audit log information or manipulate security attributes and track incidents (SIEM_RES.1(EXP). The ESM provides security definitions and watchlists to the DSM, ERC and APM.
To enhance security operations, McAfee Enterprise Security Manager also provides integrated tools for configuration and change management, case management, and centralized management of policy. (SIEM_RES.1(EXP)).

McAfee Event Receiver (ERC) collects third-party events and logs from monitored devices on the network and performs native network flow collection aggregating it for SIEM consumption. The ERC is responsible for the collection of log and event information from third-party devices including firewalls, IDS/IPS devices, UTMs, switches, routers, applications, servers and workstations, identity and

authentication systems, and vulnerability assessment scanners (SIEM_ANL.1(EXP)). McAfee Event Receiver uses a variety of collection methods including passive log collection, authenticated log collection, CEF, OPSEC, SDEE, XML, and ODBC. The collected logs are then passed on to the ELM for further processing.

McAfee Database Event Monitor (DSM) for SIEM collects database transactions by monitoring network access to database configurations and data (SIEM_ANL.1(EXP)). It sends the consolidated database activity to the ELM, the central audit repository. DSM monitors all transactions, including query results, and analyzes them against policy rules and dictionaries provided by ESM to detect which databases are storing sensitive data.

McAfee Application Data Monitor (APM) collects network traffic from applications and decodes an entire application session to Layer 7, providing a full analysis of everything from the underlying protocols and session integrity all the way up to the actual contents of the application (such as the text of an email or its attachments). This level of detail supports accurate analysis of real application use, while also enabling the ability to enforce application use policies and detect malicious, covert traffic. APM collects information from network traffic from monitored systems (SIEM_ANL.1(EXP)). APM sends the collected information to the ELM for storage.

McAfee Advanced Correlation Engine (ACE) monitors real-time data from the ESM, allowing simultaneous use of both rule-based and rule-less correlation engines to detect risks and threats before they occur. ACE provides event correlation with two dedicated correlation engines (SIEM_ANL.1(EXP)):

- A risk detection engine that generates a risk score using rule-less risk score correlation
- A threat detection engine that detects threats using traditional rule-based event correlation

McAfee Enterprise Log Manager (ELM) automates log management and analysis for all log types, including Windows Event logs, Database logs, Application logs, and Syslogs. Logs are signed and validated, ensuring authenticity and integrity. ELM receives database related logs from the DSM, log and event information from third-party devices from the ERC and application related logs from the APM. The ELM provides this data to the ESM for further analysis (SIEM_ANL.1(EXP)).

Note: Two of the components discussed in this document are abbreviated differently here than they are in the User Guides. In this document the Data Event Monitor is abbreviated as DSM and the Application Data Monitor is abbreviated as APM. In the User Guides, the abbreviations are DEM and ADM, respectively.

1.7.2 TOE Platform

All of the following platforms are included in the evaluated configuration of the TOE.

1.7.2.1 Virtual Machines

The following TOE components are available on virtual machines (VM).

- McAfee Enterprise Security Manager
- McAfee Enterprise Log Manager
- McAfee Event Receiver

- McAfee Advanced Correlation Engine

The hardware and software requirements for the operational environment to support the VM are listed in the table below:

Component	Minimum Requirement
Processor	4 cores 64-bit - Dual Core2/Nehalem or higher or AMD Dual Athlon64/Dual Opteron64 or highter
RAM	4 GB
Disk	500 GB
VM Software	VMware vSphere Hypervisor (ESXi) 4.1 and 5.0

Table 1-3 - Virtual Machine Environment Requirements

1.7.2.2 Appliances

The TOE components are also available on the following appliance models with the following TOE components:

