Security Target

Securonix Security Intelligence Platform 4.0

Document Version 1.12

January 9, 2015

Prepared For:

Securonix

5777 W. Century Blvd

Suite #838

Los Angeles, CA 90045

www.securonix.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), the Securonix Security Intelligence Platform 4.0. 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.

 Copyright © Securonix

Table of Contents

List of Tables

List of Figures

1 Introduction

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

1.1 ST Reference

ST Title	Security Target: Securonix Security Intelligence Platform 4.0
ST Revision	1.12
ST Publication Date	January 9, 2015
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	Securonix Security Intelligence Platform 4.0.5 Build:20140612

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)

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 Description

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 *underlined 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.

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 provides a list of terms and acronyms used within this document:

TERM	DEFINITION
CC	Common Criteria version 3.1 (ISO/IEC 15408)
DBMS	Database Management System
DLP	Data Loss Prevention
EAL	Evaluation Assurance Level
GB	Gigabits
Gbps	Gigabits per second

GHz	Gigahertz
HDD	Hard disk drive
HR	Human Resources
IAM	Identify and Access Management
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OS	Operating System
OSP	Organizational Security Policy
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RPM	Revolutions per minute
SATA	Serial Advance Technology Attachment
SIEM	Security Incident and Event Management
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TB	Terabytes
TOE	Target of Evaluation
TSF	TOE Security Function

Table 1-2 – Document Terms and Acronyms

1.6 TOE Overview

The TOE is the Securonix Security Intelligence Platform 4.0, is an enterprise application written in Java and supports many major databases. The TOE is a software-only TOE. The TOE has native integration with a majority of products in the security industry – Log Management, SIEM, Database Monitoring, Identity Management, DLP and Privileged Access Management solutions. The TOE type is a security incident and event management (SIEM) system used to manage risk.

The TOE uses a proprietary signature-less threat detection and flexible risk scoring algorithms to accurately detect and score rogue transactions, access privileges and security events. The technology utilizes intelligent behavior based risk analytics and peer group analysis techniques that are capable of even detecting unseen attacks launched from within or outside the perimeter of the organization.

The TOE consumes identity, access, activity and transaction data from critical applications or existing security tools and identifies high-risk users, activity, transactions and access for focused, proactive threat identification and risk mitigation.

The TOE enables security professionals to take a risk-based approach to security. Use the TOE as an enterprise risk management platform to find abnormal patterns in user access, activities and violations and get more context for your current SIEM, DLP, logging, monitoring, or IAM solutions.

1.6.1 Identity Correlation

The TOE correlates all activity, transaction, access, and user accounts to a single person or identity for meaningful business context and a unified 360° view of the enterprise IT infrastructure. Integrate the TOE's technology easily into your IT infrastructure using native connectors and standard protocols. The advanced correlation engine is one of its kind in the industry and uses a hybrid of static rules and fuzzy

logic to determine the best possible match along with suggestions and confidence levels for unmatched identities.

1.6.2 Access Risk Intelligence

The TOE brings the power of Peer Group Analysis to the access management domain. By focusing on identifying access outliers, the solution will help you establish security controls and meet your access related compliance goals while eliminating rogue access privileges.

Use the TOE's Access Risk Manager module to identify the rogue access privileges held by users that require remediation. With a targeted risk based approach to access management, The TOE enables risk based certifications, risk based access requests and even clean up of access on legacy applications.

1.6.3 Activity Risk Intelligence

The TOE provides two innovative techniques to detect and rank suspicious activities.

- Behavior Based Detection
- Peer Group Analysis Based Detection

The TOE brings the first behavior-based risk analytics engine to the information security market. The engine consumes activity data, identifies normal behavior patterns for users, peer groups, and resources using over 120 different dimensions such as time slices, frequency, network sources and many more. This capability allows for "signature-less" security management that self-adapts to the environment and pro-actively identifies suspicious behavior before it is too late.

The TOE uses peer group analysis techniques to dynamically detect suspicious activities conducted by users. This technique is especially useful in the detection and ranking of threats originating from within the organization or by business partners accessing applications

1.6.4 Event Risk Intelligence

The TOE adds business intelligence to events generated by security solutions. By correlating events to user identities, the TOE solution provides business context to events and reduces the unnecessary noise, thus enabling targeted remediation. The engine consumes security events, correlates the events to user identities and performs risk analytics.

Use the TOE's Security Event Risk Analytics module to add business intelligence to security events. By using a comprehensive security policy engine that spans user identity, access, activity and event data, the TOE solution performs continuous monitoring for enterprise security policies.

1.6.5 Security Policy Engine

The TOE provides a self-service policy engine for custom policy development or industry standard out-of-the box risk and compliance policies. Context aware policies automatically apply business and identity changes such as role and HR status changes to the context of security alerts or activity for immediate and proactive management.

