IBM Tivoli Security Operations Manager Security Target

ST Version 1.0
March 25, 2009

Prepared For:
IBM
6303 Barfield Rd. NE
Mail Drop A1-034
Atlanta, GA 30328

Prepared By:

Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Gateway Drive
Columbia, MD 21046

1 SECURITY TARGET (ST) INTRODUCTION 1

1.1 SECURITY TARGET, TOE, VENDOR, AND CC IDENTIFICATION 1
1.2 COMMON CRITERIA CONFORMANCE CLAIMS 1
1.3 CONVENTIONS 1
1.3.1 Acronyms 2
1.3.2 Terminology 3
1.4 SECURITY TARGET OVERVIEW AND ORGANIZATION 3
1.4.1 Overview 3
1.4.2 Organization 3

2 TARGET OF EVALUATION (TOE) DESCRIPTION 4

2.1 TOE OVERVIEW 4
2.2 TOE ARCHITECTURE 4
2.2.2 Physical Boundary 7
2.2.3 Logical Boundary 8

3 TOE SECURITY ENVIRONMENT 11

3.1 THREATS TO SECURITY 11
3.1.1 Threats addressed by the TOE 11
3.2 SECURE USAGE ASSUMPTIONS 11
3.2.1 Physical Assumptions 11
3.2.2 Personnel Assumptions 11
3.2.3 Intended Usage Assumptions 12
3.3 ORGANIZATIONAL SECURITY POLICES 12

4 SECURITY OBJECTIVES 13

4.1 SECURITY OBJECTIVES OF THE TOE 13
4.2 SECURITY OBJECTIVE OF THE IT ENVIRONMENT 13
4.3 SECURITY OBJECTIVE OF THE NON - IT ENVIRONMENT 13

5 IT SECURITY REQUIREMENTS 15

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 16
5.1.1 Security Audit (FAU) 16
5.1.2 User Data Protection (FDP) 17
5.1.3 Identification and Authentication (FIA) 17
5.1.4 Security Management (FMT) 18
5.1.5 Protection of the TSF (FPT) 19
5.1.6 IDS Components Requirements (IDS) 19
5.2 IT ENVIRONMENT SECURITY FUNCTIONAL REQUIREMENTS 20
5.2.1 Security Audit 20
5.2.2 Protection of the TSF (FPT) 20
5.3 TOE SECURITY ASSURANCE REQUIREMENTS 21
5.3.1 Configuration management (ACM) 21
5.3.2 Delivery and operation (ADO) 22
5.3.3 Development (ADV) 22
5.3.4 Guidance documents (AGD) 23
5.3.5 Life cycle support (ALC) 24
5.3.6 Tests (ATE) 24
5.3.7 Vulnerability assessment (AVA) 25

6 TOE SUMMARY SPECIFICATION 27

6.1 TOE SECURITY FUNCTIONS 27
6.1.1 Audit Function 27
6.1.2 Identification and Authentication 27

6.1.3 User Data Protection *28*
6.1.4 Security Management *29*
6.1.5 Protection of TSF *29*
6.1.6 IDS Function *30*
6.2 SECURITY ASSURANCE MEASURES 32
6.2.1 Configuration Management *32*
6.2.2 Delivery and Guidance *32*
6.2.3 Development *33*
6.2.4 Life cycle support *33*
6.2.5 Tests *33*
6.2.6 Vulnerability Assessment *33*

7 PROTECTION PROFILE CLAIM 34

8 RATIONALE 35

8.1 SECURITY OBJECTIVES RATIONALE 35
8.2 SECURITY REQUIREMENTS RATIONALE 40
8.2.1 Explicitly Stated Requirements Rationale *43*
8.2.2 Security Functional Requirement Dependency Rationale *44*
8.2.3 Security Assurance Requirements Rationale *44*
8.3 TOE SUMMARY SPECIFICATION RATIONALE 44
8.4 STRENGTH OF FUNCTION RATIONALE 46
8.5 INTERNAL CONSISTENCY AND SUPPORT 46

List of Tables

FIGURE 1: TIVOLI SECURITY OPERATIONS MANAGER SYSTEM ARCHITECTURE 7
TABLE 1: SECURITY FUNCTIONAL REQUIREMENTS 15
TABLE 2: AUDITABLE EVENTS 16
TABLE 3: ASSURANCE COMPONENTS FOR EAL3 21
TABLE 4: SECURITY ENVIRONMENT VS. SECURITY OBJECTIVES 36
TABLE 5: SECURITY FUNCTIONAL REQUIREMENTS VS. SECURITY OBJECTIVES 41
TABLE 5: SECURITY FUNCTIONAL REQUIREMENTS DEPENDENCIES 44
TABLE 6: SECURITY FUNCTIONAL REQUIREMENTS VS. SECURITY FUNCTIONS 45
TABLE 7: SECURITY ASSURANCE REQUIREMENTS VS. ASSURANCE MEASURES 46

1 Security Target (ST) Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) specifies the ST conventions and ST conformance claims; and describes the ST organization.

