# e-Security Sentinel 5 v5.1.1
# Security Target

Release Date: November 20, 2006

Version: 0.34 Final

Prepared By: ARCA CCTL
45901 Nokes Blvd.
Sterling, VA 20166

Prepared For: e-Security
1921 Gallows Road
Suite 700
Vienna, VA 22182

Table of Contents

List of Figures

# 1 Introduction

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

## 1.1 Identification

TOE Identification: e-Security Sentinel 5 v5.1.1 [1]

ST Identification: e-Security Sentinel 5 v5.1.1 Security Target

ST Version: v0.34 (Final)

ST Publish Date: November 20, 2006

ST Authors: Rick West, ARCA CCTL, SAVVIS, Inc.

Joe Cudby, ARCA CCTL, SAVVIS, Inc.

PP Identification: N/A

## 1.2 Overview

e-Security Sentinel 5 v5.1.1 is a complete security event management system that enables you to view all of your security information in one place and report on the entire picture of the enterprise. (In the remainder of this document e-Security Sentinel 5 v5.1.1 will be referred to as the TOE or Sentinel 5) The

[1] During the CC evaluation e-Security was purchased by Novell, Inc. For the purposes of the evaluation "e-Security Sentinel 5 v5.1.1" referenced in the CC documentation is equivalent to "Sentinel from Novell Version 5.1.1". The ST reflects this change in TOE Identification and Description only.

Sentinel 5 modules are as follows in support of security features:

Sentinel Server

Server based, Sentinel 5 receives standardized alert information collected from any networked source throughout the enterprise's heterogeneous network environment, prioritizes it and performs correlation – all in real-time. Based on its very flexible agent configuration options, Sentinel 5 can be configured to collect data from security products on the market and provides the flexibility to collect data from new technologies and products as business requirements evolve. Through Sentinel Server, security teams can monitor the entire trusted network, and perform reporting. The Sentinel Server is managed through the Sentinel 5 Console.

Sentinel Wizard

Sentinel Wizard enables administrators to develop and customize Agents to monitor any device* in the distributed enterprise. Wizard's drag-and-drop interface allows administrators to create rules-based Agents to collect, filter and normalize data from any networked source and communicate relevant information to the Sentinel server for correlation and the Sentinel Control Center for review. e-Security delivers the ability to create Agents that collect security alert information from any device* or application throughout the enterprise's heterogeneous network environment and normalize it into standard fields for correlation and analysis. *The security management software collects data from diverse security devices and programs that allow data to be collected via one of the following methods: Log files (local and via Syslog), ODBC or JDBC processes, TCP sockets, serial ports, OPSEC LEA, Cisco RDEP, and SNMP.

Sentinel Advisor

Note: The security functionality of the Sentinel Advisor is not included within the CC evaluation. Thus, the installation and use of the Sentinel Advisor component will remove the TOE from its evaluated configuration. Sentinel Advisor is an optional module that provides incident response through the mapping of collected data from Enterprise IDS's to a large collection of known threats. Advisor brings pre-packaged incident response capabilities to e-Security Sentinel 5. Without it the administrator creates their own mappings according to their own experience.

In addition to the Sentinel Control Center console, historical reporting can also be performed using a third party software BusinessObjects Enterprise XI. The reporting engine uses its mechanisms to extract data from the database and integrates the displaying of reports into the Sentinel Control Center using HTML documents over an HTTP connection. BusinessObjects Enterprise XI is not part of the TOE and therefore not included with the CC evaluation. Installation or use will remove the TOE from its evaluated configuration.

e-Security Sentinel 5 v5.1.1 also includes software to integrate into 3rd party products, HP Service Desk or Remedy. This is not part of the TOE and therefore not included with the CC evaluation. Installation or use will remove the TOE from its evaluated configuration.

The Command Line version of the Sentinel Data Manager is also not part of the evaluated configuration. The use of the Command Line version of the Sentinel Data Manager will remove the TOE from its evaluated configuration.

See section 2 for the exact TOE description and environmental definitions.

## 1.3 Common Criteria (CC) Conformance Claim

The TOE is Common Criteria Version 2.3 (ISO/IEC 15408:2005) Part 2 extended and Part 3 conformant at EAL2.

## 1.4 Organization

| Section | Title | Description |
|---|---|---|
| 1 | Introduction | Provides an overview of the security target. |
| 2 | TOE Description | Defines the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE. |
| 3 | TOE Security Environment | Contains the threats, assumptions and organizational security policies that affect the TOE. |
| 4 | Security Objectives | Contains the security objectives the TOE is attempting to meet. |
| 5 | IT Security Requirements | Contains the functional and assurance requirements for this TOE. |
| 6 | TOE Summary Specification | A description of the security functions and assurances that this TOE provides. |
| 7 | PP Claims | Protection Profile Conformance Claims |
| 8 | Rationale | Contains pointers to the rationales contained throughout the document. |

**Table 1 - ST Organization and Description**

## 1.5 Document Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify these operations.

Assignment: indicated with **bold text**

Selection: indicated with underlined text

Refinement: indicated with ***bold text and italics***

Iteration: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MSA.1a)

## 1.6 Document References

| | |
|---|---|
| e-Security Sentinel Install Guide for Solaris and Windows | 5.1.1 |
| e-Security Sentinel User's Guide for Solaris and Windows | 5.1.1 |
| e-Security Sentinel User's Reference Guide for Solaris and Windows | 5.1.1 |
| e-Security Sentinel Wizard User's Guide for Solaris and Windows | 5.1.1 |
| e-Security Sentinel Product Release Notes | 5.1.1 |
| e-Security Sentinel 3rd Party Integration | 5 |

**Table 2 - Document References**

Note: The e-Security Sentinel 3rd Party Integration document is not in the scope of the TOE.

## 1.7 Document Terminology

**Agent** They are used to collect and normalize alerts from security devices and programs.

**Active Agent** This is an agent that is in operation to normalize the incoming data.

**Alert** An action or occurrence that is detected by a device or application. Alerts can be security-related, performance-related, or informational in nature. Alerts can be anything from a login failure to a malformed data packet on the network.

**Data Access Service (DAS)** Provides a data driven interface to the database.

**DBO** Database owner. A database owner has full permission to the database.

**Event** Once the data has passed the agent it has become an 'event'. Internally generated data based on Administrative actions or auditable actions are also called 'events'

**Global Filter** Process data based on specific criteria for both events coming into the system and users of the system.

**Public/Private Filters** Filters that determine which events are depicted in the real time event tables, charts and graphs.

**GUI** Graphical User Interface

**Incidents** A grouping a set of events together as a whole representing something of interest (group of similar events or set of different events that indicate a pattern of interest such an attack).

**Java** An object-oriented programming language based loosely on C++ language and developed by Sun Microsystems, Inc.

**Java Message Service (JMS)** Allows Java programs to exchange messages with other Java programs sharing a messaging system.

**JMS Message** A self contained entity used to exchange information. A JMS message consists of a header and a message body containing payload data.

**JMS Message Header** Identifies, routes, manages, and delivers JMS messages

**Java Runtime Environment** Provides the minimum requirements for executing a Java application. It consists of the Java Virtual Machine (JVM), core classes, and supporting files.

**Java Virtual Machine** JVM is an execution environment that converts Java compiled code into machine language and executes it.

**JDBC** A database access driver that provides Java programs with access to the Database.

**Log file** A file that lists actions that have occurred. For example, web servers maintain log files listing every request made to the server.

**Modified Agent** An agent that has been modified but not made active by the

authorized administrator.

**Normalize** The processing of raw data into events that can be correlated, reported and used for incident response.

**ODBC** Abbreviation of **O**pen **D**ata**b**ase **C**onnectivity, a standard database access method developed by Microsoft Corporation. The goal of ODBC is to make it possible to access any data from any application, regardless of which database management system (DBMS) is handling the data. ODBC manages this by inserting a middle layer, called a database driver, between an application and the DBMS. The purpose of this layer is to translate the application's data queries into commands that the DBMS understands. For this to work, both the application and the DBMS must be ODBC-compliant -- that is, the application must be capable of issuing ODBC commands and the DBMS must be capable of responding to them.

**OPSEC LEA** In 1997, Check Point created the OPSEC (Open Platform for Security) alliance program for security application and appliance vendors to enable an open industry-wide framework for interoperability. LEA is Log Export API (Application Programming Interfaces) used by external applications to retrieve real-time and historical log information

**ST** **Security Target –** A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

**SDM** **Sentinel Data Manager –** Utility used to manage the archival of enterprise alert and TOE data**.**

**Serial Port** A port, or interface, that can be used for serial communication - in which only 1 bit is transmitted at a time. (Serial data transfer refers to transmitting data one bit at a time. The opposite of serial is parallel, in which several bits are transmitted concurrently)

**SNMP** Is used to obtain data on remote devices, such as a configurable switch. Typically, a network-management station uses SNMP (Simple Network Management Protocol) to poll the devices in a network and to retrieve data regarding the devices current and past conditions.

**Sockets** Is an object that connects an application to a network protocol. Example a program can send and receive TCP/IP messages by opening a socket and reading and writing data to and from the socket. Note that a socket in this sense is completely soft – it's a software object, not a physical component.

**TOE** **Target of Evaluation –** An IT product of system and it's associated administrator and user guidance documentation that is the subject of an evaluation.

**Wizard Port** Enables an Agent to locate the security event data on the network by providing the IP address and other information about the source.

# 2 TOE Description

The TOE is e-Security Sentinel 5.1.1 (Sentinel 5)**Error! Bookmark not defined.**. Sentinel 5 consists of the Sentinel Server managed by the Sentinel Control Center, Sentinel Wizard, and a database repository which work together to deliver security event management via a central console. It's multi-platform infrastructure event management software.

NOTE - The Advisor module will not be part of the TOE. See section 1.2 for more detail regarding this module. Should Advisor be installed the installation of e-Security sentinel will no longer be CC certified.

## 2.1 Overview

Sentinel 5 collects alerts from devices (see section 5.2.4 for complete details) or applications and provides both real-time and historical event analysis using the Sentinel Control Center console.

### 2.1.1 Sentinel Wizard

The Sentinel Wizard module comprises the Wizard Agent Builder and Wizard Agent Manager components.

The Wizard Agent Builder is a GUI used to build, select, configure, and control agents. Agents collect and normalize alerts from security devices and programs. These normalized alerts – now known as events are then sent to the Sentinel server over the protected iSCALE[2] communication path (known simply as iSCALE) for use in correlation, reporting, and incident response. In addition to

---

2

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

running agents on the local Wizard system, the Agent Builder can be used to upload, download, and control agents on remote Wizard systems. The Wizard Builder comprises the following:

- An Agent: is the receptor that collects, filters, and normalizes the raw alerts from security devices and programs and outputs normalized alerts known as events that can be correlated, reported, and used for incident response.
- Wizard Port: Enables an Agent to locate the security event data on the network by providing the IP address and other information about the source.

The Wizard Agent Manager is the back-end that manages agents, generates system status messages, forwards events to Sentinel server, and performs global event filtering. A machine that has the Wizard Agent Manager installed is also referred to as a 'Wizard host'. A Wizard host becomes active once an Agent Builder has uploaded an agent to the Wizard Agent Manager on this machine. The Wizard Agent Manager machine may host many agents all collecting different types of data from different machines located throughout the enterprise.

### 2.1.2 Sentinel Server

The Sentinel Server comprises the communication server component, the Correlation Engine, and Base Components.

The communication server component establishes the iSCALE Message Bus. The iSCALE Message Bus is a Java Messaging Services (JMS) based framework through which the Wizard, Sentinel Console Center, DAS, and Sentinel Data Manager communicate. iSCALE is explicitly installed only on the Sentinel Server. The Wizard, Sentinel Console, DAS, and Sentinel Data Manager are not explicitly installed with iSCALE, however they do have sufficient built-in functionality to communicate with it. These TOE components communicate with each other using publisher/subscriber messaging. In this type of JMS communication, a publisher component publishes messages to topics and a subscriber component subscribe to topics. iSCALE routes messages from publishers to subscribers based on topics they have registered. This allows a component to publish a message to a topic channel that multiple subscribers consume, without the publishing component knowing which process subscribes to it. Subscribers can receive published messages from publishers without knowing what publishers are available. For example, if a new Wizard is added to the system, no configuration is required on the Sentinel server. The only information needed during installation is the network location (host name and tcp port) where sentinel server is located.

Once installed, these components protect inter-TOE transfer of data. All TOE components with the exception of the Database communicate over iSCALE[2].

The Correlation Engine and Base components, along with DAS defined in section 2.1.3 below, are specialized message-based services known as java containers. A java container is a self-contained functional software entity that runs as java process within a JVM.

The Correlation engine collects normalized events from the Wizard Agent Manager, correlates these events to find patterns, and then reports on real-time and historical information which can be viewed in the Sentinel Control Center.