1.6.6 Reporting and Analytics

The TOE leverages its data rich repository of correlated information and analytical tools to give the user complete flexibility in creating custom views and reports while performing powerful security analytics.

The TOE provides reports including high privileged account usage reports, User access privilege report,

Account Critical Activity report for meeting compliance mandates

1.6.7 TOE Scope

The TOE contains several components that perform Security Audit. User Data Protection, Identification and Authentication, Security Management, and Incident Management functions. The TOE executes on a general-purpose computing platform and interfaces with monitored system in the Operational Environment to collect security incident and event data. The TOE also interfaces with an Identity Source in the Operational Environment to obtain user identity information.

1.7 TOE Description

The TOE is composed on Java applets running in an application server (part of the Operational Environment) and interfaces with a DBMS for data storage. The following are the major components of the TOE:

- Data Collector
- Monitoring
- Identity Correlation
- Threat Analysis
- Event Correlation
- Alerts and Reporting

These components work together to perform the following actions:

- Import user identities
- Import access privileges
- Accept events from multiple event collectors
- Support web interface for administrator and user interaction
- Run reports
- Run behavior based suspect analysis
- Run Access Outlier analysis
- Run Risk analysis
- Each Event Collector (Universal Forwarder) is responsible for the following tasks:
  - Collect, normalize and correlate event logs from multiple resources
  - Forward the event logs to the Master Node

The figure below shows the TOE in the surrounding Operational Environment.

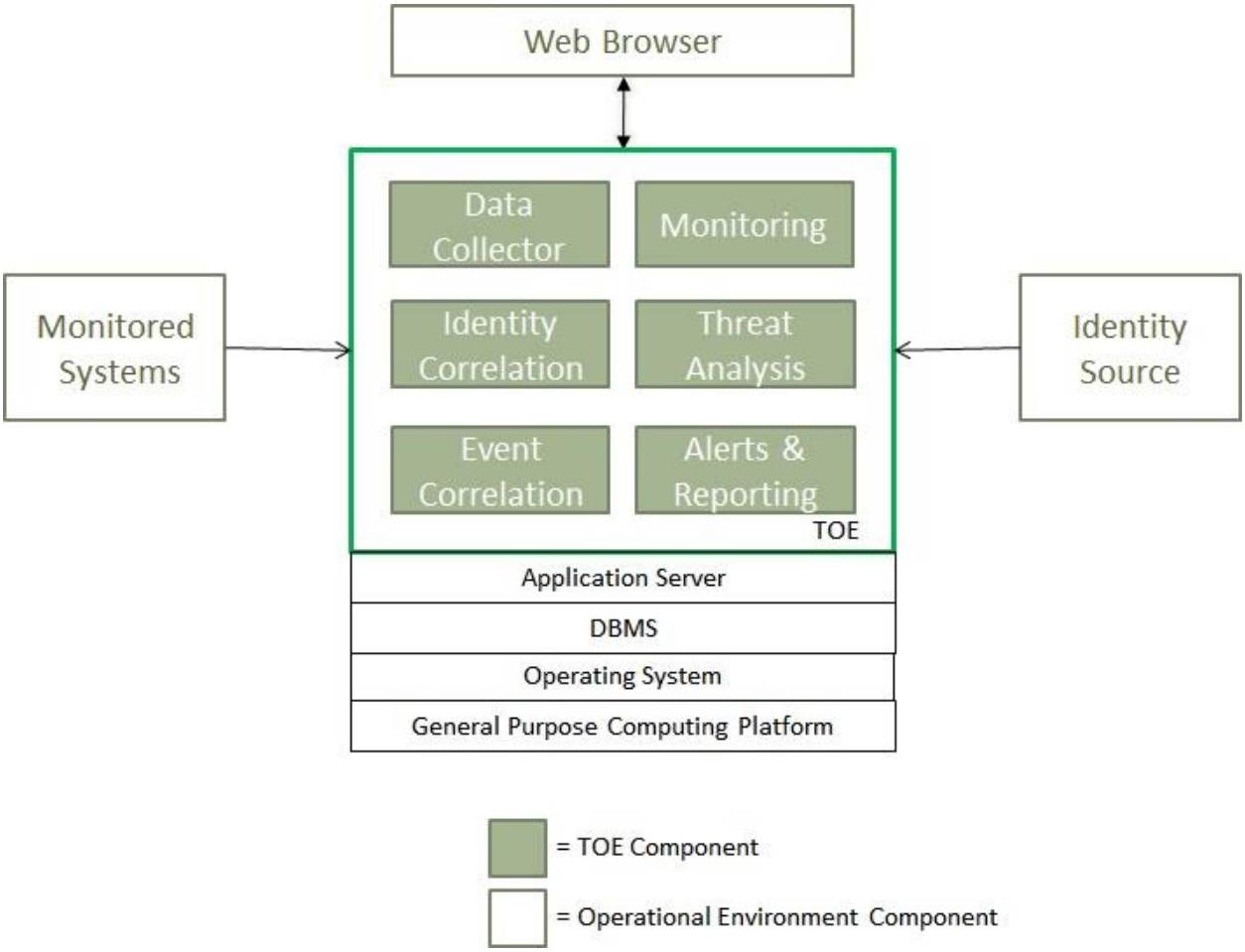

Figure 1 - TOE Diagram

1.7.1 Data Collector

- Collect, normalize and correlate event logs from multiple resources
- Forward the event logs to the central log repository