ACE2600 (McAfee Advanced Correlation Engine)
ACE3450 (McAfee Advanced Correlation Engine)
APM3450 (McAfee Application Data Monitor)
DSM2600 (McAfee Database Event Monitor)
DSM3450 (McAfee Database Event Monitor)
DSM4600 (McAfee Database Event Monitor)
ELM4600 (McAfee Enterprise Log Manager)
ELM5600 (McAfee Enterprise Log Manager)
ELM6000 (McAfee Enterprise Log Manager)
ELMERC2600 (McAfee Enterprise Log Manager & McAfee Event Receiver)
ELMERC3450 (McAfee Enterprise Log Manager & McAfee Event Receiver)
ELMERC4600 (McAfee Enterprise Log Manager & McAfee Event Receiver)
ELMERC5600 (McAfee Enterprise Log Manager & McAfee Event Receiver)
ELMERC6000 (McAfee Enterprise Log Manager & McAfee Event Receiver)
ENMELM4600 (McAfee Enterprise Security Manager & McAfee Receiver Log Manager combos)
ENMELM5600 (McAfee Enterprise Security Manager & McAfee Receiver Log Manager combos)
ENMELM6000 (McAfee Enterprise Security Manager & McAfee Receiver Log Manager combos)
ERC1250 (McAfee Event Receiver)
ERC2600 (McAfee Event Receiver)
ERC3450 (McAfee Event Receiver)
ERC4600 (McAfee Event Receiver)
ETM5600 (McAfee Enterprise Security Manager)
ETM6000 (McAfee Enterprise Security Manager)
ETMX4 (McAfee Enterprise Security Manager)
ETMX6 (McAfee Enterprise Security Manager)

Each appliance model uses the following hardware and software:

Component	Minimum Requirement
Processor	4-8 cores (2) Intel® Xeon® Processor E5-2670 (20M Cache, 2.60 GHz)
Chassis	Integrated Intel Server System R2312GZ4GC4
RAM	16, 64 or 96GB DDR3 1333 Mhz ECC

Component	Minimum Requirement
Disk	1-4 @ 2 TB
Operating System	McAfee-customized Linux operating system

Table 1-4 - Appliance Hardware

The only significant difference between the appliance models is the TOE component software loaded on them.

1.7.3 Hardware and Software Supplied by the IT Environment

The following table identifies the minimum system requirements for McAfee ESM Interface (ESMI) platforms when managing the ESM via the web client for components provided by the IT Environment:

Component	Minimum Requirement
Processor	4 cores 64-bit - Dual Core2/Nehalem or higher or AMD Dual Athlon64/Dual Opteron64 or higher
Operating system	Windows 2008 Server Windows 7 SP1
Browser	IE 7.x Firefox 3.0 Chrome 12.0.742.91
Flash Player	11.2.x.x

Table 1-5 – Hardware and Software Requirements for IT Environment for ESMI Platforms

Several features within the ESMI use popup windows when uploading or downloading files. It is recommended that the popup blocker for the IP address or host name of your ESM be disabled.

1.7.4 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following table:

TSF	DESCRIPTION
Security Management	The TOE provides administrators with the capabilities to configure, monitor and manage the TOE to fulfill the Security Objectives. Security Management principles relate to management of access control policies as well as management of events and incidents. Administrators configure the TOE with the ESM interface via Web-based connection.

TSF	DESCRIPTION
Security Audit	The TOE generates reports that show data from events and flows managed on the ESM. These reports can be configured in either HTML or PDF format and delivered to 1) a single user or a group of users or 2) saved to the ESM, and/or 3) saved to a remote location. Additionally, the TOE supports the provision of log data from each system component, such as user login/logout and incident/ticket management actions. It also records security events such as failed login attempts, etc. Audit trails can be stored for later review and analysis. Audit data is also collected by the TOE from the various devices that send event data, and the TOE analyzes this information against a set of correlation rules and filters.
User Data Protection	The TOE enforces discretionary access rules using an access control list with user attributes.
Identification and Authentication	The TOE enforces individual I&A in conjunction with group/role based I&A mechanisms. Operators must successfully authenticate (validated via IT Environment) using a unique identifier and password prior to performing any actions on the TOE.
Incident Management	The TOE enforces functions that analyze security event data and incident workflow.