The Sentinel Server Base Components comprise of:

- Watchdog Process: Manages all other Sentinel Server processes.
- Event Statistics Process: Manages Data used by the Active Views in the Sentinel Control Center.
- Data Synchronizer Process: Manages modification of data by multiple users.
- RuleLg Checker Process: Validates the syntax of filter & correlation rule expressions.
- Query Manager Process: Processes the requests for quick query & drill down data from the Control Center and passes the requests to the Data Access Service.

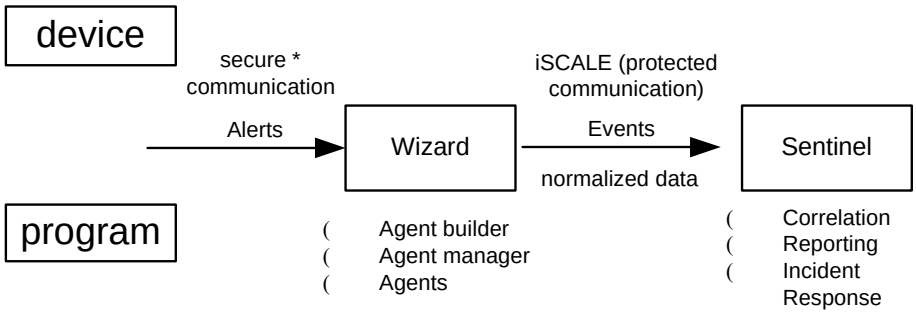


**Figure 1 - Overview of Wizard & Sentinel functions**

* Figure 1 – Secure implies that for certain collection methods e-Security have written SSL based transports, Cisco IDS (RDEP) & Checkpoint (OPSEC LEA) specifically. All other transports are in clear text. These transport mechanisms are not part of the evaluated configuration.

### 2.1.3 DAS

DAS (Data Access Service): DAS communicates with the iSCALE message bus to process all events and requests to store configuration information and inserts them into the database. It also receives database query requests, processes it, and replies back. DAS manages the database as an object, in which metadata is defined to the backend database such that DAS does not need to understand protocols or how messages get routed. The operations of DAS include a default data access via JDBC and optionally high-performance event insert strategies using native connectors (i.e., OCI for Oracle 9i and ADO for Microsoft SQL Server).

### 2.1.4 Sentinel Control Center

Sentinel Control Center provides the central management console to view real-time or historical events and system overview of changes in activity triggered by agent settings. It also provides administration of users, filters, correlated rules and security event management through incidents.

### 2.1.5 Database Server

The database server (SQL Server or Oracle) provides user authentication and dedicated storage for audit and event data.

### 2.1.6 Sentinel Data Manager

The Sentinel Data Manager is a graphical tool used to manage TOE and audit data. It allows the system administrator to View/Add/Archive/Delete database partitions.

Note: The equivalent command line version of the Sentinel Data Manager is not part of the evaluated configuration.

## 2.2 Architecture Description

The following Diagram shows the distributed architecture of the e-Security 5.1.1 TOE.

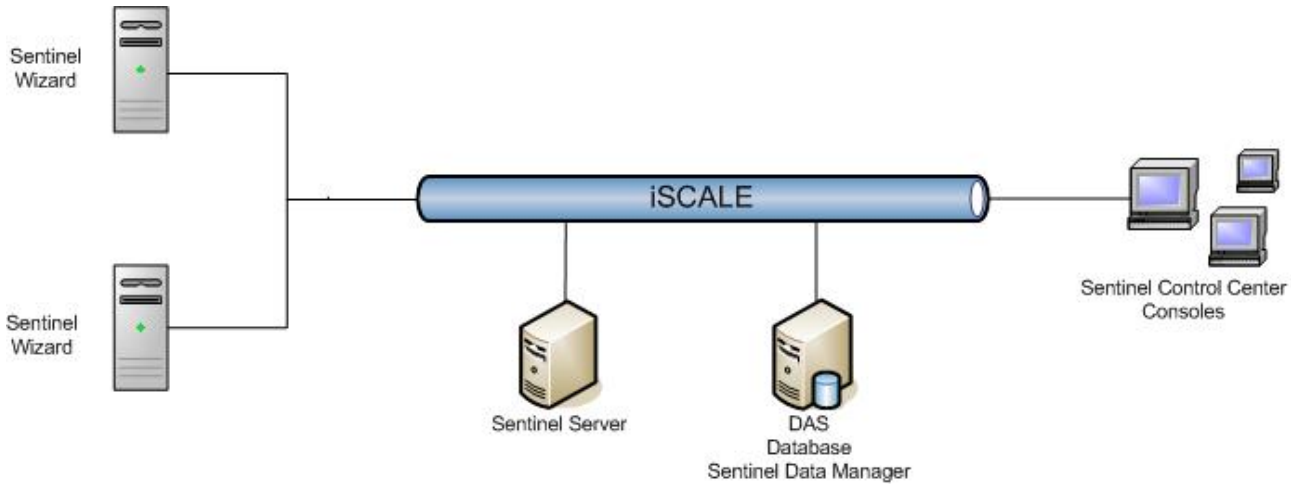


**Figure 2 - e-Security Distributed architecture**

## 2.3 Physical Boundaries

The TOE will consist of the following software based modules.

- One Sentinel Server.
- One or more Sentinel Wizards
- One or more Sentinel Control Center(s). This component can be installed both locally to the Sentinel Server and remotely.
- One Sentinel Data Manager Utility
- One Data Access Service (DAS)
- One Oracle OR One Microsoft SQL Server database.

The Agents configured and running on a Wizard Agent Manager are simply configuration parameters of the Accept Alerts SFP (see section 5.1.6). They all use the same system code to operate and perform their function of receiving Enterprise Alert Data and turning it into Enterprise Event Data through a normalization process.

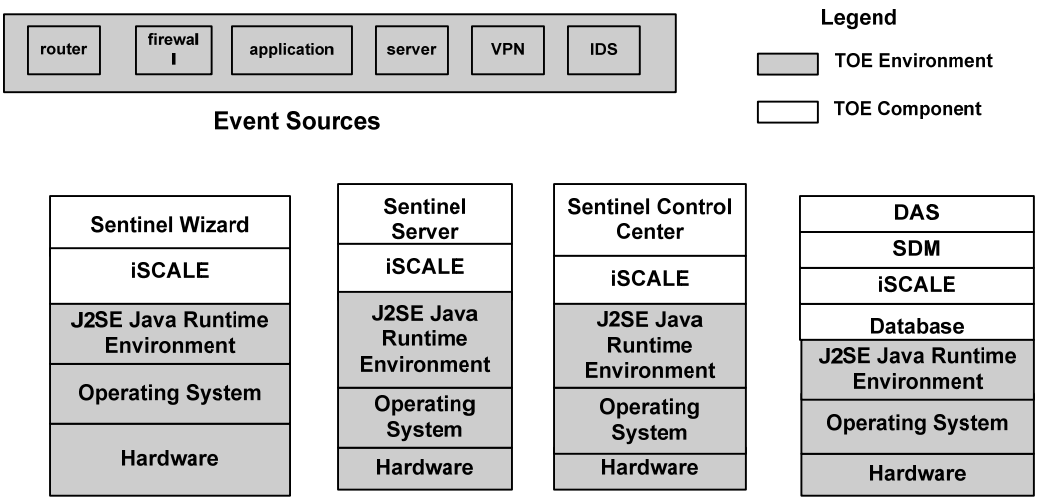


**Figure 3 - TOE Boundary**

Each physically separated TOE component communicates with each other using a logical communication path managed by iSCALE. The TOE is used inside a secure trusted network.

NOTE – A word of clarification regarding TOE vs User data in the context of the e-Security TOE.

For the purposes of the evaluation data being generated by devices in the network is considered to be belonging to the administrator. Hence the Wizard takes this user data in, normalizes it and at this point it has become TOE data.

### 2.3.1 TOE Physical Components

This table contains versions of the software that are part of the TOE. (NOTE – see section 2.4 for the environmental requirements to run this software)

| Software | Version |
|---|---|
| *Sentinel Server* | |
| Communication Server | Version 5.1.1 |
| Base Services | Version 5.1.1 |
| Correlation Engine | Version 5.1.1 |
| *Sentinel Wizard* | |
| Agent Manager | Version 5.1.1 |
| Agent Builder | Version 5.1.1 |
| *Sentinel Control Center* | Version 5.1.1 |
| *Database* | |
| Data Access Service (DAS) | Version 5.1.1 |
| Sentinel Data Manager (SDM) | Version 5.1.1 |
| Microsoft SQL Server<br>-OR-<br>Oracle | Version 2000 Enterprise Edition (SP3a) (Installed in Mixed Mode) *<br><br>Version 9i Enterprise Edition with 9.2.0.6 mega patch set (32 bit mode) * |

| | |
|---|---|
| | Oracle Critical Patch Update - April 2006 |

***** Includes respective database management utility

**Table 3 - TOE Physical Components**

## 2.4 Environment Physical Requirements.

The TOE environment requires the following hardware & software (OS's / versions / patches). The Hardware and Operating System are not part of the TOE. The table is broken out by requirements by TOE component.

| Software | Hardware |
|---|---|
| **Sentinel Control Center** | |
| Windows 2000 Professional (SP4)<br>Windows XP (SP1)<br>Windows 2003 SP1<br>Solaris 9 64bit Full Distribution plus OEM Support (May 03/05 Patch Cluster)<br>J2SE Java Runtime Environment 1.4.2 | Single 1.1 GHZ CPU (Solaris)<br>Single 3.2 GHZ CPU (Windows)<br>1 GB RAM |
| **Sentinel Server (Communication Server, Base Services, Correlation Engine)** | |
| Solaris 9 64bit Full Distribution plus OEM Support (May 03/05 Patch Cluster)<br>Windows 2000 SP4<br>Windows 2003 SP1<br>J2SE Java Runtime Environment 1.4.2 | Quad 1.1 GHZ CPU (Solaris)<br>Quad 3.2 GHZ CPU (Windows)<br>4 GB of RAM |
| **Sentinel Wizard (Agent Manager and Wizard Builder)** | |
| Windows 2000 (SP4)<br>Windows 2003 (SP1)<br>Solaris 9 64bit Full Distribution plus OEM Support (May 03/05 Patch Cluster)<br>J2SE Java Runtime Environment 1.4.2 | Dual 3.2 GHZ CPU (Solaris)<br>Dual 3.2 GHZ CPU (Windows)<br>2 GB RAM |
| **Sentinel Database – (Windows/Microsoft SQL Server)** | |
| Windows 2000 (SP4)<br>Windows 2003 (SP1)<br>Microsoft SQL Server 2000 (SP3a)<br>J2SE Java Runtime Environment 1.4.2 | Quad 3.2 GHZ CPU (Windows)<br>4GB RAM |
| **Sentinel Database - (Solaris 9 /Oracle)** | |

| | |
|---|---|
| Solaris 9 (May 03/05)<br>Oracle 9i Enterprise on Solaris 9 (9.2.0.6 Patch)<br>J2SE Java Runtime Environment 1.4.2 | Quad 1.1 GHZ CPU (Solaris)<br>4GB RAM |

**Table 4 – TOE Environment Software and Hardware Requirements**

## 2.5 Logical Boundaries

### 2.5.1 Audit

Auditing of TOE Security functions is achieved in the following manner.

The TOE generates 2 types of Audit Records, Performance & Internal events. Auditing of TOE management actions is accomplished through the same interface as that used to audit enterprise event data, the Sentinel Control Center. The internal audit records are sent along iSCALE and received by the Sentinel Server for correlation and are then passed to the database for permanent storage.

### 2.5.2 Identification and authentication

There are three roles defined for the TOE, an Operator (read only), Enterprise information Administrator (read and sentinel server administration) and the System Administrator (full control). User accounts can be assigned to either role. The System administrator has specific permissions assigned in the database beyond those assigned in the SCC GUI to allow it to manage the TOE data.

For purposes of this ST, the term “authorized administrator” shall refer to both the authorized system administrator and authorized Enterprise information administrator. The term “authorized operator” shall refer to the operator.

The Sentinel Control Center requires an authorized administrator or operator to authenticate using their provided user ID & Password.

The Sentinel Wizard requires an authorized system administrator to authenticate using their provided user ID & Password.

The Sentinel Data Manager requires an authorized system administrator to authenticate using their provided user ID & Password.

These components take this information and pass it via the encryption mechanism of iSCALE to DAS which inserts it in either Oracle or SQL Server (known as the Database).

The Database validates the identification information, using it’s native user management systems. Each user of the TOE is defined as a Database user.

Once the Database has validated the provided information, the response is passed back to requesting component.

### 2.5.3 Protection of TOE security functions

iSCALE provides protection of the TOE security functions. The traffic at the data packet level between the pieces of the TOE is encrypted using a shared private cryptographic key (AES or ARC4).