1.7.2 Monitoring

- Accept events from multiple event collectors

1.7.3 Identity Correlation

- Import user identities
- Import access privileges

1.7.4 Threat Analysis

- Run behavior based suspect analysis
- Run Access Outlier analysis
- Run Risk analysis

1.7.5 Event Correlation

- Correlate event logs from multiple resources

1.7.6 Alerts and Reporting

- Run reports

1.7.7 TOE Documentation

The TOE includes the following documentation:

TITLE	REFERENCE
Release Notes: Version 4.0	http://community.securonix.com/index.php/RTI_4.0_Release_Notes
Deployment Guide: Version 4.0	http://community.securonix.com/index.php/4.0_Deployment_Guide/4.0_Deployment_Guide
Install Guide: Version 4.0	http://community.securonix.com/index.php/4.0_Install_Guide/Introduction
User Guide: Version 4.0	http://community.securonix.com/index.php/4.0_RTI_UG_Chapter_1:Table_of_Contents
Administrator Guide: Version 4.0	http://community.securonix.com/index.php/4.0_RTI_AG_Administrator_Guide_Preface

1.7.8 Logical Boundaries

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 sections.

TSF	DESCRIPTION
Security Audit	The TOE generates reports on the event analysis activities. Additionally, the TOE records administrator login/logout success and failures.
User Data Protection	The TOE enforces discretionary access controls to users for TOE functionality and data. The TOE also enforces the import of user data from outside the TOE.
Identification and Authentication	The TOE enforces individual I&A in conjunction with role based I&A mechanisms. Administrators must successfully authenticate using a unique identifier and password prior to performing any actions on the TOE.
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 incidents and tickets. The TOE also allows the administrator to • review/query audit data,

TSF	DESCRIPTION
	• modify the behavior of data collection, and • restrict access to TOE data to the appropriate authorized user/authorized role.
Incident Management	The TOE provides the capability to collect, analyze, and respond to security events in accordance to policies established and maintained by authorized administrators.

Table 1-3 - Logical Boundary

1.7.9 TOE Security Function Policies

The TOE supports the following Security Function Policy:

1.7.9.1 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 Management Console.

1.7.10 TOE Software Requirement

In order to comply with the evaluated configuration, the following software components must be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	Securonix Security Intelligence Platform 4.0

Table 1-4 – Evaluated Configuration for the TOE

1.8 Hardware and Software Provided by Operational Environment

The TOE is a Java EE application that runs on Java-supported application servers. The TOE also requires a database. The hardware and software platform requirements are shown in the tables below.

OPERATING SYSTEMS	VERSION	JRE VERSION
CentOS 64 bit	6.5	1.7

Table 1-5 – Supported Operating Systems for the TOE

APPLICATION SERVERS	VERSION
Apache Tomcat - Securonix hardened	7.0 Date Nov 1 1980 03:16:25 Number 2010

Table 1-6- Supported Application Servers

DATABASE SERVERS	VERSION
MySQL 64 bit	5.5.x and later

Table 1-7 - Supported Database Servers

The Securonix administrator user interface is presented to the client within a web browser. The following Browsers are supported:

WEB BROWSERS	VERSION
Mozilla Firefox	6 or Greater

Table 1-8 - Supported Web Browsers

HARDWARE	SPECIFICATIONS
General Purpose Computer	Minimum Intel i7 Processor, 16GB RAM, 1TB Internal Storage

Table 1-9 - Supported Hardware

1.8.1 Identity Sources

The TOE typically imports user identity and access information from outside sources.

HARDWARE	SOFTWARE
General Purpose Computer	Flat files containing user identity information.

Table 1-10 - Identity Sources

1.8.2 Monitored Systems Platforms

The systems monitored by the TOE must have the following Operational Environment requirements:

HARDWARE	SOFTWARE
General Purpose Computer	Unix log files

Table 1-11 - Monitored Systems Requirements

2 Conformance Claims

2.1 CC Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 4 (September 2012) Part 2 extended and Part 3 conformant at Evaluation Assurance Level 2 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 4 (September 2012). 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 assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used
- 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

3.1 Threats

The TOE and IT environment address the threats identified in the following sections.

3.1.1 Threats Addressed by the TOE and the IT Environment

The TOE addresses the following threats:

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.

3.2 Organizational Security Policies

The organizational security policies relevant to the operation of the TOE are as follows:

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.