Table 1-6 – Logical Boundary Descriptions

1.7.5 TOE Security Functional Policies

The TOE supports the following Security Functional Policy:

1.7.5.1 Administrative Access Control SFP

The TOE implements an access control SFP named *Administrative Access Control SFP*. This SFP determines and enforces the privileges associated with operator roles. An authorized administrator can define specific services available to administrators and users via the ESM.

1.7.6 TOE Product Documentation

The TOE includes the following product documentation:

- McAfee Enterprise Security Manager Interface 9.1.3 ESM/Event Receiver VM Users Guide
- McAfee Enterprise Security Manager Interface 9.1.3 ESMI Users Guide
- McAfee Enterprise Security Manager Interface 9.1.3 ESMI Quick Start Guide
- McAfee Enterprise Security Manager Interface 9.1.3 ESMI Setup and Installation Guide
- McAfee ESM Release 9.1.3 Release Notes

2 Conformance Claims

2.1 CC Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 extended and Part 3 conformant and augmented with ALC_FLR.2.

2.2 PP Claim

The TOE does not claim conformance to any registered Protection Profile.

2.3 Package Claim

The TOE claims conformance to the EAL2 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 3 (July 2009). The TOE does not claim conformance to any functional package.

2.4 Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

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

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.NO_AUTH	An unauthorized user may gain access to the TOE and alter the TOE configuration.
T.NO_PRIV	An authorized user of the TOE exceeds his/her assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data.

Table 3-1 – Threats Addressed by the TOE

The IT Environment does not explicitly addresses any threats.

3.2 Organizational Security Policies

The TOE meets the following organizational security policies:

ASSUMPTION	DESCRIPTION
P.EVENTS	All events from network-attached devices shall be monitored and reported.
P.INCIDENTS	Security events correlated and classified as incidents should be managed to resolution

Table 3-2 – Organizational Security Policies

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.MANAGE	Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.
A.NOEVIL	Administrators of the TOE and users on the local area network are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation
A.LOCATE	The processing platforms on which the TOE resides are assumed to be located within a facility that provides controlled access
A.CONFIG	The TOE is configured to receive all events from network-attached devices.
A.TIMESOURCE	The TOE has a trusted source for system time via NTP server

Table 3-3 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.CAPTURE_EVENT	The TOE shall collect data (in the form of events) from security and non-security products with accurate timestamps and apply analytical processes to derive conclusions about events.
O.MANAGE_INCIDENT	The TOE shall provide a workflow to manage incidents.
O.SEC_ACCESS	The TOE shall ensure that only those authorized users and applications are granted access to security functions and associated data.

Table 4-1 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.TIME	The TOE operating environment shall provide an accurate timestamp (via reliable NTP server).
OE.ENV_PROTECT	The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed
OE.PERSONNEL	Authorized administrators are non-hostile and follow all administrator guidance and must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any operator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.
OE.PHYSEC	The facility surrounding the processing platform in which the TOE resides must provide a controlled means of access into the facility

Table 4-2 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

OBJECTIVES / ASSUMPTIONS/ THREATS/ POLICIES	O.CAPTURE_EVENT	O.MANAGE_INCIDENT	O.SEC_ACCESS	OE.TIME	OE.ENV_PROTECT	OE.PERSONNEL	OE.PHYSEC
A.CONFIG						✓	
A.MANAGE						✓	
A.NOEVIL						✓	
A.LOCATE							✓
A.TIMESOURCE				✓			
T.NO_AUTH			✓		✓	✓	✓
T.NO_PRIV			✓				
P.EVENTS	✓			✓		✓	
P.INCIDENTS		✓		✓		✓	

Table 4-3 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

4.3.1.1 Rationale for Security Threats to the TOE

ASSUMPTION/THREAT/POLICY	RATIONALE
A.CONFIG	This assumption is addressed by OE.PERSONNEL, which ensures that the TOE is managed and administered to receive all events from network-attached devices. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner
A.MANAGE	This assumption is addressed by OE.PERSONNEL, which ensures that the TOE is managed and administered by in a by appropriately trained personnel. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner
A.NOEVIL	This assumption is addressed by OE.PERSONNEL, which ensures that administrators of the TOE and users on the local area network are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner
A.LOCATE	This assumption is addressed by OE.PHYSEC which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility
A.TIMESOURCE	This assumption is addressed by OE.TIME, which ensures the provision of an accurate time source.