The e-Security Sentinel architecture enables efficient data routing, since events are selectively routed through iSCALE to desired components like Sentinel

servers & Databases. iSCALE supports multi-threaded processing with a configurable number of available threads for event processing.

### 2.5.4 Data Protection

Data protection is provided by a combination of the Wizard Agent Builder where the Security Policies are managed, the Agents where they are enforced, iSCALE where all the TOE data is transported and the database where the data is stored.

The data flow into the TOE from the monitored security devices is filtered at the Wizard where the system administrator configures the appropriate policy to allow the flow of data.

This policy is compiled and saved as an agent with the appropriate IP address of the Host, data flow pattern and other required variables.

The data, once the agent has received it, is normalized according to the data import specifications of the authorized system administrator.

The data is then encrypted using the shared cryptographic key and pass it via the encryption mechanism of iSCALE to DAS which inserts it in either Oracle or SQL Server (known as the Database). iSCALE supports multi-threaded processing with a configurable number of available threads for efficient event processing.

Either MS SQL Server or the Oracle Database on stores all of the data generated by the monitored devices.

User Attribute data is stored in either MS SQL Server or the Oracle Database including name, user-id & password and default filter at a minimum. The user data is stored using the user management systems of the databases. Each user of the TOE is defined as a database user.

### 2.5.5 Management of TOE security functions

The management of TOE security functions takes place at the Sentinel Control Center, Sentinel Server, Sentinel Data Manager, and the Wizard Agent Builder.

There are also some scripts located on Sentinel Server that perform specific actions upon certain TOE Components.

The Sentinel Control Center provides an interface into all aspects of TOE management including the Real Time correlation results, the System Overview, Incident lists, analysis activities and the Administration Activities of user creation / look & feel of the interface and user permissions.

The Wizard Agent Builder allows the system administrator to fully select and configure the Agents and Wizard Ports based on the items contained in the Accept Alerts SFP (See section 5 for more detail).

The Sentinel Data Manager (SDM) allows the authorized system administrator to manage database archival & partitioning processes.

The MS SQL Enterprise Manager and SQL*PLUS Oracle Database Command line interface are used to manage the permissions of the users occupying the System Administrator role.

### 2.5.6 Enterprise Event Data

The TOE provides the ability to collect, store and analyze alert data captured

from devices around the enterprise.

The agents created and managed by the Wizard Host receive the data where it is normalized.

The normalized data (now known as ‘events’) from the agents is sent along iSCALE and received by the Sentinel Server.

Review of the data generated by the agents is performed using the Sentinel Control Center. The Sentinel Control Center provides the ability to review the data in real time, against a timeline summary graph and 3D chart. Graphical depiction of event counts and severities is also available.  The Sentinel Control Center also provides the ability to generate historical reports and incidents.

The data is stored in either MS SQL Server or the Oracle Database and managed through the Sentinel Data Manager (SDM).

# 3 TOE Security Environment

## 3.1 Assumptions

The assumptions are ordered into three groups outlined below.

### 3.1.1 Personnel Assumptions

| | |
|---|---|
| A.LOWEXP | There is a low risk of an unauthorized individual attempting to exploit vulnerabilities in the TOE |
| A.NOEVIL | Administrators are not willfully negligent, but may make mistakes. |
| A.ADMIN_TRA | The authorized administrators will be trained in the secure usage of the TOE |
| A.REMOTE_ADMIN | The authorized administrators will only be able to access the TOE remotely from within the trusted network containing the TOE |

**Table 5 - Personnel Assumptions**

### 3.1.2 Physical Environment Assumptions

| | |
|---|---|
| A.PHYSEC | The pieces of the TOE will be housed securely |
| A.NETWORK_COMMUNICATION | The environment will provide reliable network communication between the pieces of the TOE and the monitored devices |
| A.COMPATIBLE_FORMAT | The devices in the enterprise will be configured to use following formats for data export.<br>Generic Log File (Syslog, ASCII)<br>Microsoft's Windows Event Log (Windows proprietary format)<br>Serial<br>SNMP v1,v2 & v3<br>TCP Socket<br>ODBC<br>JDBC<br>Cisco's RDEP<br>Checkpoint's OPSEC |
| A.SECURE_NETWORK | The TOE is used inside a secure trusted network for the use of managing alerts from other security products located on that network. |

**Table 6 - Physical Environment Assumptions**

### 3.1.3 Operational Assumptions

| | |
|---|---|
| A.SOLEPUR | The TOE environment will not store general purpose |

| | |
|---|---|
| | applications or public data |
| A.TIME_SRC | Time sources in the environment are assumed to be placed in a secure location and configured accurately so as to provide a trusted clock source for the TOE. |
| A.SEL_PRO | The TOE environment will be configured in such a manner as to prevent an unauthorized person from reading, modifying or destroying security critical TOE configuration data |
| A.AUDIT_STORAGE | The TOE environment will be configured in such a way as to prevent an unauthorized person from reading or modifying the TOE Audit Trail |
| A.OSLOGIN | The TOE environment will be configured in such a way to require authorized administrators to login |

**Table 7 - Operational Assumptions**

## 3.2 Threats

The TOE or IT environment addresses the threats identified in the following sections.

### 3.2.1 Threats Addressed by the TOE

The TOE addresses the threats discussed below.

The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself.

| | |
|---|---|
| T.UNAUTH_LOGIN | An unauthorized person logs into the Sentinel server, allowing them, through unauthorized use of the management functions, to disrupt the alert flow thus preventing the administrator from reacting to the alerts. |
| T.UNAUTH_AGENT_UPDATE | An unauthorized person updates an active agent to stop and/or divert the alert flow. |
| T.UNAUTH_DATABASE_ACCESS | An unauthorized person accesses the database storing the alert flow modifying the alert record. |
| T.UNAUTH_REMOTE_ADMIN | An unauthorized person logs into the Sentinel server via the Sentinel Control Center remotely allowing them, through unauthorized use of the management functions, to disrupt the alert flow thus preventing the administrator from reacting to the alerts. |
| T.SECURITY_MANAGEMENT | The security functions of the TOE are unmanageable leading to missed security alerts. |
| T.ALERT_UNCOLLECTED | An alert from an enterprise device goes uncollected due to no applicable configured collection agent preventing the administrator from reacting to the alert. |
| T.ALERT_UNREVIEWED | An alert from a monitored device is missed due to the inability to review the alert trail preventing the administrator from reacting to the alert. |
| T.ALERT_LOST | An alert from a monitored device is not able to be stored due to insufficient storage space preventing the |

| | |
|---|---|
| | administrator from reacting to the alert. |
| T.ALERT_MISSED | An alert from a monitored device is missed due to a communications failure preventing the administrator from reacting to the alert. |
| T.TRAFFIC_MODIFIED | An alert from a monitored device OR the data from a remote administration session is modified in transit by an unauthorized person masking unauthorized network activity. |
| T.NO_AUDIT | Unauthorized and authorized actions occur with no audit trail generation preventing an authorized administrator from reviewing the actions of others and allowing an attacker to escape detection. |
| T.NO_ACCOUN | The TOE audit trail is not recorded, preventing an authorized administrator from reviewing the actions of others and allowing an attacker to escape detection. |
| T.SEL_PRO | An unauthorized person may read, modify or destroy security critical TOE configuration Data. |

**Table 8 – Threats addressed by the TOE**

### 3.2.2 Threats Addressed by Operating Environment

| | |
|---|---|
| TE.MGMT_ERROR | An authorized administrator makes a mistake during the administration of the TOE and disrupts the alert flow. |
| TE.NO_ALERTS | No alerts are received from the devices in the Environment |
| TE.NO_ACCOUN | Authorized administrators do not review the audit log allowing an attacker to escape detection. |
| TE.EVENT_SEQUENCE | An authorized administrator is unable to distinguish the sequence of events and therefore cannot detect any alerts. |

**Table 9 – Threats to the Environment**

## 3.3 Organizational Security Policies (OSP)

There are no Organizational Security Policies required for the TOE.

# 4 Security Objectives

### 4.1.1 Security Objectives For The TOE

The Administrators will be trained in the use of the TOE security objectives. The following are the IT security objectives for the TOE:

| | |
|---|---|
| O.LOGIN | Excluding 'Utilities[3]', Administrators are required to uniquely identify themselves to the Sentinel Server, Sentinel Control Center, Sentinel Wizard Agent Builder and Sentinel Data Manager to prevent unauthorized changes to the TOE Security Functions and these components will end a session if such identification is not provided |
| O.SECURE_COMMUNICATIONS | The TOE will protect communications between the distributed pieces to prevent eavesdropping and data modification |
| O.ALERT_COLLECT | The TOE will provide the ability to collect alert data from disparate devices |
| O.ALERT_STORAGE | The TOE will provide secured & manageable storage for the alerts |
| O.ALERT_REVIEW | The TOE shall provide a way for the authorized administrator to review the alerts |
| O.AUDIT_TRAIL | The TOE shall be able to generate notification of auditable events |
| O.AUDIT_STORAGE | The TOE shall provide a way to store it's audit data |
| O.AUDIT_REVIEW | The TOE shall provide a way to allow the authorized administrator to review the audit records |
| O.SECURITY_MANAGEMENT | The TOE shall provide tools to manage it's security functions |
| O.SEL_PRO | The TOE shall provide, in conjunction with the environment, means to prevent unauthorized persons from reading, modifying or destroying security critical TOE configuration Data. |

**Table 10 - Security objectives for the TOE**

### 4.1.2 Security Objectives For The Environment

The Administrators will be trained in the use of the TOE security objectives for the environment. The security objectives for the IT environment are listed below.

| | |
|---|---|
| OE.ADMIN_TRA | Administrators receive all guidance and training regarding the secure operation of the TOE |
| OE.ALERT_STREAM | Devices in the environment are configured to provide the Alert stream to the agents. |
| OE.NETWORK_COMMUNICATION | The TOE environment will provide a reliable network to allow the pieces of the TOE to work together. |
| OE.LOWEXP | There is a low risk of an unauthorized individual |

| | |
|---|---|
| | attempting to exploit vulnerabilities in the TOE |
| OE.SOLEPUR | The TOE environment will have no other applications installed, nor public data stored on it. |
| OE.NOEVIL | Administrators will be trained in the use of the TOE, are not willfully negligent, but may make mistakes. |
| OE.REMOTE | Only authorized Administrators will access the TOE remotely. |
| OE.PHYSEC | The pieces of the TOE will be housed securely |
| OE.SECURE_NETWORK | The TOE Environment is inside a secure trusted network for the use of managing alerts from other security products located on that network. |
| OE.AUDIT_REVIEW | The authorized administrators will be trained to and responsible for reviewing the audit logs to prevent an attacker from escaping detection. |
| OE.COMPATIBLE_FORMAT | The devices in the enterprise will be configured to use one of the following formats for export.<br>Generic Log File (Syslog, ASCII)<br>Microsoft's Windows Event Log (Windows proprietary format)<br>Serial<br>SNMP v1, v2 &v3<br>TCP Socket<br>ODBC<br>JDBC<br>Cisco's RDEP<br>Checkpoint's OPSEC |
| OE.TIME_SRC | The TOE environment will provide a reliable time source for the TOE. |
| OE.SEL_PRO | The TOE environment will be configured in such a manner as to work in conjunction with the TOE to prevent an unauthorized person from reading, modifying or destroying security critical TOE configuration data |
| OE.AUDIT_STORAGE | The TOE Environment will be configured in such a manner as to work in conjunction with the TOE to prevent an unauthorized person from reading or modifying the TOE Audit trail. |
| OE.I&A_AUDIT_REVIEW | The TOE Environment will provide authorized administrators with the capability to review Identification and Authentication audit records and also allow searches, sorting, and ordering of audit data. |
| OE.OSLOGIN | The TOE Environment will require authorized administrators to identify and authenticate themselves to the OS (Windows or Solaris) |

**Table 11 - Security Objectives for the Environment**

## 4.2 Rationale - Security Objectives For The TOE

This section provides the rationale that all security objectives are traced back to aspects of the addressed threats and organizational security policies.

| | T.UNAUTH_LOGIN | T.UNAUTH_AGENT_UPDATE | T.UNAUTH_DATABASE_ACCESS | T.UNAUTH_REMOTE_ADMIN | T.SECURITY_MANAGEMENT | T.ALERT_UNCOLLECTED | T.ALERT_UNREVIEWED | T.ALERT_LOST | T.ALERT_MISSED | T.TRAFFIC_MODIFIED | T.NO_AUDIT | T.NO_ACCOUN | T.SEL_PRO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.LOGIN | X | X | | X | | | | | | | | | |
| O.SECURE_COMMUNICATIONS | | | | X | | | | | X | X | | | |
| O.ALERT_COLLECT | | | | | | X | | | | | | | |
| O.ALERT_STORAGE | | | X | | | | | X | | | | | |
| O.ALERT_REVIEW | | | | | | | X | | | | | | |
| O.AUDIT_TRAIL | | | | | | | | | | | X | | |
| O.AUDIT_REVIEW | | | | | | | | | | | X | X | |
| O.AUDIT_STORAGE | | | | | | | | | | | | X | |
| O.SECURITY_MANAGEMENT | | | | | X | | | | | | | | |
| O.SEL_PRO | | | | | | | | | | | | | X |

**Table 12 – Threats, IT Security Objectives & Organizational Security Policy Mappings**

### 4.2.1 O.LOGIN

To counter the threats of T.UNAUTH_REMOTE_ADMIN, T.UNAUTH_AGENT_UPDATE and T.UNAUTH_LOGIN administrators are required to log into the Sentinel Control Center, Wizard Agent Builder, and Sentinel Data Manager using passwords of at least 8 alphanumeric characters. The Sentinel Control Center and Sentinel Wizard Agent Builder limit an unauthorized user trying to guess a password by ending the session after 3 invalid attempts.