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The assumptions are ordered into three groups: personnel, physical environment, and operational assumptions.

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 operational environment must be managed in accordance with assurance requirements documentation for delivery, operation, and user/administrator guidance. The following specific conditions are assumed to exist in an environment where the TOE is

employed.

3.3.1 Personnel Assumptions

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.

3.3.2 Physical Environment Assumptions

A.LOCATE	The processing platforms on which the TOE resides are assumed to be located within a facility that provides controlled access.
A.PROTECT	The processing platforms on which the TOE resides and the TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

3.3.3 Operational Assumptions

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.

4 Security Objectives

This section describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

O.CAPTURE_EVENT	The TOE shall collect data (in the form of events) from security and non-security products 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.

4.2 Security Objectives for the Operational Environment

The IT security objectives for the operational environment are addressed below:

OE.ENV_PROTECT	The Operational Environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.
OE.TIME	The Operational Environment shall provide an NTP server to provide a trusted source of time to the TOE
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.

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.

OBJECTIVE / THREATS/ ASSUMPTIONS	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.PROTECT					✓		
A.TIMESOURCE				✓			
T.NO_AUTH			✓		✓	✓	✓
T.NO_PRIV			✓				
P.EVENTS	✓			✓		✓	
P.INCIDENTS		✓		✓		✓	

Table 4-1 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

4.3.1 Rationale for Security Objectives of the TOE

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.

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.
P.INCIDENTS	This organizational security policy is enforced by O.MANAGE_INCIDENT, which ensures that the TOE will provide the capability to provide workflow functionality to manage the resolution of incidents.

4.3.2 Rationale for Security Objectives of the Operational Environment

The IT security objectives for the Operational environment are addressed below:

A.TIMESOURCE	This assumption is addressed by OE.TIME, which ensures the provision of an accurate time source.
A.PROTECT	This assumption is addressed by OE.ENV_PROTECT, which ensures that TSF components cannot be tampered with or bypassed.
A.MANAGE	This assumption is addressed by 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.
A.NOEVIL	This assumption is addressed by 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.
A.CONFIG	This assumption is addressed by 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.
A.LOCATE	This assumption is addressed by OE.PHYSEC, which ensures that the TOE is operated in an environment that will protect it from unauthorized access and physical threats and attacks that can disturb and corrupt the information generated.
T.NOAUTH	This threat is countered by the following:

- This threat is countered by OE.ENV_PROTECT, which ensures that TSF components cannot be tampered with or bypassed.
- OE.PERSONNEL, which ensures that the TOE is managed and administered in a secure manner by 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.
- OE.PHYSEC, which ensures that the TOE is operated in an environment that will protect it from unauthorized access and physical threats and attacks that can disturb and corrupt the information generated.

P.EVENTS This policy is addressed by the following:

- OE.TIME provides support for enforcement of this policy by ensuring the provision of an accurate time source.
- OE.PERSONNEL provides support for the enforcement of this policy by ensuring that the TOE is managed and administered in a secure manner by 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.

P.INCIDENTS This policy is addressed by the following:

- OE.TIME provides support for enforcement of this policy by ensuring the provision of an accurate time source.
- OE.PERSONNEL provides support for the enforcement of this policy by ensuring that the TOE is managed and administered in a secure manner by 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.

5 Extended Components Definition

5.1 Incident Management (SIM) Class of SFRs

The purpose of this class of requirements is to address the unique nature of the incident management products and provide for the requirements about detecting and responding to incidents on protected IT resources.