1.1 Security Target, TOE, Vendor, and CC Identification

ST Title – IBM Tivoli Security Operations Manager Security Target

ST Version – 1.0

TOE Identification – IBM Tivoli Security Operations Manager 4.1.1

Vendor –IBM

Evaluation Assurance Level (EAL) – EAL3

Common Criteria Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

1.2 Common Criteria Conformance Claims

This TOE and ST are consistent with the following specifications:

Common Criteria (CC) for Information Technology (IT) Security Evaluation Part 2: Security functional requirements, Version 2.3, August 2005.

- Part 2 Extended

Common Criteria (CC) for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.3, August 2005.

- Part 3 Conformant
- Evaluation Assurance Level 3 (EAL3)
- The minimum strength of function of SOF-Basic.

Note: Refer to Section 1.4 (Overview) for important information regarding the relationship of this ST to the *Intrusion Detection System Analyzer Protection Profile, Version 1.2, April 27, 2005*.

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FCS_COP.1(a) and FCS_COP.1(b) indicate that the ST includes two iterations of the FCS_COP.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold for additions. (e.g., "… **all** objects …") Deletions are removed without annotation.(eg. "…big some things…" notated as "…big things …").

- Security Assurance Requirements – Modifications and additions to components based on Interpretations are annotated by using bold.
- Explicitly stated requirements are identified with the short class name, IDS and (EXP) in the requirement title.

Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.1 Acronyms

CC	Common Criteria
CMS	Central Management System
DNS	Domain Name Server
EAL	Evaluation Assurance Level
EAM	Event Aggregation Module
GPS	Global Positioning System
GUI	Graphical User Interface
HIT	Host Investigative Toolkit
I&A	Identification and Authentication
IDS	Intrusion Detection System
IT	Information Technology
JRE	Java Runtime Environment
LDAP	Lightweight Directory Access Protocol
OPSEC	Open Platform for Security
SFP	Security Function Policy
SFR	Security Function Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSOM	Tivoli Security Operations Manager
TSP	TOE Security Policy
UCM	Universal Collection Module
XML	Extensible Markup Language
UI	User Interface

1.3.2 Terminology

Security Domain	A hierarchical, logical grouping of devices, networks, hosts and their associated data; used to compartmentalize information.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Target of Evaluation (TOE)	An IT product or system and its associated guidance documentation that is the subject of an evaluation.
Ticketing System	Ticketing System allows users to automatically or manually attach relevant events to a single ticket and pass the related events among groups and individuals,

1.4 Security Target Overview and Organization

1.4.1 Overview

This Security Target was originally written to conform to the *Intrusion Detection System Analyzer Protection Profile, Version 1.2, April 27, 2005*. Although the ST no longer claims conformance to this PP, most of the security objectives and requirements originate from the IDS Analyzer PP and the PP serves as a basis and rationale for various claims made in this ST as documented in application notes and footnotes throughout.

1.4.2 Organization

This security target is organized as follows:

- Section 2 – Target of Evaluation (TOE) Description - This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Environment - This section details the assumptions of the environment and the threats that are countered by the TOE and its environment.
- Section 4 – TOE Security Objectives - This section details the security objectives of the TOE and its environment.
- Section 5 – IT Security Requirements - This section presents the security functional requirements (SFRs) for the TOE and the IT Environment that supports the TOE, and details the assurance requirements for EAL3.
- Section 6 – TOE Summary Specification -This section describes the security functions represented in the TOE that satisfy the security requirements.
- Section 7 – Protection Profile Claims - This section presents any protection profile claims.
- Section 8 – Rationale - This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness and suitability.

2 Target of Evaluation (TOE) Description

The Target of Evaluation (TOE) is the IBM Tivoli Security Operations Manager (TSOM) Version 4.1.1. The TOE is a security event management software solution designed to provide a comprehensive and coherent view of enterprise security. The TOE correlates event data from disparate machines outside the TOE, called sensors. Sensors are third-party products such as firewalls, intrusion detection systems, computer systems, and routers. Once data is correlated from sensors, the TOE analyzes the data to uncover legitimate threats to the enterprise.