### 4.2.2 O.SECURE_COMMUNICATIONS

To counter the threats of T.ALERT_MISSED, T.TRAFFIC_MODIFIED and T.UNAUTH_REMOTE_ADMIN, the TOE will protect communications between the distributed pieces to prevent eavesdropping (of administrative credentials for example) and data modification.

### 4.2.3 O.ALERT_COLLECT

To counter the threat of T.ALERT_UNCOLLECTED the TOE will provide a mechanism to collect Enterprise Event Data from disparate devices.

### 4.2.4 O.ALERT_STORAGE

To counter the threat of T_ALERT_LOST and T.UNAUTH_DATABASE_ACCESS the

TOE will provide secured, manageable storage for the Enterprise Event Data.

#### 4.2.5 O.ALERT_REVIEW

To counter the threat of T.ALERT_UNREVIEWED the TOE shall provide a way to review the Enterprise Event Data generated from disparate devices.

#### 4.2.6 O.AUDIT_TRAIL

To counter the threat of T.NO_AUDIT The TOE shall be able to generate a record of auditable events.

#### 4.2.7 O.AUDIT_REVIEW

To counter the threat of T.NO_ACCOUN & T.NO_AUDIT the TOE shall provide a way for the authorized administrator to review the audit logs.

#### 4.2.8 O.AUDIT_STORAGE

To counter the threat of T.NO_ACCOUN the TOE shall provide a way for the audit data to be stored.

#### 4.2.9 O.SECURITY_MANAGEMENT

To counter the threat of T.SECURITY_MANAGEMENT that the security functions of the TOE are unmanageable the TOE shall provide tools to manage its security functions.

#### 4.2.10 O.SEL_PRO

To counter the threat of T.SEL_PRO the TOE (In concert with the environment) must protect itself against attempts by unauthorized users to bypass, deactivate or temper with the TOE Security functions.

## 4.3 Rationale - Security Objectives For The Environment

This section provides the rationale that all security objectives for the environment are traced back to aspects of the addressed threats or assumptions.

| | TE.NO_ALERTS | TE.MGMT_ERROR | TE.NO_ACCOUN | TE.EVENT_SEQUENCE | A.REMOTE_ADMIN | A.NETWORK_COMMUNICATION | A.PHYSEC | A.ADMIN_TRA | A.NOEVIL | A.LOWEXP | A.SOLEPUR | A.COMPATIBLE_FORMAT | A.SEL_PRO | A.AUDIT_STORAGE | A.SECURE_NETWORK | A.OSLOGIN |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| OE.ADMIN_TRA | | X | | | | | | X | | | | | | | | |
| OE.ALERT_STREAM | X | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| OE.NETWORK_COMMUNICATION | | | | | | X | | | | | | | | | |
| OE.PHYSEC | | | | | | | X | | | | | | | | |
| OE.SECURE_NETWORK | | | | | | | | | | | | | | X | |
| OE.OSLOGIN | | | | | | | | | | | | | | | X |
| OE.LOWEXP | | | | | | | | | | X | | | | | |
| OE.SOLEPUR | | | | | | | | | | | X | | | | |
| OE.NOEVIL | | | | | | | | | X | | | | | | |
| OE.REMOTE | | | | | X | | | | | | | | | | |
| OE.AUDIT_REVIEW | | | X | | | | | | | | | | | | |
| OE.COMPATIBLE_FORMAT | | | | | | | | | | | | X | | | |
| OE.TIME_SRC | | | | X | | | | | | | | | | | |
| OE.SEL_PRO | | | | | | | | | | | | | X | | |
| OE.AUDIT_STORAGE | | | | | | | | | | | | | | X | |

**Table 13 – Threats, IT Security Objectives & Assumption Mappings for the Environment**

### 4.3.1 OE.ADMIN_TRA

This counters the threat of TE.MGMT_ERROR and covers the assumption, A.ADMIN_TRA, by ensuring that the authorized administrators are trained in the secure use of the TOE

### 4.3.2 OE.ALERT_STREAM

This counters the threat of TE.NO_ALERTS, by ensuring that alerts are received from the devices in the Environment.

### 4.3.3 OE.NETWORK_COMMUNICATION

This covers the assumption of A.NETWORK_COMMUNICATION, by ensuring that the TOE environment will provide a reliable network to allow the pieces of the TOE to work together

### 4.3.4 OE.PHYSEC

This covers the assumption of A.PHYSEC, by ensuring that the TOE is physically protected.

### 4.3.5 OE.SECURE_NETWORK

This covers the assumption A.SECURE_NETWORK by ensuring that the TOE environment will be inside a secure trusted network for the use of managing alerts from other security products located on that network.

### 4.3.6 OE.OSLOGIN

This covers the assumption A.OSLOGIN by ensuring that the TOE environment will require authorized administrators to successfully identify themselves to the OS.

### 4.3.7 OE.LOWEXP

This covers the assumption of A.LOWEXP, by identifying that there is a low risk of an unauthorized individual attempting to exploit vulnerabilities in the TOE.

#### 4.3.8 OE.SOLEPUR

This covers the assumption of A.SOLEPUR, by stating that the TOE environment will not house other applications nor store public data.

#### 4.3.9 OE.NOEVIL

This covers the assumption of A.NOEVIL, by stating that the Administrators in the environment, whilst following all guidance are capable of error.

#### 4.3.10 OE.REMOTE

This covers the assumption of A.REMOTE_ADMIN, by stating the authorized administrators will be the only people accessing the TOE remotely.

#### 4.3.11 OE.AUDIT_REVIEW

This covers the Environmental threat of TE.NO_ACCOUN by stating that the authorized administrators will review the audit logs, not allowing an attacker to escape detection.

#### 4.3.12 OE.COMPATIBLE_FORMAT

This covers the assumption A.COMPATIBLE_FORMAT that states that the devices in the enterprise must use one of the identified formats for export of data.

#### 4.3.13 OE.TIME_SRC

This covers the Environmental threat TE.EVENT_SEQUENCE that states that the TOE Environment shall provide a reliable time stamp for the TOE's use.

#### 4.3.14 OE.SEL_PRO

This covers the assumption A.SEL_PRO that states that the TOE Environment shall, in conjunction with the TOE, protect itself against attempts by unauthorized users to bypass, deactivate or temper with the TOE Security functions

#### 4.3.15 OE.AUDIT_STORAGE

This covers the assumption A.AUDIT_STORAGE that states that the TOE Environment shall, in conjunction with the TOE, protect itself against attempts by unauthorized users to read or modify the TOE Audit Trail

# 5 IT Security Requirements

The security functional requirements for this Security Target consist of the following components from Part 2 of the CC, identified in the following table. These security requirements are defined in Section 5.1.

| SFR – TOE | Name |
|---|---|
| FAU_GEN.1 | Audit Data Generation |
| FAU_SAR.1 | Audit review |
| FAU_SAR.3 | Selectable Audit Review |
| FDP_IFF.1[AA] | Simple security attributes |
| FDP_IFF.1[MB] | Simple security attributes |
| FDP_IFC.1[AA] | Subset information flow control |
| FDP_IFC.1[MB] | Subset information flow control |
| FDP_ITT.1 | Basic internal transfer protection |
| FDP_ITC.1 | Import of user data without security attributes |
| FIA_ATD.1 | User attribute definition |
| FIA_UAU.1 | Timing of Authentication |
| FIA_UID.1 | Timing of Identification |
| FMT_MOF.1 | Management of security functions behavior |
| FMT_MSA.3[AA] | Static attribute initialization |
| FMT_MSA.3[MB] | Static attribute initialization |
| FMT_MTD.1 | Management of TSF data |
| FMT_SMR.1 | Security Roles |
| FMT_SMF.1 | Security Functions |
| FPT_ITT.1 | Basic internal TSF data transfer protection |

**Table 14 – TOE Security Functional Requirements**

| SFR – Explicitly Stated | Name |
|---|---|
| FAU_STG_EXP.1 | Protected audit trail storage |
| FPT_RVM_EXP.1 | Non-Bypassability of the TSP |
| FPT_SEP_EXP.1 | TSF Domain Separation |
| ESEC_COL.1 | Collection of Enterprise Event Data |
| ESEC_RDR.1 | Restricted Review of Enterprise Event Data |
| ESEC_STG.1 | Protected Storage of Enterprise Event Data |
| ESEC_STG.2 | Prevention of Loss of Enterprise Event Data |

**Table 15 – TOE Explicitly Stated Security Functional Requirements**

| SFR – Environment | Name |
|---|---|
| FAU_SAR.1 | Audit Review |
| FAU_SAR.3 | Selectable Audit Review |
| FPT_STM.1 | Reliable Time Stamp |

**Table 16 – TOE Environment Security Functional Requirements**

| SFR – Environment Explicitly Stated | Name |
|---|---|
| FAU_STG_OS.1 | Protected Audit Trail Storage |
| FPT_RVM_OS.1 | Non-Bypassability of the TSP |
| FPT_SEP_OS.1 | TSF Domain Separation |
| FIA_UAU_OS.1 | User Authentication |
| FIA_UID_OS.2 | User Identification |

**Table 17 – TOE Environment – Explicitly Stated Security Functional Requirements**

## 5.1 TOE Security Functional Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

### 5.1.1 FAU_GEN.1 – Audit Generation

#### 5.1.1.1 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; ***for the events listed in table 18***; and
c) **none**

#### 5.1.1.2 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, **none.**

| Functional Component | Level | Auditable Events | Additional Audit Record Contents |
|---|---|---|---|
| FIA_UAU.1 | None | Login Succeeded | |
| | | Login Failed | |
| ESEC_COL.1 | None | SummaryUpdateFailure | |
| | | InsertEventsFailed | |
| | | InsertIntoOverflowPartition | |
| | | EventInsertionIsBlocked | |
| | | EventInsertionResumed | |
| | | EventRouterIsRunning | |
| | | EventRouterInitializing | |
| | | EventRouterStopping | |

| | | | |
|---|---|---|---|
| | | OutOfSyncDetected | |
| | | EventRouterTerminating | |
| FMT_MOF.1 | None | PortStop | |
| | | PortStart | |

**Table 18 - Auditable events**

### 5.1.2 FAU_SAR.1 - Audit review

#### 5.1.2.1 FAU_SAR.1.1

The TSF shall provide **authorized administrators** with the capability to read

**1. Date and Time stamp of the event**

**2. Type of Event (startup, shutdown, creation, modification, deletion)**

**3. Identity of subject whom initiated the event**

**4. Outcome of Event (Success or Failure)**

**for events corresponding to the collection of Enterprise Event Data and Management of Security Function behavior** from the audit records.

#### 5.1.2.2 FAU_SAR.1.2

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

### 5.1.3 FAU_SAR.3 - Selectable audit review

#### 5.1.3.1 FAU_SAR.3.1

The TSF shall provide the ability to perform searches, sorting, ordering of audit data based on **Date & Time, and Type of event**.

### 5.1.4 FDP_IFC.1[AA] - Subset information flow control

#### 5.1.4.1 FDP_IFC.1.1[AA]

The TSF shall enforce the **Accept Alerts SFP** on

**SUBJECTS**

**monitored devices**

**INFORMATION**

**user data**

**OPERATIONS**

**Normalize and pass the data to Sentinel Server**.

### 5.1.5 FDP_IFC.1[MB]

#### 5.1.5.1 FDP_IFC.1.1[MB]

The TSF shall enforce the **Message Bus SFP** on

**SUBJECTS**

**Sentinel Wizard**

**Sentinel Servers**

**Sentinel Control Centers**

**Sentinel Data Manager**

**DAS Process**

**INFORMATION**

**Normalized event data**

**User data**

**TOE Management data**

**OPERATIONS**

**Pass the JMS message containing event, user & management data along iSCALE to the appropriate recipient TOE component**

### 5.1.6 FDP_IFF.1[AA] - Simple security attributes

Interp Note : The following element is changed as a result of Interpretation 104.