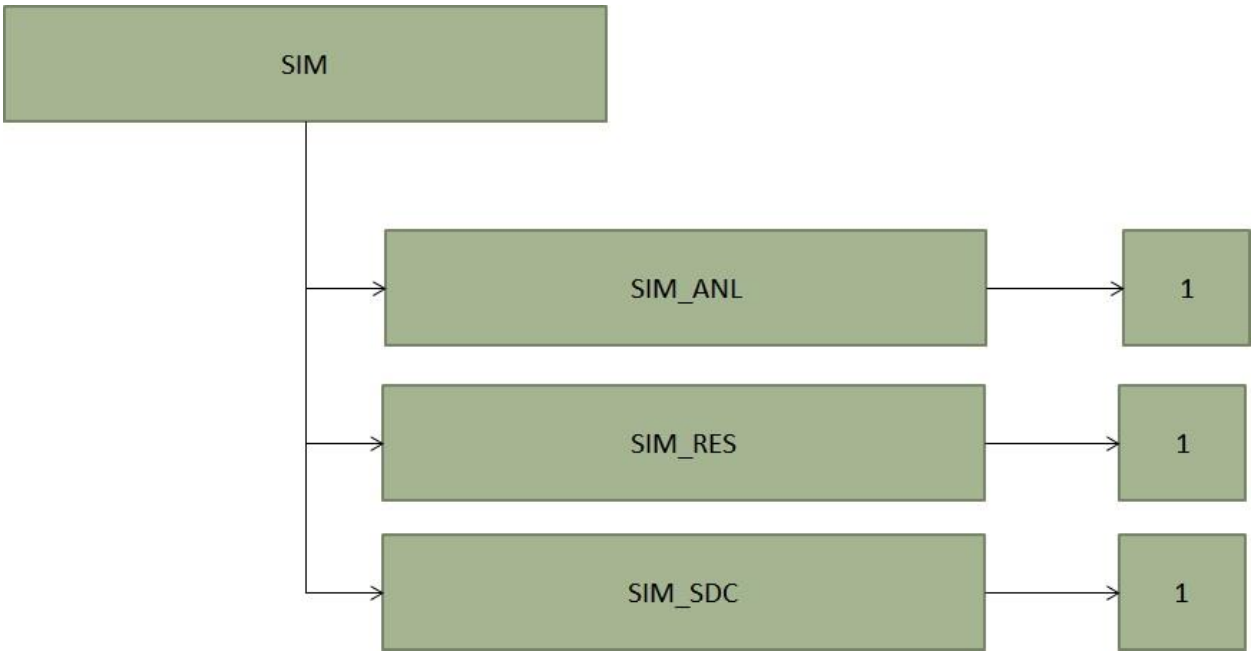

Figure 2 – SIM Class

5.1.1 SIM_ANL Event Analysis (EXT)

Family Name

SIM_ANL Event Analysis

Family Behavior

This family defines the requirements for security event analysis.

Component Leveling

Figure 3 - SIM_ANL.1 – Security Event Analysis

Management:

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

a) Configuration of the actions to be taken.

Audit:

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

a) Basic: Action taken in response to detection of an event.

SIM_ANL.1 Event Analysis (EXT)

Hierarchical to: No other components.

Dependencies: No dependencies

SIM_ANL.1.1 (EXT) The TSF shall perform [assignment: list of actions] analysis function(s) on data collected.

5.1.2 SIM_RES Incident Resolution (EXT)

Family Name

SIM_RES Incident Resolution

Family Behavior

This family defines the requirements for security incident resolution.

Component Leveling

Figure 4 - SIM_RES.1 – Security Incident Resolution

Management:

There are no management activities foreseen.

Audit:

There are no auditable events foreseen.

SIM_RES.1 Incident Resolution (EXT)

Hierarchical to: No other components.

Dependencies: No dependencies

SIM_RES.1.1 (EXT) The TSF shall provide a means to track work items that are necessary to resolve an

incident.

5.1.3 SIM_SDC Security Data Collection (EXT)

Family Name

SIM_SDC Security Data Collection

Family Behavior

This family defines the requirements for security data collection.

Component Leveling

Figure 5 - SIM_SDC.1 - Security Data Collection

Management:

There are no management activities foreseen.

Audit:

There are no auditable events foreseen.

SIM_SDC.1 Security Data Collection (EXT)

Hierarchical to: No other components.

Dependencies: No dependencies

SIM_SDC.1.1 (EXT) The TSF shall provide a means to collect security event data from managed systems.

6 Security Requirements

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

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were extended, all of which are summarized in the following table.

TSF	SFR	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
User Data Protection	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security Attribute Based Access Control
	FDP_ITC.1	Import of User Data without Security Attributes
Identification and Authentication	FIA_UAU.2	User Authentication before Any Action
	FIA_UID.1	Timing of Identification
Security Management	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Incident Management	SIM_ANL.1 (EXT)	Event Analysis
	SIM_RES.1 (EXT)	Incident Resolution
	SIM_SDC.1 (EXT)	Security Data Collection

Table 6-1 – TOE Security Functional Requirements

6.1 TOE Security Functional Requirements

The SFRs defined in this section are derived from Part 2 of the CC unless otherwise noted with "(EXT)" following the requirement description. Rationale for the extended requirements can be found in Section 6.5 - Rationale for Extended Security 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) [Administrator login/logout events,

d) Administrator activity].

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, 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 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 [Administrator login/logout events and adminitrator activity event logs] 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.

6.1.2 User Data Protection (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: All Administrators

Objects: User account information, policies

Operations: all operations].

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: All Administrators

Objects: User account information, policies

Operations: all operations].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [administrators are granted access based on permissions set by their role].

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 [no additional rules].

6.1.2.3 FDP_ITC.1 Import of User Data without Security Attributes

FDP_ITC.1.1 The TSF shall enforce the [Administrative Access Control SFP] when importing user data, controlled under the SFP, from outside the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [no additional importation control rules].

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_UAU.2 User Authentication before Any Action

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

6.1.3.2 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow [none] 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.

6.1.4 Security Management (FMT)

6.1.4.1 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 create, *modify and delete* the security attributes [user accounts, user roles, policies] to [an authorized administrator].

6.1.4.2 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.