2.1 TOE Overview

The TOE provides specific features that include the following:

- Centralized logging from all deployed security devices across the enterprise including firewalls, network-based and host-based intrusion detection/prevention systems, computer systems and routers/switches, policy compliance devices, vulnerability assessment devices, integrated investigative tools, discover tools, application security devices, VPN, anti-virus, management systems, and web servers.
- Cross-device correlation of related events for more complete threat analysis.
- Detection and prioritization of invasive activities using threat analysis and rapid filtering.
- Notification of threats through a client console and alerting through third party applications such as e-mail and SNMP traps to network management tools
- The Event Console (Real Time Viewer) and the PowerGrid point and click graphical user interface (GUI) for viewing, searching and querying all event and audit data.
- The configuration of Action rules which automate common tasks associated with threat analysis and attack investigation such as remote host lookups and hostname and OS queries, portscans and traceroutes.
- Firewall blocking through interfaces to third party OPSEC firewalls such as Checkpoint.
- Detailed reporting for management and compliance initiatives. (Note: The correctness of the reports provided by the TOE to support these initiatives and the usability of the interface are not security-relevant and were not assessed by this evaluation effort.)
- Intuitive client interface for anytime and anywhere secure access.

2.2 TOE Architecture

The TOE is composed of the following subsystems:

- Event Aggregation Module (EAM)
- Universal Collection Module (UCM)
- Central Management System (CMS)

2.2.1.1 Event Aggregation Module

The Event Aggregation Module (EAM) gathers data from various third-party sensors, then normalizes, filters, batches and transmits that data to the Central Management System (CMS). The EAM provides the following functions:

- Interface to third-party Sensors
- Optional Filtering of Event Data
- Formatting Event Data into TSOM normalized format

- Secure transmission of the Event Data to the Central Management System

The EAM collects Security Event Data from third-party sensors such as Firewalls, Intrusion Detection Systems and Servers etc. For those devices that support standards based interfaces such as SNMP, SYSLOG and XML, TSOM uses device specific rules to interpret the data. For some devices, such as Checkpoint FW1, TSOM has developed an interface to their proprietary interfaces. Some devices do not support any appropriate mechanism to get the security event data from the device to the EAM; in these situations TSOM deploys the UCM on the sensor that extracts the data locally on the device and then sends the data to the EAM over a secure interface.

The EAM can optionally filter out non-essential event data so that this data will not be sent to the CMS. Once the EAM has formatted event data, it transmits this data to CMS over a secure encrypted connection for correlation and permanent storage.

2.2.1.2 Universal Collection Module

The Universal Collection Module (UCM) is a platform agnostic data collection device. The UCM is used to gather data from security devices that reside on platforms that cannot support an EAM. The UCM can be deployed on any platform in the IT environment as long as the UCM will have access to the data required. For example, the UCM might connect via JDBC to a database to query for updates. This situation is satisfactory as long as the platform the UCM has been deployed on has network access to both the database in question and the EAM. The UCM can also be configured to monitor a Windows event log or a directory used to store files containing event data. The UCM transfers the data gathered from the device to the EAM utilizing a proprietary XML format to communicate events to the EAM. This proprietary XML interface is solely used by the TOE to transport raw events from the UCM to the EAM.

2.2.1.3 Central Management System

The Central Management System (CMS) brings together event data streams from all of the EAMs deployed in a network. The CMS correlates the event data and a threat analysis is performed. The CMS caches a running subset of the correlated event data for real-time display, while directing the correlated event data-stream to the archiver (ie. database) for persistent storage. Both the real-time and persistent data is used in presenting relevant information through the user interface and advanced analytics module.

- **Event Correlation and Threat Determination**

  Event correlation and threat determination involve a combination of embedded logic and configurable rules to correlate events while determining the threat level of each event.

  The embedded logic performs many of the routine tasks currently performed by security analysts; sorting and determining the relationship between events; assigning a weighted threat value to each event; and associating each event to source and destination hosts.

  The configurable rules provide a concurrent approach to threat determination. By applying stateless and stateful rules, the CMS screens the event stream against configurable enterprise-level attack signatures, and triggers actions based on these signatures.

- **Event Caching and Archiving**

  Once correlation and threat determination has been completed, the CMS caches a copy of the correlated event for real-time viewing. The event-stream is also directed to the Event archiver for persistent storage in the underlying audit and event database which is in the IT environment of the TOE. Event queries and reporting using analytical tools provided by the CMS are conducted from the events within this database.

  The Correlation process performs the following actions upon data in the event cache.

  - Dropping non essential events, user definable
  - Atomic threat level calculations based upon the source and destination addresses of the event
  - Business Rule processing of events (stateless and stateful analysis)

- Storage of the correlated events into the event ready cache

- **User Interface**

  The User Interface is a set of modules that access and update various in-memory and database tables for the presentation and maintenance of data within the system. Key components of the User Interface are.