#### 5.1.6.1 FDP_IFF.1.1[AA]

The TSF shall enforce the **Accept Alerts SFP** based on the following types of subject and information security attributes:

**Subjects attributes:**
**Monitored device IP addresses**

**Monitored device Product Type**

**Security information attributes:**

**See table 20 – Details column for the list of possible data attributes by monitored product type.**

#### 5.1.6.2 FDP_IFF.1.2[AA]

The TSF shall permit information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **the alert received from the monitored device IP address matches the defined criteria for the product type as configured by the administrator**

#### 5.1.6.3 FDP_IFF.1.3[AA]

The TSF shall enforce the **none**.

#### 5.1.6.4 FDP_IFF.1.4[AA]

The TSF shall provide the following **none**.

#### 5.1.6.5 FDP_IFF.1.5[AA]

The TSF shall explicitly authorize an information flow based on the following rules: **none.**

5.1.6.6 FDP_IFF.1.6[AA]

The TSF shall explicitly deny an information flow based on the following rules: **none**.

5.1.7 FDP_IFF.1[MB] - Simple security attributes

Interp Note : The following element is changed as a result of Interpretation 104.

5.1.7.1 FDP_IFF.1.1[MB]

The TSF shall enforce the **Message Bus SFP** based on the following types of subject and information security attributes:

Subjects attributes:
**JMS message header**

**Security information attributes:**
**1. Shared cryptographic key**

5.1.7.2 FDP_IFF.1.2[MB]

The TSF shall permit information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **the data transmission from the subject is encrypted with the shared cryptographic key.**

5.1.7.3 FDP_IFF.1.3[MB]

The TSF shall enforce the **none**.

5.1.7.4 FDP_IFF.1.4[MB]

The TSF shall provide the following **none**.

5.1.7.5 FDP_IFF.1.5[MB]

The TSF shall explicitly authorize an information flow based on the following rules: **none.**

5.1.7.6 FDP_IFF.1.6[MB]

The TSF shall explicitly deny an information flow based on the following rules: **none**.

5.1.8 FDP_ITC.1 - Import of user data without security attributes

5.1.8.1 FDP_ITC.1.1

The TSF shall enforce the **Accept Alerts SFP** when importing user data, controlled under the SFP, from outside of the TSC.

5.1.8.2 FDP_ITC.1.2

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

#### 5.1.8.3 FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **The data shall be normalized according to the configuration of the Accept Alerts SFP**.

### 5.1.9 FDP_ITT.1 - Basic internal transfer protection

#### 5.1.9.1 FDP_ITT.1.1

The TSF shall enforce the **Message BUS SFP** to prevent the disclosure, modification of user data when it is transmitted between physically-separated parts of the TOE.

### 5.1.10 FIA_ATD.1 - User attribute definition

#### 5.1.10.1 FIA_ATD.1.1

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

**User ID**
**password**
**assigned permissions comprising the role System Administrator, Enterprise Information Administrator or Operator.**

### 5.1.11 FIA_UAU.1 Timing Of Authentication

#### 5.1.11.1 FIA_UAU.1.1

The TSF shall allow **the use of the Utilities**[3] on behalf of the user to be performed before the user is authenticated

[3] The Utilities are defined in Chapter 11 of the Sentinel_5_1_SCC_Guide document.

5.1.11.2 FIA_UAU.1.2

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

5.1.12 FIA_UID.1 Timing of Identification

5.1.12.1 FIA_UID.1.1

The TSF shall allow **the use of the Utilities**[3] on behalf of the user to be performed before the user is identified

5.1.12.2 FIA_UID.1.2

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

5.1.13 FMT_SMR.1 - Security roles

5.1.13.1 FMT_SMR.1.1

The TSF shall maintain the roles

**System Administrator (SA - Full Control)**

**Enterprise Information Administrator (EA - Full control except for User administration and Audit data management)**

**Operator (Enterprise Event Data - read only)**

5.1.13.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

5.1.14 FMT_SMF.1 – Security Functions

5.1.14.1 FMT_SMF.1.1

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

**Manage Agents (Select, Build, Modify) with Wizard Agent Builder**

**Manage (Stop/Start) Agent Manager**

**Manage (Create/Edit/Delete) Global Filters**

**Manage (Create/Edit/Delete) Public/Private Filters**

**Manage (Add/Edit/Delete) TOE user accounts**

**Read the Enterprise Event Data**

**Read the TOE Audit Data**

**Manage database partitions through the SDM**

5.1.15 FMT_MOF.1 - Management of security functions behavior

5.1.15.1 FMT_MOF.1.1

The TSF shall restrict the ability to determine the behavior of, disable, enable,

modify the behavior of the functions **as defined in table 19.** [4]

| User Class | Function |
|---|---|
| System Administrator | Manage Agents (Select, Build, Modify) with Wizard Agent Builder<br>Manage (Stop/Start) Agent Manager<br>Manage (Create/Modify/Delete/View) TOE user accounts<br>Manage (Create/Edit/Delete) Global Filters<br>Manage (Create/Edit/Delete) Public/Private Filters.<br>Manage database partitions through the SDM |
| Enterprise Information Administrator | Manage (Stop/Start) Agent Manager<br>Manage (Create/Edit/Delete) Global Filters<br>Manage (Create/Edit/Delete) Public/Private Filters. |

**Table 19 - FMT_MOF Role to Function Assignment**

[4] Please see Appendix A for the complete listing of individual permissions related to these functions.

5.1.16 FMT_MSA.3[AA] - Static attribute initialization

Interp Note : The following element is changed as a result of Interpretation 202.

5.1.16.1 FMT_MSA.3.1[AA]

The TSF shall enforce the **Accept Alerts SFP** to provide restrictive default values for security attributes that are used to enforce the *SFP*.

5.1.16.2 FMT_MSA.3.2[AA]

The TSF shall allow the **System Administrator** to specify alternative initial values to override the default values when an object or information is created.

5.1.17 FMT_MSA.3[MB] - Static attribute initialization

Interp Note : The following element is changed as a result of Interpretation 202.

5.1.17.1 FMT_MSA.3.1[MB]

The TSF shall enforce the **Message Bus SFP** to provide restrictive default values for security attributes that are used to enforce the *SFP*.

5.1.17.2 FMT_MSA.3.2[MB]

The TSF shall allow the **System Administrator** to specify alternative initial values to override the default values when an object or information is created.

5.1.18 FMT_MTD.1 - Management of TSF data

5.1.18.1 FMT_MTD.1.1

The TSF shall restrict the ability to modify the **database contents, Wizard ports** to the **System Administrator role**.

5.1.19 FPT_ITT.1 - Basic internal TSF data transfer protection

5.1.19.1 FPT_ITT.1.1

The TSF shall protect TSF data from disclosure, modification when it is transmitted between separate parts of the TOE.

## 5.2 Explicitly Stated TOE Security Functional Requirements

The following Security Functional Requirements have been explicitly stated.

There are three to allow for the TOE to work in concert with the environment to provide Domain Separation, Enforcement of TOE functions and Protection of Audit Trail Storage.

The TOE provides Enterprise Collection analysis and notification capabilities that are not exactly covered by any of the CC SFRS. There are 4 SFR's defined covering enterprise event collection, review and storage.

5.2.1 FAU_STG_EXP.1 - Protected audit trail storage

Based on the CC requirement FAU_STG.1

5.2.1.1 FAU_STG_EXP.1.1

The TSF, **in conjunction with the underlying OS,** shall protect the stored audit records from unauthorized deletion.

5.2.1.2 FAU_STG_EXP.1.2

The TSF, **in conjunction with the underlying OS,** shall be able to prevent unauthorized modifications to the audit records in the audit trail.

5.2.2 FPT_RVM_EXP.1 - Reference mediation

Based on the CC requirement FPT_RVM.1

5.2.2.1 FPT_RVM_EXP.1.1

The TSF, **when invoked by the underlying host OS**, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2.3 FPT_SEP_EXP.1 - Domain separation

Based on the CC requirement FPT_SEP.1

5.2.3.1 FPT_SEP_EXP.1.1

The TSF, **when invoked by the underlying host OS**, shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

5.2.3.2 FPT_SEP_EXP.1.2

The TSF, **when invoked by the underlying host OS**, shall enforce separation between the security domains of subjects in the TSC.

5.2.4 ESEC_COL.1 Collection of Enterprise Event Data

This SFR is required to identify the breadth of enterprise alert data that can be collected by defining the list of Product Types, Event Types and Event Details that can be identified from each product type.

This requirement is based on the CC requirement FAU.GEN.1

5.2.4.1 ESEC_COL.1.1

The active agents, configured by the Wizard shall be able to collect the following **event informtion**, depending upon the product type being monitored:

a) **Startup and Shutdown events,**

b) **The events specified in the event column of Table 20 Enterprise Event Data.**

5.2.4.2 ESEC_COL.1.2

The TSF shall record within each **event** record at least the following information

a) **Date and time of the event,**

b) **The details specified in the detail column of Table 20 Enterprise Event Data.**

| Component | Product Type | Event | Details |
|---|---|---|---|
| ESEC_COL.1 | Network-Based IDS (NIDS) | I&A Events<br>Service requests<br>Network Traffic | Sensor Name<br>Source IP Address<br>Source Port<br>Destination IP Address<br>Destination Port<br>Protocol<br>Event Type<br>Signature |
| ESEC_COL.1 | Network Devices (Router, Switch, Gateway) | I&A Events<br>Service requests<br>Network Traffic | Node Name<br>Source IP Address<br>Source Port<br>Destination IP Address<br>Destination Port<br>Protocol<br>Event Name |
| ESEC_COL.1 | Firewalls | I&A Events<br>Service requests<br>Network Traffic | Node Name<br>Source IP Address<br>Destination IP Address<br>Protocol<br>Source Port<br>Destination Port<br>Event Name<br>Direction |
| ESEC_COL.1 | Antivirus | Service requests<br>Security config changes | Source User Name<br>Destination User Name<br>File<br>Method<br>Virus Name<br>Action Name |
| ESEC_COL.1 | Databases | Data Access<br>Service requests<br>Security config changes<br>Data introduction | Requested access<br>Source User Name<br>Source Port Name<br>Event Name<br>Object Name<br>Owner<br>Return Code |
| ESEC_COL.1 | Operating Systems | Data Access<br>Service requests<br>Security config changes<br>Data introduction | Requested access<br>Source IP Address or Hostname<br>Destination User Name<br>Source Port Name<br>Event Name<br>Event Level (Severity)<br>Facility<br>Location of Object |
| ESEC_COL.1 | Host-Based IDS (HIDS) | Security config changes | Requested access |

| | | | |
|---|---|---|---|
| | | Data introduction<br>Data Access | Source IP Address or Hostname<br>Destination User Name<br>Source Port Name<br>Event Name<br>Event Level (Severity)<br>Facility<br>Location of Object |
| ESEC_COL.1 | Telecommunication Equipment | Security config changes<br>Network Traffic | Requested access<br>Event Name<br>Event Level (Severity)<br>Facility |
| ESEC_COL.1 | Web Servers | Data Access<br>Service requests<br>Security config changes<br>Data introduction | Requested access<br>Source IP Address or Hostname<br>Source Port Name<br>Event Name<br>Event Level (Severity)<br>Status Code<br>Location of Object |

**Table 20 – ESEC_COL.1 Details**

### 5.2.5 ESEC_RDR.1 Restricted Review of Enterprise Event Data

This SFR is required to show that the TOE provides a way to review all the data that has been collected through ESEC_COL.1.

This requirement is based on a combination of FAU_SAR1 & FAU_SAR.2

#### 5.2.5.1 ESEC_RDR.1.1

The Sentinel Control Center Console will provide the authorized administrator and Operator role with access to read the Enterprise Event Data.

#### 5.2.5.2 ESEC_RDR.1.2

The Sentinel Control Center Console shall provide the Enterprise Event data in a manner suitable for the user to interpret the information.

#### 5.2.5.3 ESEC_RDR.1.3

The Sentinel Control Center Console shall prohibit all users read access to the Enterprise Event data, except those users that have been granted explicit read-access.

### 5.2.6 ESEC_STG.1 Protected Storage of Enterprise Event Data

This SFR is required to show that the collected enterprise event data can be stored securely and managed.

This requirement is based on a combination of FAU_STG.1 & FAU_STG.2

#### 5.2.6.1 ESEC_STG.1.1

The TSF shall protect the stored **Enterprise Event data** from unauthorized deletion.

5.2.6.2 ESEC_STG.1.2

The TSF shall be able to prevent unauthorized modifications to the stored **Enterprise Event Data**.

5.2.6.3 ESEC_STG.1.3

The TSF shall ensure that the Enterprise Event Data stored in the database shall be maintained when the following conditions occur: Enterprise Event data storage exhaustion.

5.2.7 ESEC_STG.2 Prevention of Loss of Enterprise Event Data

This SFR is required to show how the TOE would handle the exhaustion of its enterprise event data storage location.