6.1.4.3 FMT_SMF.1 Specification of Management Functions

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

- [Create user accounts
- Modify user accounts

- Delete user accounts
- Create user roles
- Modify user roles
- Delete user roles
- Create policies
- Modify policies
- Delete policies].

6.1.4.4 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.

6.1.5 Incident Management (SIM)

6.1.5.1 SIM_ANL.1 Event Analysis (EXT)

SIM_ANL.1.1 (EXT) The TSF shall perform [correlation] analysis function(s) on data collected.

6.1.5.2 SIM_RES.1 Incident Resolution (EXT)

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

6.1.5.3 SIM_SDC.1 Security Data Collection (EXT)

SIM_SDC.1.1 (EXT) The TSF shall provide a means to collect security event data from managed systems.

6.2 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are derived from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.2. 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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
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
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ASE: Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
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 6-2 – Security Assurance Requirements at EAL2 Augmented with ALC_FLR.2

6.3 Security Requirements Rationale

6.3.1 Summary of TOE Security 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	✓	✓	
FDP_ACC.1			✓
FDP_ACF.1			✓
FDP_ITC.1	✓	✓	
FIA_UAU.2			✓
FIA_UID.1			✓
FMT_MSA.1			✓
FMT_MSA.3			✓
FMT_SMF.1		✓	
FMT_SMR.1		✓	
SIM_ANL.1 (EXT)	✓		
SIM_RES.1 (EXT)		✓	
SIM_SDC.1 (EXT)	✓		

Table 6-3 – Mapping of TOE Security Functional Requirements and Objectives

6.3.2 Rationale for Security Functional Requirements of the TOE Objectives

This section provides the rationale for how the TOE security objectives are satisfied by the security functional requirement claims.

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:

OBJECTIVE	RATIONALE
	• 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 • FDP_ITC.1 allows the import of user data from outside the TOE (such as threat, vulnerability, and attack activity information provided by Symantec Global Intelligence Network) to help ensure the latest vulnerabilities and threats are reported • SIM_ANL.1 (EXT) ensures that the TOE performs analysis on all security events received from network devices • SIM_SDC.1 (EXT) ensures that the TOE collects security event data 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 • FDP_ITC.1 allows the import of user data from outside the TOE (such as threat, vulnerability, and attack activity information provided by Symantec Global Intelligence Network) to help ensure the latest vulnerabilities and threats are reported • FMT_SMF.1 and FMT_SMR.1 support the security functions relevant to the TOE and ensure the definition of an authorized administrator role • SIM_RES.1 (EXT) ensures that the TOE provides the capability to manage status and track action items in the resolution of incidents
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. • FDP_ACC.1 requires that all user actions resulting in the access to TOE security functions and configuration data are controlled • FDP_ACF.1 supports FDP_ACC.1 by ensuring that access to TOE security functions, configuration data, audit logs, and account attributes is based on the user privilege level and their allowable actions • FIA_UAU.2 and FIA_UID.1 require the TOE to enforce identification and authentication of all users prior to configuration

OBJECTIVE	RATIONALE
	of the TOE • FMT_MSA.1 specifies that only privileged administrators can access the TOE security functions and related configuration data • FMT_MSA.3 ensures that the default values of security attributes are restrictive in nature as to enforce the access control policy for the TOE

Table 6-4 – Sufficiency of Security Requirements

6.4 TOE Summary Specification Rationale

The following table provides a mapping of Security Functional Requirements to TOE Security Functions (TSF):

TOE SECURITY FUNCTION / TOE SFR	SECURITY AUDIT	USER DATA PROTECITON	IDENTIFICATION AND AUTHENTICATION	SECURITY MANAGEMENT	INCIDENT MANAGEMENT
FAU_GEN.1	✓				
FAU_SAR.1	✓				
FDP_ACC.1		✓			
FDP_ACF.1		✓			
FDP_ITC.1		✓			
FIA_UAU.2			✓		
FIA_UID.1			✓		
FMT_MSA.1				✓	
FMT_MSA.3				✓	
FMT_SMF.1				✓	
FMT_SMR.1				✓	

 Copyright © Securonix

TOE SECURITY FUNCTION / TOE SFR	SECURITY AUDIT	USER DATA PROTECITON	IDENTIFICATION AND AUTHENTICATION	SECURITY MANAGEMENT	INCIDENT MANAGEMENT
SIM_ANL.1 (EXT)					✓
SIM_RES.1 (EXT)					✓
SIM_SDC.1 (EXT)					✓

Table 6-5 – Mapping of Security Functional Requirements to TOE Security Functions

6.4.1 Sufficiency of TOE Security Functions

This section provides appropriate justification that the TOE Security Functions are suitable to meet the TOE Security Functional Requirement and that when implemented, contributes to meeting that requirement.