ASSUMPTION/THREAT/POLICY	RATIONALE
T.NO_AUTH	This threat is countered by the following: • O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications and • OE.ENV_PROTECT, which ensures that TSF components cannot be tampered with or bypassed and • OE.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner and • OE.PHYSEC, which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility
T.NO_PRIV	This threat is countered by O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications.
P.EVENTS	This organizational security policy is enforced by • O.CAPTURE_EVENT, which ensures that the TOE collects security events from security products and non-security products deployed within a network and applies analytical processes to derive conclusions about the events and • OE.TIME, which provides support for enforcement of this policy by ensuring the provision of an accurate time source and • OE.PERSONNEL, which ensures that authorized administrators are non-hostile and follow all administrator guidance and ensures that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any operator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.

ASSUMPTION/THREAT/POLICY	RATIONALE
P.INCIDENTS	This organizational security policy is enforced by • O.MANAGE_INCIDENT, which ensures that the TOE will provide the capability to provide case management functionality to manage the resolution of incidents and • OE.TIME, which ensures that the TOE operating environment shall provide an accurate timestamp (via reliable NTP server) and • OE.PERSONNEL, which ensures that authorized administrators are non-hostile and follow all administrator guidance and ensures that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any operator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.

Table 4-4 – Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

A class of Security Information and Event Management (SIEM) requirements was created to specifically address the data collected, analyzed, and managed by a SIEM solution. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this class is to address the unique nature of SIEM solutions and provide requirements about collecting events and managing incidents. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

5.1 Rationale for Extended Components

The SIEM class was created because the Common Criteria standard classes do not have any Security Functional Requirements (SFR) that accurately described the unique capabilities of a security information and event management system.

5.2 Definition of Extended Components

5.2.1 Class SIEM: Incident Management

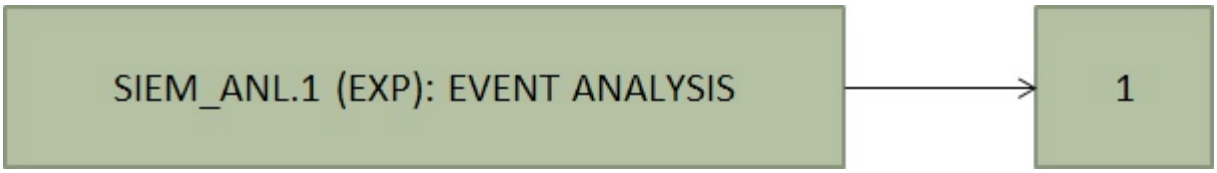
Incident Management functions provide the capability to analyze security event data and incident workflow.

5.2.1.1 Event Analysis SIEM_ANL.1 (EXP)

Family Behavior

This family defines the requirements for security event analysis functionality.

Component Leveling



SIEM_ANL.1 (EXP) Event Analysis provides the analysis of security event data.

Management: SIEM_ANL.1 (EXP)

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

a) Configuration of the analysis to be performed

Audit: SIEM_ANL.1 (EXP)

There are no auditable events foreseen.

SIEM_ANL.1 (EXP) Event Analysis

Hierarchical to: No other components

Dependencies: No dependencies

SIEM_ANL.1.1 (EXP) The TSF shall perform the [assignment: list of functions] function(s) on event data.

5.2.1.2 SIEM_RES.1 Incident Resolution (EXP)

Family Behavior

This family defines the requirements for security incident functionality.