This requirement is based on FAU_STG.4

5.2.7.1 ESEC_STG.2.1

The database shall **ignore all new Enterprise Event Data**, the Sentinel Server shall 'overwrite the oldest stored Enterprise Event data in the iSCALE buffer' and send an alarm if the **Enterprise Event Data** storage capacity has been reached.

## 5.3 TOE IT Environment Security Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

5.3.1 FAU_SAR.1 - Audit Review

5.3.1.1 FAU_SAR.1.1

The ***host OS of the Database Server*** shall provide an **authorized system administrator** with the capability to read **all logged identification and authentication events** from the audit records.

5.3.1.2 FAU_SAR.1.2

The ***host OS of the Database Server*** shall provide the audit records in a manner suitable for the user to interpret the information.

5.3.2 FAU_SAR.3 - Selectable Audit Review

5.3.2.1 FAU_SAR.3.1

The ***host OS of the Database Server*** shall provide the ability to perform searches, sorting, ordering, of audit data based **on Date & Time, and Type of event**.

5.3.3 FPT_STM.1 - Reliable time stamps

5.3.3.1 FPT_STM.1.1

The ***TOE IT Environment*** shall be able to provide reliable time stamps for the ***use of the TOE***.

## 5.4 Explicitly Stated TOE IT Environment Security Functional Requirements

The following IT Environment Security Functional Requirements have been explicitly stated. The SFR's defined below are based on FAU_STG.1, FPT_RVM.1, FPT_SEP.1, FIA_UAU.1, and FIA_UID.2 taken from Part 2 of the CC.

The first three to allow for the IT Environment to work in concert with the TOE to provide Domain Separation, Enforcement of TOE functions, and Protection of Audit Trail Storage.

FIA_UAU_OS.1 and FIA_UID_OS.2 provide security for the use of the **Utilities**[3]

### 5.4.1 FAU_STG_OS.1 - Protected audit trail storage

#### 5.4.1.1 FAU_STG_OS.1.1

The ***security functions of the host OS*** shall, ***in conjunction with the security functions of the TOE,*** protect the stored audit records from unauthorized deletion.

#### 5.4.1.2 FAU_STG_OS.1.2

The ***security functions of the host* OS** shall, ***in conjunction with the security functions of the TOE,*** be able to prevent unauthorized modifications to the audit records in the audit trail.

### 5.4.2 FPT_RVM_OS.1 Non-bypassability of the TSP

#### 5.4.2.1 FPT_RVM_OS.1.1

The ***security functions of the host OS*** shall ensure that ***host OS security* policy** enforcement functions are invoked and succeed before each function within the **scope *of control of the host OS*** is allowed to proceed.

### 5.4.3 FPT_SEP_OS.1 TSF domain separation

#### 5.4.3.1 FPT_SEP_OS.1.1

The ***security functions of the host OS*** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects ***in the scope of control of the host OS***.

#### 5.4.3.2 FPT_SEP_OS.1.2

The ***security functions of the host OS*** shall enforce separation between the security domains of subjects in the ***scope of control of the host OS.***

### 5.4.4 FIA_UAU_OS.1 User Authentication

#### 5.4.4.1 FIA_UAU_OS.1.1

The IT Environment shall allow **identification as stated in FIA_UID_OS.2** on behalf of the ***authorized administrator accessing the TOE*** to be performed

before the ***authorized administrator*** is authenticated

5.4.4.2 FIA_UAU_OS.1.2

The IT Environment shall require each ***authorized administrator*** to be successfully authenticated before allowing any other IT Environment-mediated actions on behalf of that ***authorized administrator***.

5.4.5 FIA_UID_OS.2 User Identification

5.4.5.1 FIA_UID_OS.2.1

The IT Environment shall require each user to identify itself before allowing any other IT Environment-mediated actions on behalf of that user

## 5.5 TOE Strength of Function Claim

The only probabilistic or permutation mechanisms in the product are the password mechanism used to authenticate users and the cryptographic mechanisms. Strength of cryptographic algorithms is outside the scope of the Common Criteria.

The claimed minimum strength of function is SOF-BASIC. FIA_UAU.1 is the only non-cryptographic TOE security functional requirement that contains a permutation function, for which the claim of minimum strength of SOF-basic is made.

A complex password is required.

## 5.6 TOE Security Assurance Requirements

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

| Assurance Class | Assurance Components | |
|---|---|---|
| ACM: Configuration management | ACM_CAP.2 | Configuration items |
| ADO: Delivery and operation | ADO_DEL.1 | Delivery procedures |
| | ADO_IGS.1 | Installation, generation, and start-up procedures |
| ADV: Development | ADV_FSP.1 | Informal functional specification |
| | ADV_HLD.1 | Descriptive high-level design |
| | ADV_RCR.1 | Informal correspondence demonstration |
| AGD: Guidance documents | AGD_ADM.1 | Administrator guidance |
| | AGD_USR.1 | User guidance |
| ATE: Tests | ATE_COV.1 | Evidence of coverage |
| | ATE_FUN.1 | Functional testing |
| | ATE_IND.2 | Independent testing – sample |
| AVA: Vulnerability assessment | AVA_SOF.1 | Strength of TOE security function evaluation |
| | AVA_VLA.1 | Developer vulnerability analysis |

**Table 21 - Assurance Requirements: EAL2**

## 5.7 Rationale - TOE Security Requirements

### 5.7.1 TOE Security Functional Requirements to Objectives mapping

| | FAU_GEN.1 | FAU_SAR.1 | FAU_SAR.3 | FAU_STG_EXP.1 | FDP_IFF.1[AA] | FDP_IFC.1[AA] | FDP_IFF.1[MB] | FDP_IFC.1[MB] | FDP_ITC.1 | FDP_ITT.1 | FIA_ATD.1 | FIA_UAU.1 | FIA_UID.1 | FMT_MOF.1 | FMT_MSA.3[AA] | FMT_MSA.3[MB] | FMT_MTD.1 | FMT_SMR.1 | FMT_SMF.1 | FPT_ITT.1 | FPT_RVM_EXP.1 | FPT_SEP_EXP.1 | ESEC_COL.1 | ESEC_RDR.1 | ESEc_STG.1 | ESEC_STG.2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.LOGIN | | | | | | | | | | | X | X | X | | | | | | | | | | | | | |
| O.SECURE_COMMUNICATIONS | | | | | | | X | X | | X | | | | | | X | | | | X | | | | | | |
| O.ALERT_COLLECT | | | | | X | X | | | X | | | | | | X | | X | | | | | | X | | | |
| O.ALERT_STORAGE | | | | | | | | | | | | | | | | | X | | | | | | | | X | X |
| O.ALERT_REVIEW | | | | | | | | | | | | | | | | | | | | | | | | X | | |
| O.AUDIT_TRAIL | X | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.AUDIT_STORAGE | | | | X | | | | | | | | | | | | | | | | | | | | | | |
| O.AUDIT_REVIEW | | X | X | X | | | | | | | | | | | | | | | | | | | | | | |
| O.SECURITY_MANAGEMENT | | | | | | | | | | | | | | X | X | X | | X | X | | | | | | | |
| O.SEL_PRO | | | | | | | | | | | | | | | | | | | | | X | X | | | | |

**Table 22 – SFR and Security Objectives Mapping**

#### 5.7.1.1 FAU_GEN.1

Audit Generation is required to meet the objective O.AUDIT_TRAIL and achieves this by stating that the actions in table 16 will generate audit events as described in table 16.

#### 5.7.1.2 FAU_SAR.1

Audit Review is required to meet the objective O.AUDIT_REVIEW and achieves this by requiring the TOE to provide a way to review the data in readable form.

#### 5.7.1.3 FAU_SAR.3

Selectable Audit Review is required to meet the objective O.AUDIT_REVIEW and achieves this by requiring the TOE to provide tools to search, sort & order the audit logs based on criteria selected by the authorized administrator.

#### 5.7.1.4 FDP_IFF.1[AA]

Simple security attributes is required to partially meet the O.ALERT_COLLECT objective by defining the attributes that determine if user data can be imported into the TOE

#### 5.7.1.5 FDP_IFC.1[AA]

Subset information flow control is required to partially meet the O.ALERT_COLLECT objective by enforcing the flow control policy allowing user data to enter the TOE.

#### 5.7.1.6 FDP_IFF.1[MB]

Simple security attributes is required to partially meet the

O.SECURE_COMMUNICATIONS objective by defining the attributes that determine if the console can communicate to other TOE components.

#### 5.7.1.7 FDP_IFC.1[MB]

Subset information flow control is required to partially meet the O.SECURE_COMMUNICATIONS objective by enforcing the flow control policy allowing communication between the pieces of the TOE.

#### 5.7.1.8 FDP_ITC.1

Import of user data without security attributes is required to meet the O.ALERT_COLLECT objective by defining how the data is imported into the TOE from the environment.

#### 5.7.1.9 FDP_ITT.1

Basic internal transfer protection is required to meet the O.SECURE_COMMUNICATIONS objective by ensuring that the TOE provides the facilities to encrypt and validate the data communications between the pieces of the Distributed TOE. [2]

#### 5.7.1.10 FIA_ATD.1

User Attribute Definition is required to meet the O.LOGIN objective by requiring the authorized administrator's user id representing a person.

#### 5.7.1.11 FIA_UAU.1

Timing of Authentication is required to meet the O.LOGIN objective by providing named accounts and unique passwords to access the TOE.

#### 5.7.1.12 FIA_UID.1

Timing of Identification is required to meet the O.LOGIN objective by providing a limited set of functions that can be performed without the user identifying themselves to the TOE.

#### 5.7.1.13 FMT_MOF.1

Management of security functions behavior is required to meet the O.SECURITY_MANAGMENT objective by defining the parameters for the management of the TOE security functions and the alert stream.

#### 5.7.1.14 FMT_MSA.3[AA]

Static Attribute Initialization is required to meet O.ALERT_COLLECT by setting restrictive default values upon the Accept Alerts SFP. The modification of these values is handled by O.SECURITY_MANAGEMENT

#### 5.7.1.15 FMT_MSA.3[MB]

Static Attribute Initialization is required to meet O.SECURE_COMMUNICATIONS by setting restrictive default values upon the Message Bus SFP. The modification of these values is handled by O.SECURITY_MANAGEMENT

#### 5.7.1.16 FMT_MTD.1

The management of TOE data is required to meet the O.ALERT_STORAGE objective by requiring the authorized administrator to manage the TOE data storage.

Wizard port configuration is needed to meet O.ALERT_COLLECT by defining location parameters of security event data.

#### 5.7.1.17 FMT_SMR.1

Security roles are required to meet the objective O.SECURITY_MANAGEMENT by enforcing privilege during the management process.

#### 5.7.1.18 FMT_SMF.1

Security Functions are required to meet the objective O.SECURITY_MANAGEMENT by providing the functions necessary to manage the TOE.

#### 5.7.1.19 FPT_ITT.1

Basic internal TSF data transfer protection is required to meet the objective O.SECURE_COMMUNICATIONS by enforcing the TOE's ability to encrypt data using AES or ARC4.

#### 5.7.1.20 FAU_STG_EXP.1

Protected audit trail storage is required to meet the objective O.AUDIT_REVIEW by preventing unauthorized modification /deletion of the audit trail in conjunction with the TOE environment.

Protected audit trail storage is required to meet O.AUDIT_STORAGE by providing a managed location for the TOE Audit trail in conjunction with the TOE environment.

#### 5.7.1.21 FPT_RVM_EXP.1

Non-Bypassability of the TOE is required to meet the O.SEL_PRO objective by enforcing that the TOE in concert with the TOE environment is configured to ensure that all TSP enforcement functions and invoked and succeed before any function is allowed to proceed.

#### 5.7.1.22 FPT_SEP_EXP.1

Domain Separation is required to meet the O.SEL_PRO objective by enforcing that the TOE in concert with the TOE environment maintains a security domain for it's own execution to protect it from tampering by un-trusted subjects.

#### 5.7.1.23 ESEC_COL.1

Active Agents configuration is needed to meet O.ALERT_COLLECT by defining the normalization of Enterprise Event Data from disparate enterprise devices.

#### 5.7.1.24 ESEC_RDR.1

Restricted Data review is required to meet O.ALERT_REVIEW by defining who can review what of the collected Enterprise Event Data.

#### 5.7.1.25 ESEC_STG.1

Protected Storage of Enterprise Event Data is required to meet O.ALERT_STORAGE by restricting who can delete, modify and how the data is maintained in the event of storage space exhaustion.

#### 5.7.1.26 ESEC_STG.2

Prevention of loss of Enterprise Event data is required to meet O.ALERT_STORAGE by defining the actions occurring should the storage capacity be exhausted.

## 5.8 TOE Security Assurance Requirements - Rationale

EAL2 was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws.