SFR	RATIONALE TO SUPPORT SUFFICIENCY OF SECURITY FUNCTION
FAU_GEN.1	This TOE SFR is satisfied by the Security Audit function, which generates audit logs and reports various security events.
FAU_SAR.1	This TOE SFR is satisfied by the Security Audit function by enabling only authorized users to review and query the audit logs and reports.
FDP_ACC.1	This TOE SFR is satisfied by the User Data Proteciton function, which permits each user to be assigned a privilege level and the respective privileges for that level and only allow access to event and incident management functions for which the user is authorized.
FDP_ACF.1	This TOE SFR is satisfied by the User Data Proteciton function by permitting TOE access based on the privileges assigned a specific privilege level.
FDP_ITC.1	This TOE SFR is satisfied by the User Data Protection function, which process the information entering the system. The TOE allows the import of user data from outside the TOE (e.g., user identity servers).
FIA_UAU.2	This TOE SFR is satisfied by the Identification and Authentication security function by requiring operators to successfully authenticate themselves using a unique identifier and password prior to performing any action on the TOE.
FIA_UID.1	This TOE SFR is satisfied by the Identification and Authentication security

	function by requiring operators to successfully identify themselves using a unique identifier.
FMT_MSA.1	This TOE SFR is satisfied by Security Management functions, which provide the TOE Administrators with authority and ability to modify and delete user accounts and their privileges. These security functions also provide control (via configuration) over the security functions of the TOE.
FMT_MSA.3	This TOE SFR is satisfied by Security Management function, which allows the TOE Administrator to change default settings for each operator and privilege level.
FMT_SMF.1	This TOE SFR is satisfied by Security Management function by providing the TOE Administrator the capability for the administrator to select the type of information structure with respect to selected services to be monitored and processed, and the ability to install and configure the TOE services. The Security Management function also provides the capability to modify operator accounts and privilege levels.
FMT_SMR.1	This TOE SFR is satisfied by Security Management function, which assigns each operator to the role of Administrator or User, the latter of which has a subset of Administrator services. These subset services are defined by the Administrator at the time the account is created.
SIM_ANL.1 (EXT)	This TOE SFR is satisfied by the Incident Management security function, which provides mechanisms to correlate, and view event data from monitored devices.
SIM_RES.1 (EXT)	This TOE SFR is satisfied by the Incident Management security function, which provides mechanisms to report and manage incidents to track their resolution.
SIM_SDC.1 (EXT)	This TOE SFR is satisfied by the Incident Management security function, which provides mechanisms to collect security data from monitored devices.

Table 6-6 – Sufficiency of TOE Security Functions

6.5 Rationale for Extended Security Requirements

A class of Security Information Management (SIM) requirements was created to specifically address the data collected, analyzed, and managed by a SIM solution. The purpose of this class is to address the unique nature of SIM 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.

6.6 Rationale for IT Security Requirement 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.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	No other components	FPT_STM.1	See note below table
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied
FDP_ACC.1	No other components	FDP_ACF.1	Satisfied
FDP_ACF.1	No other components	FDP_ACC.1 FMT_MSA.3	Satisfied
FDP_ITC.1	No other components	FDP_ACC.1 FMT_MSA.3	Satisfied
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied
FIA_UID.1	No other components	None	Satisfied
FMT_MSA.1	No other components	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	Satisfied
FMT_MSA.3	No other components	FMT_SMR.1 FMT_MSA.1	Satisfied
FMT_SMF.1	No other components	None	Not applicable
FMT_SMR.1	No other components	FIA_UID.1	Satisfied
SIM_ANL.1 (EXT)	No other components	None	Not applicable
SIM_RES.1 (EXT)	No other components	None	Not applicable
SIM_SDC.1 (EXT)	No other components	None	Not applicable

 Copyright © Securonix

Table 6-7 – TOE SFR Dependency Rationale

Note: Although the FPT_STM.1 requirement is a dependency of FAU_GEN.1, it has not been included in this TOE because the timestamping functionality is provided by the IT Environment (OE.TIME). The audit mechanism within the TOE uses this timestamp in audit data, but the timestamp function is provided by the operating system in the IT Environment.

6.6.1 Security Assurance Requirements

This section identifies the Lifecycle , Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: Securonix Security Intelligence Platform 4.0
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: Securonix Security Intelligence Platform 4.0
ADV_TDS.1: Basic Design	Basic Design: Securonix Security Intelligence Platform 4.0
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Securonix Security Intelligence Platform 4.0
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Securonix Security Intelligence Platform 4.0
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: Securonix Security Intelligence Platform 4.0
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: Securonix Security Intelligence Platform 4.0
ALC_DEL.1: Delivery Procedures	Delivery Procedures: Securonix Security Intelligence Platform 4.0
ALC_FLR.2: Flaw Reporting	Flaw Reporting: Securonix Security Intelligence Platform 4.0
ATE_COV.1: Evidence of Coverage	Security Testing: Securonix Security Intelligence Platform 4.0
ATE_FUN.1: Functional Testing	Security Testing: Securonix Security Intelligence Platform 4.0

Table 6-8 – Security Assurance Measures

6.6.1.1 Rationale for TOE Assurance Requirements Selection

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

The general level of assurance for the TOE is:

1. 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.
2. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.
3. Consistent with current best practice for tracking and fixing flaws as well as providing fixes to customers to meet ALC_FLR.2.