Component Leveling

SIEM_RES.1 (EXP) provides the incident resolution workflow functionality.

Management: SIEM_RES.1 (EXP)

There are no management activities foreseen.

Audit: SIEM_RES.1 (EXP)

There are no auditable events foreseen.

SIEM_RES.1 (EXP) Incident Resolution

Hierarchical to: No other components

Dependencies: No dependencies

SIEM_RES.1.1 (EXP) The TSF shall provide a means to track work items that are necessary to resolve an incident.

6 Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
	FAU_STG.1	Audit Protection
User Data Protection	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security Attribute Based Access Control
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UID.2	User Identification before Any Action
Security Management	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Incident Management	SIEM_ANL.1 (EXP)	Event Analysis
	SIEM_RES.1 (EXP)	Incident Resolution

Table 6-1 – TOE Security Functional Requirements

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) [items specified in column 2 in Table 6-2 - Table of Auditable Events]

SFR	EVENT

SFR	EVENT
FAU_GEN.1	None.
FAU_SAR.1	Reading of information from the audit records.
FAU_STG.1	None.
FDP_ACC.1	None.
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP.
FIA_ATD.1	None.
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided;
FMT_MSA.1	All modifications of the values of security attributes.
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules.
FMT_MTD.1	All modifications to the values of TSF data.
FMT_SMF.1	Use of the management functions.
FMT_SMR.1	Modifications to the group of users that are part of a role;
SIEM_ANL.1 (EXP)	None.
SIEM_RES.1 (EXP)	None.

Table 6-2 - Table of Auditable Events

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, [no other audit relevant information].

6.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [the Administrator] with the capability to read [all audit data generated within the TOE] 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_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

6.1.2 Information Flow Control (FDP)

6.1.2.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the [Administrative Access Control SFP] on [

Subjects: Administrators and users

Objects: User Privileges, User Account Attribute, Audit Logs, Correlation Rules

Operations: all user actions as defined in FMT_SMF.1]

6.1.2.2 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the [Administrative Access Control SFP] to objects based on the following: [

Subjects: Administrators and users

Subject Attributes: User Identity, Authentication Status, Privileges

Objects: User Privileges, User Account Attribute, Audit Logs, Correlation Rules

Object Attributes: None

Operations: all user actions as defined in FMT_SMF.1]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [verify the operator's User Identity, Authentication Status, Privileges].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [no additional rules].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [invalidation of username/password].

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [User Identity, Authentication Status, Privileges].

6.1.3.2 FIA_UID.2 User Identification before Any Action

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.

6.1.3.3 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [Administrative Access Control SFP] to restrict the ability to [*change default, query, modify, delete, clear*] the security attributes [User accounts, privileges] to [Administrator].

6.1.3.4 FMT_MSA.3 Static Attribute Initialization

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

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

6.1.3.5 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [control] the [data described in Table 6-3 – Management of TSF data below] to [Administrator]:

DATA	CHANGE DEFAULT	QUERY	MODIFY	DELETE	CLEAR
User Privileges	✓	✓	✓	✓	✓
User Account Attributes		✓	✓		
Audit Logs		✓			
Correlation Rules			✓		

Table 6-3 – Management of TSF data

6.1.3.6 FMT_SMF.1 Specification of Management Functions

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

a) Create accounts

b) Modify accounts

c) Define User privileges

d) Change Default, Query, Modify, Delete, Clear the attributes associated with the Administrative Access Control SFP

e) Modify the behavior of the Administrative Access Control SFP

f) Manage security incidents

g) Manage correlation rules].

Application Note: Security incidents are groups of events that represent an actionable security incident, plus associated state and meta-information. Incidents are created manually or through Correlation rules.

6.1.3.7 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Administrator, User].

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

6.1.4 Incident Management (SIEM)

6.1.4.1 SIEM_ANL.1 Event Analysis (EXP)

SIEM_ANL.1.1 The TSF shall perform the [collecting, filtering and correlation] function(s) on event data.