## 5.9 Rationale For IT Environment Security Requirements

| | FAU_SAR.1 | FAU_SAR.3 | FPT_STM.1 | FAU_STG_OS.1 | FPT_RVM_OS.1 | FPT_SEP_OS.1 | FIA_UAU_OS.1 | FIA_UID_OS.2 |
|---|---|---|---|---|---|---|---|---|
| OE.TIME_SRC | | | X | | | | | |
| OE.SEL_PRO | | | | | X | X | | |
| OE.AUDIT_STORAGE | | | | X | | | | |
| OE. I&A_AUDIT_REVIEW | X | X | | | | | | |
| OE.I&A_AUDIT_STORAGE | | X | | | | | | |
| OE.OSLOGIN | | | | | | | X | X |

**Table 23 – Security Functional Requirements for the Environment**

### 5.9.1 FAU_STG_OS.1

Protected Audit storage is required to meet the environmental objective, OE.AUDIT_STORAGE that states that the TOE environment, in conjunction with the TOE shall prevent unauthorized reading or modification of the TOE Audit Trail.

### 5.9.2 FPT_RVM_OS.1

Non-Bypassability of the TSP is required to meet the environmental objective OE.SEL_PRO that states that TOE, in conjunction with the environment, protect itself against attempts by unauthorized users to bypass, deactivate or temper with the TOE Security functions

### 5.9.3 FPT_SEP_OS.1

Domain Separation of the TSF is required to meet the environmental objective

OE.SEL_PRO that states that the TOE, in conjunction with the environment, protect itself against attempts by unauthorized users to bypass, deactivate or temper with the TOE Security functions

### 5.9.4 FAU_SAR.1

Audit Review of Identification and Authentication events is required to meet the environmental objective OE. I&A_AUDIT_REVIEW that states the TOE environment shall provide system administrators with the capability to review Identification and Authentication audit records.

### 5.9.5 FAU_SAR.3

Searches, sorting, and ordering of Identification and Authentication audit event data is required to meet the environmental objective OE. I&A_AUDIT_REVIEW that states the TOE environment shall provide system administrators with the capability to perform searches, sorting, and ordering of Identification and Authentication audit event records.

### 5.9.6 FAU_STG_OS.1

Protected Audit storage is required to meet the environmental objective, OE.I&A_AUDIT_STORAGE that states that the TOE environment shall prevent unauthorized reading or modification of the TOE Audit Trail.

### 5.9.7 FIA_UAU_OS.1

Identification is required to meet the environmental objective OE.OSLOGIN which states that the TOE environment shall require identification and authentication of authorized administrators

### 5.9.8 FIA_UID_OS.2

Authentication is required to meet the environmental objective OE.OSLOGIN which states that the TOE environment shall require identification and authentication of authorized administrators

### 5.9.9 FPT_STM.1

Reliable Time Stamps is required to meet the objective OE.TIME_SRC that states that the TOE environment shall provide a reliable time stamp for the use of the TOE.

## 5.10 Rationale For IT Security Requirement Dependencies

This section includes a table of the requirements are their dependencies and a rational for any dependencies that are not satisfied. Unless stated other wise the dependency, as listed is met. See also 5.11

| SFR | Dependencies |
|---|---|
| FAU_GEN.1 | FPT_STM.1 (Covered by the environment) |
| FAU_SAR.1 | FAU_GEN.1 |
| FAU_SAR.3 | FAU_SAR.1 |

| | |
|---|---|
| FDP_IFF.1[AA] | FDP_IFC.1[AA]<br>FMT_MSA.3[AA] |
| FDP_IFF.1[MB] | FDP_IFC.1[MB]<br>FMT_MSA.3[MB] |
| FDP_IFC.1[AA] | FDP_IFF.1[AA] |
| FDP_IFC.1[MB] | FDP_IFF.1[MB] |
| FDP_ITT.1 | FDP_IFC.1[MB] |
| FDP_ITC.1 | FDP_IFC.1[AA]<br>FMT_MSA.3[AA] |
| FIA_ATD.1 | None |
| FIA_UAU.1 | FIA_UID.1 |
| FIA_UID.1 | None |
| FMT_MOF.1 | FMT_SMF.1<br>FMT_SMR.1 |
| FMT_MSA.3[AA] | FMT_MSA.1<br>FMT_SMR.1 |
| FMT_MSA.3[MB] | FMT_MSA.1<br>FMT_SMR.1 |
| FMT_MTD.1 | FMT_SMF.1<br>FMT_SMR.1 |
| FMT_SMR.1 | FIA_UID.1 |
| FMT_SMF.1 | None |
| FPT_ITT.1 | None |
| FAU_STG_EXP.1 | FAU_STG_OS.1 (Environmental Contributing SFR) |
| FPT_RVM_EXP.1 | FPT_RVM_OS.1 (Environmental Contributing SFR) |
| FPT_SEP_EXP.1 | FPT_SEP_OS.1 (Environmental Contributing SFR) |
| ESEC_COL.1 | None |
| ESEC_RDR.1 | ESEC_COL.1 |
| ESEC_STG.1 | ESEC_COL.1 |
| ESEC_STG.2 | ESEC_COL.1 |

**Table 24 – SFR Dependencies**

## 5.11 Rationale for not including dependencies.

Functional component FMT_MSA.3 depends on functional component FMT_MSA.1 Management of Security Attributes. In an effort to place all the management requirements in a central place, FMT_MOF.1 was used. Therefore FMT_MOF.1 more than adequately satisfies the concerns of leaving FMT_MSA.1 out of this Security Target.

Since the TOE is software only it requires the time to be provided from an external source – hence FPT_STM.1 is provided by the host hardware and operating system. Since the TOE assumes no unauthorized physical access the time source can be assumed to be valid as it can only be modified by the TOE Administrator.

Since the TOE is software only it also requires help from the Environment to meet FAU_STG.1, FPT_RVM.1 & FPT_SEP.1. These Functions have been iterated and split across the TOE & Environment to illustrate that the TOE & Environment are a mutually supporting set of components.

## 5.12 Rationale For Internal Consistency and Mutually Supportive

All operations performed on the security requirements comply with the rules and intent required by the operation in the CC. The requirements defined in the ST are not contradictory.

The selected requirements together form a mutually supportive whole by:

- satisfying all dependencies as demonstrated in Sections 5.10 & 5.11
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.7.1
- including audit requirements to detect security-related actions and potential attacks
- including security management requirements to ensure that the TOE is managed and configured securely.

## 5.13 Rationale For Strength of Function Claim

The rationale for choosing SOF-basic is based on the low attack potential of threats identified in this ST. The security objectives provide probabilistic security mechanisms and the strength of function claim is satisfied by the password management features provided by the TOE.

This applies to the Authentication Mechanism identified in FIA_UAU.1 and maps to the Identification and Authentication Security Function.

The administratively required complex passwords will meet SOF-Basic with a less than 1 in a million chance of randomly guessing the password.

The user authentication mechanism requires a password length of 8 characters that includes alphanumeric characters. By requiring passwords the claim exceeds the minimum strength of function requirement of SOF-basic.

# 6 TOE Summary Specification

## 6.1 TOE Security Functions

### 6.1.1 Identification and Authentication

The TOE provides a single authentication mechanism that is used to access different functional areas and complies with SOF-Basic.

**FIA_UAU.1, FIA_UID.1**

The TOE uses the Database (either MS SQL Server 2000 or Oracle 9i) authentication code to authorize the users. The Sentinel Control Center, Wizard Agent Builder, and Sentinel Data Manager all provide a login dialog box. Logging in sends the authentication data along iSCALE to the DAS and then to either MS SQL Server or the Oracle Database where the database authenticates the request against it's internal user management system, provides the yes/no answer to the GUI that responds by allowing or denying the user access.

The Sentinel Control Center provides the Management console. The authorized administrator or operator is required to log in to the Sentinel Control Center prior to being able to performing any other TOE function.

The authorized system administrator is required to log in to the Sentinel Data Manager and Wizard Agent Builder prior to being able to performing any other TOE function.

The authorized system administrator is required to log in to the SQL Server Enterprise Manager, a management application for SQL Server 2000 or SQL*PLUS, a Command Line execution program for Oracle Database prior to managing permissions for accounts necessary to occupy the system administrator role.

User passwords must be chosen with at least 8 with characters in length and include at least one UPPER CASE, one lower case, one special symbol (#$_) and one numeric (0-9).

**FIA_ATD.1**

The TOE provides the database (either MS SQL Server 2000 or Oracle 9i) to store permissions belonging to users. Role based permissions are not supported by default by the TOE however for the purposes of the CC evaluated version a set of specific permissions comprising 3 roles have been defined. These user roles are the Operator (Read Only), the Enterprise Information Administrator and the System Administrator (full access).

User accounts are managed through User Manager, located on the Admin tab within Sentinel Control Center – see section 6.1.4 for more detail.

In addition to the User Manager, the System Administrator's permissions necessary to manage the TOE Audit data and the Enterprise Event Data are managed through SQL Server Enterprise Manager, a management application for SQL Server 2000 or SQL*PLUS, a Command Line execution program for Oracle Database. In this manner, permissions are added to the System Administrator's account. This allows that user to access the Sentinel Data Manager to View/Add/Archive/Delete database partitions.

If the authorized administrator or operator fails to enter correct credentials 3

times their session is disconnected from the Sentinel Control Center.

Once authenticated to Sentinel Control Center the authorized system administrator has full access to all of the security features of the TOE.

Once authenticated to the Sentinel Control Center the authorized operator has read only access to the TOE data and enterprise event data.

Once authenticated to the Sentinel Control Center the Enterprise Information Administrator has an intermediate level of access.

When the TOE is installed 5 esecurity user accounts are created (see table 25).

Esecapp represents the user name used by the e-Security applications to access the database – it has dbo level permissions over the database. (dbo represents database owner and has full permissions to the database).

Esecadm - The default account created during installation occupying the System Administrator role.

The esecapp & esec_corr accounts are not used by human users.

| Account name | Account Purpose |
|---|---|
| Esecapp | The account Sentinel processes use to access the database (This is configurable at install time) |
| esecadm | Sentinel administrator user (configurable at install time). Note: For Solaris, the Installer also creates the operating system user with the same user name and password. |
| esecrpt | Reporter user account – used by the BusinessObjects XI service to retrieve data. Not used in the TOE evaluated configuration. |
| Esec_corr | Correlation Engine users, used to create incidents. |
| Esecdba | This account is used in the initial installation stages to allow the administrator performing the installation to allocate DBO permissions to the System Administrator accounts through the SQL Enterprise Manager or the Oracle SQL client |

**Table 25 - User accounts created during installation.**

### 6.1.2 Audit

The TOE provides the capability to generate audit records as a result of successful and failed requests for it to authenticate authorized administrator/operators, collect enterprise event data, and a subset of the security management functions.

**FAU_GEN.1**

Each audit event recorded includes the date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event

Auditing of TOE Security functions is achieved in the following manner.

1. The Sentinel Server writes all audit records received to DAS via iSCALE
2. This data is then stored in either MS SQL Server or the Oracle Database. For more detail see section 6.1.3.

NOTE See Appendix A of Sentinel 5.1.1 User's Guide For Solaris and Windows

September 2005 for Details of the events generated and captured by the system.

**FAU_SAR.1, FAU_SAR.3**

Once in the database, event data and audit data corresponding to FMT_MOF.1 are available through the Sentinel Control Center using Active Views or report creation. See section 6.1.3 for the detail of the Active Views and reports of event data.

**FAU_STG_EXP.1**

The database protects and prevents the audit data from unauthorized deletion or modification through its internal mechanisms that require user identification and authentication for the Sentinel Data Manager utility. Since the database resides on a file system in the TOE Environment, the TOE relies on the host OS to protect the files that comprise the audit store from unauthorized deletion or modification.

### 6.1.3 Enterprise Event Data

**ESEC_COL.1**

The TOE provides the capability to collect, store, and review Enterprise Event Data generated from disparate devices throughout the enterprise.

The Wizard is responsible for the configuration and management of the agents and Wizard ports that are used to listen to the alerts coming from the devices and normalize that data according to the Accept Alerts SFP.

Once activated by the system administrator, the agent receives and normalizes the data. See section 5.2.4 for details regarding the type of systems and data that can be collected from those product types.

**ESEC_RDR.1**

The TOE provides the Sentinel Control Center with facilities to review the events generated by the Agents. There is no way through the Sentinel Control Center to delete any Enterprise Event Data.

The GUI provides the following:

**Active Views** – This tab allows the users of the TOE to

- Take a snapshot of an Event Real Time table at a specific point in time
- Manage the columns in an Event Real Time table
- Sort the columns in a Snapshot Event Real Time table
- View event details
- Create or add to an incident; incidents display in the Incidents tab
- Send an e-mail message about an event
- Monitor and evaluate events based on custom menu options that are configured as a Menu Configuration option in the Admin tab
- Save charts as portable network graphics (.png) files

**Incidents**

The value in collecting the data from all these systems is that seemingly unconnected events can be tied together into incidents and incidents grouped into cases. This is managed on the incidents tab.