7 TOE Summary Specification

This section presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

7.1 TOE Security Functions

The security functions described in the following subsections fulfill the security requirements that are defined in Section 6.1 – TOE Security Functional Requirements. The security functions performed by the TOE are as follows:

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

7.1.1 Security Audit

The TOE records successful and unsuccessful administrator login and logout events. These audit records include the user name, date and time of the event, and the result. The TOE also records all administrator activity.

The TOE provides a means to review the audit logs. The audit events can be reviewed through the TOE's Configuration – Auditing menu screen. This displays the timestamp, administrator user name, action, description, IP address, status, and other details. This log will record all of the events of an administrator accessing the TOE.

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

- FAU_GEN.1
- FAU_SAR.1

7.1.2 User Data Protection

The TOE enforces the discretionary access control policy to limit access to management functions and data to administrators only. Operations on user accounts and policies require that administrators are granted the proper permissions through their assigned roles. Through the TOE's Configuration – Access Control menu screens, the administrator can create and modify users and their access control permissions. These roles and their permissions are enforced by the TOE.

Policy management is performed by administrators by defining policy violation conditions. Administrators can monitor user policy violations by using the TOE's Detect – Policy Violations menu screen.

The following table describes the parameters available in policies.

Field	Description
Policy Name	Provide a short name for the Policy. This name may be displayed on the Dashboard.
Description	Provide a description for the Policy. The Policy description will be shown on the dashboard when you hover on the Policy name.
Dashboard Display	If checked, the policy will be displayed on the Risk Command Center dashboard.
Initiate Workflow	If checked, the policy violation will trigger a workflow and generate a Case ID.
Criticality	Assigns a Criticality to the Policy. The Criticality of the Policy affects the weight assigned to the Risk of the User that violates the Policy.
Category	Type of Policy from the drop down menu. • DLP Policy • Configuration • Alert • Identiy Events • Fraud • Security Policies
Applies To	Select if the Security Policy affects the risk for a User or Resource.
Owner	Owner for the Policy.
Remediator	Remediator for the Policy.

Table 7-1 - Policy Parameters

Administrators are those users who log into Securonix – they are created manually and assigned specific access privileges within Securonix. Users are the enterprise network users whose activities are being monitored and analyzed by the Securonix platform.

User information can be imported by administrators from external identity sources such as LDAP and Oracle IDM. An administrator can configure the connection type for the external identity source then schedule the import job. Import jobs can be executed periodically or on demand.

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

- FDP_ACC.1
- FDP_ACF.1
- FDP_ITC.1

7.1.3 Identification and Authentication

The TOE requires administrators to be successfully identified and authenticated before being granted access to TOE functions. Administrators must login with a valid user identifier and password. Administrators are not allowed access to TOE functions or data without first properly identifying and authenticating with the TOE through the administrator console.

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

- FIA_UAU.2
- FIA_UID.1

7.1.4 Security Management

Administrators with the appropriate permissions are allowed to manage user accounts user roles, and policies. User roles are only granted permissions explicitly – the default is that roles have no permissions until the administrator grants them permissions. Users and their roles are defined and modified by administrators through the Configuration – Access Control menu screens.

There are two roles supported by the TOE – administrator and user. Administrators manage user accounts through the Manage – Users.

Administrators are assigned to specific permissions. Administrative users are managed by administrators through the Configuration – Access Control menu screens. An Administrator may be granted specified permission within the TOE. The access assigned to the administrator is an aggregated sum of the underlying privileges. Each privilege is mapped to functionality within the TOE. .

When a new role is created within the TOE, it has no underlying access privileges unless explicitly assigned by the Administrator. An administrator logging into the TOE with the specified role will only see the functionalities that he is authorized by his role.

User policy management is performed by administrators by defining policy violation conditions. Administrators create, modify, and delete policies through the Detect – Policy Violations menu screen.

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

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

7.1.5 Incident Management

The TOE collects event (incident) data from monitored devices. The TOE also has the capability to do correlation analysis and incident tracking. Once policies have been created, they can be run. When the run completes, the results will be available on the Dashboard. The High Risk users are identified and a case is opened against each of those users. The High Risk users are shown on the dashboard. To respond

to the open cases, click on Respond and choose Incidents. The cases generated against the High Risk users are assigned to people who have the power to take action against them. A user will view only those cases assigned to him/her. Users can take action against the High Risk user and close the case.

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

- SIM_RES.1 (EXT)
- SIM_ANL.1 (EXT)
- SIM_SDC.1 (EXT)