6.1.4.2 SIEM_RES.1 Incident Resolution (EXP)

SIEM_RES.1.1 The TSF shall provide a means to track work items that are necessary to resolve an incident.

6.2 Security Assurance Requirements

The Security Assurance Requirements for this evaluation are listed in Section 6.3.4 – Security Assurance Requirements.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

SFR \ OBJECTIVE	O.CAPTURE_EVENT	O.MANAGE_INCIDENT	O.SEC_ACCESS

FAU_GEN.1	✓	✓	
FAU_SAR.1	✓	✓	
FAU_STG.1			✓
FDP_ACC.1			✓
FDP_ACF.1			✓
FIA_ATD.1			✓
FIA_UID.2			✓
FMT_MSA.1			✓
FMT_MSA.3			✓
FMT_MTD.1			✓
FMT_SMF.1			✓
FMT_SMR.1			✓
SIEM_ANL.1 (EXP)	✓		
SIEM_RES.1 (EXP)		✓	

Table 6-4 – Mapping of TOE Security Functional Requirements and Objectives

6.3.2 Dependency Rationale

This ST satisfies all the security functional requirement dependencies of the Common Criteria. The table below lists each SFR to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

SFR CLAIM	DEPENDENCIES	DEPENDENCY MET	RATIONALE
FAU_GEN.1	FPT_STM.1	YES	Satisfied by the Operational Environment (OE.TIME)
FAU_SAR.1	FAU_GEN.1 FPT_STM.1	YES	FPT_STM.1 satisfied by the Operational Environment (OE.TIME)
FAU_STG.1	FAU_GEN.1	YES	
FDP_ACC.1	FDP_ACF.1	YES	
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	YES	
FIA_ATD.1	N/A	N/A	
FIA_UID.2	N/A	N/A	
FMT_MSA.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	YES	
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	YES	
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	YES	
FMT_SMF.1	N/A	N/A	

SFR CLAIM	DEPENDENCIES	DEPENDENCY MET	RATIONALE
FMT_SMR.1	FIA_UID.1	YES	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
SIEM_ANL.1 (EXP)	N/A	N/A	
SIEM_RES.1 (EXP)	N/A	N/A	

6.3.3 Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

Objective	RATIONALE
O.CAPTURE_EVENT	The objective to ensure that the TOE will collect events from security products and non-security products deployed within a network and applies analytical processes to derive conclusions about the events is met by the following security requirements: • FAU_GEN.1 and FAU_SAR.1 define the auditing capability for events and administrative access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs • SIEM_ANL.1 (EXP) ensures that the TOE performs analysis on all security events received from network devices
O.MANAGE_INCIDENT	The objective to ensure that the TOE provides a workflow to manage incidents is met by the following security requirements: • FAU_GEN.1 and FAU_SAR.1 define the auditing capability for incidents and administrative access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs • SIEM_RES.1 (EXP) ensures that the TOE provides the capability to manage status and track action items in the resolution of incidents

Objective	RATIONALE
O.SEC_ACCESS	This objective ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications. • FAU_STG.1 requires that the stored audit records will be protected from unauthorized deletion and will prevent unauthorized modifications. • FDP_ACC.1 requires that all user actions resulting in the access to TOE security functions are controlled • FDP_ACF.1 supports FDP_ACC.1 by ensuring that access to TOE security functions, , audit logs, and account attributes is based on the user privileges and their allowable actions • FIA_UID.2 requires the TOE to enforce identification of all users prior to configuration of the TOE • FIA_ATD.1 specifies security attributes for users of the TOE • FMT_MTD.1 restricts the ability to query, add or modify TSF data to authorized users. • FMT_MSA.1 specifies that only privileged administrators can access the TOE security functions and related configuration data • FMT_MSA.3 ensures that all default values of security attributes are restrictive in nature as to enforce the access control policy for the TOE. The Administrator must explicitly grant access privileges to users – the default tis no access. • FMT_SMF.1 and FMT_SMR.1 support the security functions relevant to the TOE and ensure the definition of an authorized administrator role.