An event is an action or occurrence detected by a security device or program. Events are considered to be “stateless.”

An incident is the grouping of one or more events that are deemed to be important (a possible attack). Incidents have “states” in that they require a response and closure.

A case is the grouping of one or more related incidents. Cases also have “state” and are investigated, acted upon, and tracked to completion.

For example

an http request through a firewall
some odd network traffic reported in an IDS
processor utilization spike on a server

Taken separately these events could mean nothing but when tied together by a correlation rule into an incident could indicate a new worm.

**Analysis**

This allows the users of the TOE to

- Create historical reports - These reports allow for filtering by allowing the Authorized administrator or Operator to choose Time & Date, Device & event type (for complete details see section 5.1.1). The generated reports allow sorting & ordering of the filtered data by clicking the column headings.

**Admin tab / Global filters**

From the admin tab the Authorized administrator can

- Configure General Options (including general Analysis reporting options)
- Configure Correlation rules to look for patterns in incoming Enterprise Event Data. The rules can be defined using a wizard or free form using the RuleLG definition language.
- Configure Global filters that are applied by the Wizard Agent Manager to all Active Agents.
- The Event Table menu allows the configuration of some immediate responses that can be taken to events. For example PING the host / TRACERT / NSLOOKUP or WHOIS the source IP address
- Configure Public & Private filters
- User Account Management (see 6.1.4 for more detail)

**ESEC_STG.1**

The TOE provides the database (either MS SQL Server or Oracle) to store the Enterprise Event Data. The database protects and prevents the Enterprise Event data from unauthorized deletion or modification through it’s internal mechanisms that require user identification and authentication for the Sentinel Data Manager utility. The Sentinel Data Manager can only be accessed by a System

Administrator. (See section 6.1.4for more detail).

**ESEC_STG.2**

By default the buffers in the Sentinel Server are configured to store up to 5 MB of Enterprise Event Data should either MS SQL Server or the Oracle Database become full.

The Wizard Agent Manager machines that house the agents can also buffer events up to the capacity of their internal hard drives should communications fail.

### 6.1.4 Management of TOE security functions

**FMT_MOF.1, FMT_SMF.1**

The Sentinel Control Center, Wizard Agent Builder, and the Sentinel Data Manager applications provide the interfaces necessary to manage the TOE security functions.

The Sentinel Control Center has separate screens, accessed by tabs.

See section 6.1.3 for those screens associated with the Collection, Review & management of Enterprise Event Data.

The Admin tab, with the exception of the User management & Public & Private filters, is covered in section 6.1.3.

The Admin tab allows the authorized administrator to add, delete, & modify TOE user accounts and their associated permissions. At a minimum the user's username and password are required to create an account. It also allows administration of filters, correlated rules, and security event management through incidents.

The Admin tab allows the authorized administrator to start/stop the Agent Manager on a selected host.

The Admin tab allows the authorized administrator to manage Global Filters, and Public/Private Filters.

To select an agent or modify configuration of an active agent, the authorized administrator must authenticate to the Wizard Agent Builder.

**FMT_SMR.1**

Role assignment is achieved by assigning the appropriate set of permissions for an Operator, Enterprise Information Administrator, or System Administrator type user to a user account and then cloning this user account as the template for adding new users of that user type.

The MS SQL Server Enterprise Manager, a management application for SQL Server & the Oracle database SQL*PLUS "grant" command are used to grant additional permissions to the System Administrators.

Public and private views are ways of restricting who can see what from the alert data – a view is applied to the user account as a restriction on the data they can review. The Enterprise Information Administrator and System Administrator are able to review all incoming data and the Operator is allowed to review Enterprise Event Data.

**FMT_MSA.3[AA]**

By default the Wizard Ports are configured to accept no incoming traffic. It is up to the System Administrator to update the configuration to allow the alert stream into the TOE. The agents cannot be modified without the user identifying themselves to the TOE.

**FMT_MTD.1**

To manage the Enterprise Event Data storage, the TOE provides the Sentinel Data Manager utility. The Sentinel Data Manager (SDM) is a GUI utility used to manage data storage and archival processes. To manage the Wizard Port, the TOE provides the Wizard Agent Builder. A System Administrators credentials are required to use the SDM and the Wizard Port within Wizard Agent Builder.

**FMT_MSA.3[MB]**

The management of iSCALE consists of updating the shared cryptographic key according to the instructions contained in Chapter 10 of the Sentinel 5.1.1 Install Guide. Without this key the default value will not allow any traffic to or from the device trying to connect to iSCALE.

The Agents tab allows some basic control over the Wizard Agent Manager and the ability to view the status of the agents.

### 6.1.5 User Data Protection

**FDP_IFF.1[AA], FDP_IFC.1[AA], FDP_ITC.1**

The TOE's access policies govern the ability for the TOE to accept the alert stream from the environment.

The ACCEPT_ALERTS security flow policy by default does not allow any Enterprise Event data into the TOE.

Based on the product type and by modifying the parameters identified in section 5.2.4, the system administrator can allow alert data into the TOE through the Wizard Agent Builder application. The only options in the policy are to explicitly allow data – there is no explicit deny, and if the data does not match explicitly the criteria defined in the SFP it is ignored.

The alert data is imported with no security attributes and then the agents normalize it according to rules defined by the Authorized administrator in the ACCEPT_ALERTS SFP.

**FDP_IFF.1[MB], FDP_IFC.1[MB], FDP_ITT.1**

The Inter TOE communication is regulated by the MESSAGE_BUS SFP. This policy ensures that only identified pieces of the TOE can communicate to each other over the encrypted communication channel, iSCALE. This identification is provided by a shared private encryption key. This key is part of the installation CD and for the CC evaluated version of the TOE the administrator is required to use the process outlined in Chapter 10 of the e-Security Sentinel 5 Install Guide to update the keys to make them unique for each implementation of the TOE.

Using the MESSAGE_BUS SFP the TOE provides and uses facilities to encrypt and verify the data as it is sent in it's normalized form from the Agent to the Sentinel Server thus prohibiting tampering with or eavesdropping on the data.

### 6.1.6 Protection of TOE functions

**FPT_ITT.1**

The TOE provides iSCALE to encrypt data transfers within the distributed TOE components including the Wizard, Sentinel Control Center, Sentinel server, and the Sentinel Data Manager.

This encryption mechanism uses AES or ARC4 for encryption.

**FPT_RVM_EXP.1**

The TOE ensures that all functions are invoked and succeed before each function may proceed. Non-bypassability of management functions is achieved by the identification and authentication mechanisms that ensure that the management functions are not bypassed. The TOE protects its management functions by isolating them through authentication of administrators. Additionally, IT environment requirements ensure that untrusted subjects in the host OS cannot interfere with TOE operation or bypass its checks.

**FPT_SEP_EXP.1**

The TOE (through the Agents) maintains a domain for its own execution separate from the Enterprise Event traffic that it analyzes. Threats to the TOE from the local host are mediated by security functions on the IT Environment and by assumptions regarding the non-IT Environment. The TSF is protected from interference that would prevent it from performing its functions. Protection of the TOE from physical tampering is ensured by its environment. It is assumed that the device will remain physically connected to the network so that a device cannot be bypassed. All processes on the TOE are trusted. The TOE systems are not used for general purpose operations and non-administrative users are not allowed to directly access the TOE. Non-administrative users can only interact with the TOE indirectly. Therefore domain separation is maintained.

## 6.2 Security Assurance Measures & Rationale

| Assurance Requirement | Assurance Rationale | Assurance Components |
|---|---|---|
| ACM_CAP.2 | The configuration management documents defines the configuration items and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE. | The description of the configuration items is provided in Configuration Management for e-Security Sentinel 5 v5.1.1, v.1.8, November 20th, 2006. |
| ADO_DEL.1 | The delivery document describes the steps performed to deliver the TOE. It describes the process used to create distribution copies of the TOE software and the steps taken to ensure consistent, dependable delivery of the TOE to the customer. | The description of the delivery procedures is provided in Delivery Documentation for e-Security Sentinel 5 v5.1.1, v.1.7, November 20th, 2006. |
| ADO_IGS.1 | The installation, documents describe the steps necessary for secure installation, generation and start-up of the TOE. | The installation, generation, and start-up procedures are provided in: Wrapper Document for e-Security Sentinel 5 v5.1.1, v.0.6, November 20th, 2006, |

| | | |
|---|---|---|
| | | Sentinel 5.1.1 Install Guide For Solaris and Windows, September 2005 |
| ADV_FSP.1 | The informal functional specification document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes the effects, exceptions, and error messages for each of the external TSF interfaces. | The informal functional specification is provided in e-Security Sentinel 5 v5.1.1 Functional Specification, November 20th, 2006, v.0.12 |
| ADV_HLD.1 | The descriptive high-level design describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified. | The descriptive high-level design is provided in e-Security Sentinel 5 v5.1.1 High Level Design, November 20th, 2006, v.0.08 |
| ADV_RCR.1 | The informal correspondence document maps the security functionality as described in the FSP and ST and as described in the FSP and HLD. | The informal correspondence demonstration is provided in:<br><br>e-Security Sentinel 5 v5.1.1 Functional Specification, November 20th, 2006, v.0.12<br><br>e-Security Sentinel 5 v5.1.1 High Level Design, November 20th, 2006, v.0.08 |
| AGD_ADM.1 | The administrator guidance documents provide complete administrative guidance for the TOE, including all security features and configuration items. | The administrator guidance is provided in the following documents:<br><br>Sentinel 5.1.1 User's Guide, for Solaris and Windows, September 2005<br><br>Sentinel 5.1.1 Wizard User's Guide for Solaris and Windows, September 2005<br><br>Sentinel 5.1.1 User's Reference Guide for Solaris and Windows, September 2005<br><br>Sentinel 5.1.1 Install Guide For Solaris and Windows, September 2005 |
| AGD_USR.1 | The user guidance describes the security functions and interfaces in a | No user guidance is provided for this product as there are no non-administrative users (PD-0106). |

| | | |
|---|---|---|
| | way that allows a user to interact with the TOE securely. | |
| ATE_COV.1 | The test coverage document provides a mapping of the test cases performed against the TSF. | The evidence of coverage is provided in<br><br>Test Plan and Coverage Analysis For e-Security Sentinel 5 v5.1.1 November 20th, 2006, v.0.7 |
| ATE_FUN.1 | The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort. | The functional testing description is provided in<br><br>Test Plan and Coverage Analysis For e-Security Sentinel 5 v5.1.1 November 20th, 2006, v.0.7 |
| ATE_IND.2 | The TOE hardware, software, guidance, and testing documentation were made available to the CC testing laboratory for independent testing. | The TOE and testing documentation were made available to the CC testing laboratory for independent testing. |
| AVA_SOF.1 | The strength of function analysis document provides the SOF argument for the password mechanism. | The strength of function analysis performed is provided in<br><br>Strength of Function Analysis for e-Security Sentinel 5 v5.1.1, November 20th, 2006 v.0.4 |
| AVA_VLA.1 | The vulnerability analysis document identifies and describes the process used to discover obvious vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified obvious vulnerability. | The vulnerability analysis performed is provided in<br><br>Vulnerability Analysis for e-Security Sentinel 5 v5.1.1, November 20th, 2006 v.0.6 |

**Table 26 - Assurance Requirements & Rationale: EAL2**

## 6.3 Rationale - TOE Security Functions

This rationale comprising the SFR to security function mapping has been included with Section 6.1.

## 6.4 Appropriate Strength of Function Claim

The rationale for choosing SOF-basic is based on the low attack potential of threats identified in this ST. The security objectives provide probabilistic security mechanisms and the strength of function claim is satisfied by the password management features provided by the TOE.

This applies to the User Id & Password identified in FIA_UAU.1 and maps to the Identification and Authentication Security Function.

The administratively required complex password will meet SOF-Basic with a less than 1 in a million chance of randomly guessing the password.

The user authentication mechanism requires a password length of 8 characters

that includes alphanumeric characters. By requiring passwords and disconnecting sessions, the claim exceeds the minimum strength of function requirement of SOF-basic.

## 6.5 Rationale for Security Assurance Requirements

See section 6.2

# 7 Protection Profile Claims

This Security Target does not claim conformance to any Protection Profiles.

# 8 Rationale

### 8.1.1 Security Objectives Rationale

Section 5.7 provide the security objectives rationale.

### 8.1.2 Security Requirements Rationale

Sections 5.6 provide the security requirements rationale.

### 8.1.3 TOE Summary Specification Rationale

Sections 6.3 - 6.5 provides the TSS to Security Function rationale.

### 8.1.4 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profiles

# 9 Appendix A - Role Definitions

<This section contains proprietary information has been removed at the request of the vendor.>

# 10 Appendix B – Utility Functions

<This section contains proprietary information has been removed at the request of the vendor.>