Table 6-5 – Rationale for TOE SFRs to Objectives

6.3.4 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2). The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
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: Lifecycle Support	ALC_CMC.2	Use of a CM system

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Remediation Procedures
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 6-6 – Security Assurance Requirements at EAL2

6.3.5 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 2. EAL2+ was chosen because it is based upon good commercial development practices with thorough functional testing. EAL2+ provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

6.3.6 Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Security Architecture: McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1
ADV_TDS.1: Basic Design	Basic Design: McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1
AGD_OPE.1 Operational User Guidance	McAfee Enterprise Security Manager Interface 9.1.3 ESM/Event Receiver VM Users Guide McAfee Enterprise Security Manager Interface 9.1.3 ESMI Users Guide McAfee Enterprise Security Manager Interface 9.1.3 ESMI Quick Start Guide Operational User Guidance and Preparative Procedures Supplement: McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
AGD_PRE.1 Preparative Procedures	McAfee Enterprise Security Manager 9.1.3 ESMI Setup and Installation Guide McAfee Enterprise Security Manager Interface 9.1.3 ESM/Event Receiver VM Users Guide McAfee Enterprise Security Manager Interface 9.1.3 ESMI Users Guide McAfee Enterprise Security Manager Interface 9.1.3 ESMI Quick Start Guide Operational User Guidance and Preparative Procedures Supplement: McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1
ALC_DEL.1 Delivery Procedures	Secure Delivery Processes and Procedures: McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1
ALC_FLR.2: Flaw Reporting	*McAfee Product Flaw Remediation Process*
ATE_COV.1: Evidence of Coverage	Test Plan and Coverage Analysis: McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1
ATE_FUN.1 Functional Testing	Test Plan and Coverage Analysis: McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1
ATE_IND.2 Independent Testing - sample	Test Plan and Coverage Analysis: McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1

Table 6-7 – Security Assurance Rationale and Measures

7 TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

7.1 TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Incident Management

7.2 Security Audit

Each TOE component generates three types of logs. These logs are used to store audit records (in the event log) and to store collected data event information (in the traffic alert log and in the traffic flow log). The event log contains records not related to traffic alerts or traffic flow such as TOE management events. The event log is the TOE's log containing the audit trail.

- *event log*
  - Generated by ESM (when using GUI) and other TOE components (when receiving commands from ESM)
  - Records generated by TOE components are sent to ESM periodically in batches for storage and review on ESM. The records are protected by the Operational Environment (OE.ENV_PROTECT) during transmission using the proprietary stackless control protocol called SEM (Secure Encrypted Management). The communication between the ESM and other TOE components is always initiated by the ESM. The audit trail is protected by the ESM subsystem and is protected from unauthorized logical access by restricting access to the ESM web-based GUI interface that is used to read from the audit trail. There are no interfaces (not ESM web-based GUI interfaces or otherwise) to modify audit records stored in the audit trail.

The audit records received by the ESM are stored in the ESM subsystem's event log. The ESM subsystem's event log is also known as the audit trail. The audit trail is protected by the ESM subsystem. The audit trail is protected from unauthorized logical access by restricting access to the ESM web-based GUI interface that is used to read from the audit trail. There are no interfaces (not ESM web-based GUI interfaces or otherwise) to modify audit records stored in the audit trail.

The ESM provides web-based GUI interfaces to configure auditable events. Events are grouped into categories that correspond to sets of ESM GUI dialogs, menus, and screens. Each category will have a

checkbox that allows the user to enable/disable logging of each event category. If a category is disabled, no events that are a part of that category will be logged. The auditable event types include:

- Authentication category - Login, logout, and any user account changes
- Backup category - Database backup process
- Blacklist category - Sending blacklist entries to the device
- Device category - Any device changes or communications such as getting events, flows and logs
- Event Forwarding category - Event forwarding changes or errors
- Health Monitor category - Device status events
- Notifications category - Notification changes or errors
- Policy category - Policy management and applying policies
- Rule Server category - Download and validation of rules downloaded from the rule server
- System category - System setting changes and table rollover logging
- Views category - Changes to views and queries

In addition to the list of events above, it should be noted that audit is always on and hence the start-up and shutdown audit is fulfilled vacuously, however there is a system log that identifies the start and stop of various TOE components.

The TOE provides the Administrator with the capability to read all audit data generated within the TOE via the ESM interface. The GUI provides a suitable means for an Administrator to interpret the information from the audit log.

The A.TIMESOURCE is added to the assumptions on operational environment, and OE.TIME is added to the operational environment security objectives. The time and date provided by the operational environment are used to form the timestamps. The TOE ensures that the audit trail data is stamped when recorded with a dependable date and time received from the OE (operating system). In this manner, accurate time and date is maintained on the TOE.

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1
- FAU_SAR.1
- FAU_STG.1

7.3 User Data Protection

The TOE enforces the Administrative Access Control SFP by only allowing Administrators to access system reports, component audit logs, TOE configuration, operator account attributes. The TOE additionally enforces the Administrative Access Control SFP by verifying user Identity, authentication status, and privileges. The TOE also explicitly denies access based on invalidation of username/password combination from the IT Environment.

The User Data Protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.1
- FDP_ACF.1

7.4 Identification and Authentication

The ESM interface provides user interfaces that administrators may use to manage TOE functions. The ESM interface provides web-based access to TOE functions through supported web browsers. The operating system and the database in the TOE Environment are queried to individually authenticate administrators or users. The TOE maintains authorization information that determines which TOE functions an authenticated administrator or user (of a given role) may perform.

The TOE maintains the following list of security attributes belonging to individual users:

- User Identity (i.e., user name)
- Authentication Status (whether the IT Environment validated the username/password)
- Privileges

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1
- FIA_UID.2

7.5 Security Management

The TOE enforces that only authorized Administrators have the capability to query, modify, or delete accounts / privileges. Only authorized Administrators can control user privileges, user accounts attributes, and audit logs. The TOE provides two user roles: Administrator and User and associates users to their roles.

The TOE provides restrictive default values for security attributes by requiring the Administrator to explicitly allow access to Users. Only the Administrator may be able to change defaults. The TOE supports the following management functions:

- Create accounts
- Modify accounts
- Define User privileges
- Change Default, Query, Modify, Delete, Clear the attributes associated with the Administrative Access Control SFP
- Modify the behavior of the Administrative Access Control SFP
- Manage security incidents
- Manage correlation rules.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MSA.1
- FMT_MSA.3
- FMT_MTD.1
- FMT_SMF.1
- FMT_SMR.1

7.6 Incident Management

The TOE collects, filters and correlates event data. The ERC collects third-party events, the DSM collects database transactions, and the APM collects network traffic. The TOE provides users with the capability to filter security event data queries and searches. Correlation automates analysis of event data to find patterns of interest. The TOE enables users to define correlations between events through the definition of rules that define these patterns of interest.
Alarms provide real-time alerts when a user defined condition occurs. When an alarm is triggered, it will show up in the Alarms log and generate an optional visual alert. A triggered alarm can be viewed, acknowledged and deleted. An acknowledged alarm no longer appears in the Alarms log but will still be listed on the Triggered Alarms view until it is deleted.
The TOE provides the capability for automating and tracking incident response processes. The TOE tracks security problems from identification through resolution by allowing the creation of case management policies. The Case Management feature allows an administrator to assign and track work items and support tickets associated with network events.

The Incident Management function is designed to satisfy the following security functional requirements:

- SIEM_ANL.1 (EXP)
- SIEM_RES.1 (EXP)

End of Document