  - Event Console (Real Time Viewer),
  - Power Grid
  - Threat Displays,
  - Event Searching,
  - Host and Network queries,
  - Ticketing System, and
  - System Administration.

The TOE comes pre-configured to accept security event data from numerous security devices. Devices using SYSLOG, SNMP, XML as well as enhanced support for Check Point, ISS, and Cisco devices are easily connected to the TOE without requiring software agents. This approach simplifies deployment and eliminates the problems of updating and configuring remote agents while also eliminating the additional system load that agent-based technologies incur.

The two primary subsystems are the EAM and the CMS. There can only be one CMS, however, there can be many EAMs. The CMS and EAM's are distributed on separate machines. The User Interface is a rich Java-based client which is launched via a web browser such as IE 6.0 or higher. The Event Console (Real Time Viewer) runs as a Java application, which automatically downloads when activated if the Java Runtime Environment (JRE) is running on the desktop. The Power Grid interface provides a comprehensive view of audit and event data and allows the user to analyze and detect patterns in the data.

The major components of the TOE are identified in the following figure:

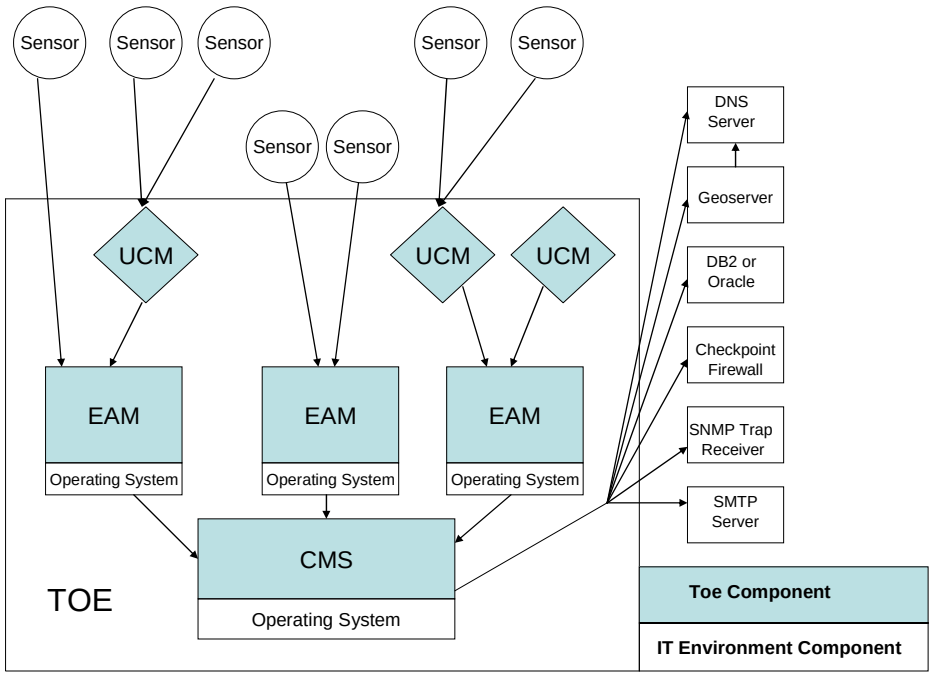

Figure 1: Tivoli Security Operations Manager System Architecture

2.2.2 Physical Boundary

The TOE is a software product that operates in a Linux/Unix or Windows environment. The operating environment includes the hardware platform, Windows Server 2003, Redhat Enterprise Server, Solaris, or AIX operating systems, the database platform which can consist of DB2 or Oracle, the sensors, the browser (Internet Explorer v6 or later or Mozilla v1.3 or later) and the Java Runtime Environment (JRE) for access to installing the User Interface. The TOE is also dependent upon the use of a GeoServer and trusted DNS servers in the IT environment for its geoserver feature and upon SMTP and SNMP servers for aspects of its IDS functionality. The operating environment is not part of the TOE.

All components (with the exception of the OPSEC interface (c++), and the event parsers (perl)) are written in Java so as to be operable on as many platforms as possible. The UI which is used to access the CMS is a Java based rich-client. The client requires Java 5 JRE and a browser which is used to download the Java client. As noted above, both the JRE and the browser are part of the IT environment of the TOE. The browser is only used to launch the TSOM UI and has no other purpose other than for viewing the reports portal. Therefore, the UI itself is not a web based interface.

Each of the components (UI, CMS, EAM) are run on different machines. The EAM and CMS leverage the same communications ports by default (2468) and although these can be changed, the EAM and CMS should be installed on separate machines for performance and configuration reasons.

The CMS and EAM are to be installed on any of the following Operating Systems:

- RedHat Linux ES 5.0
- AIX 5L Version 5.31[1]

[1]It should be noted that when the CMS and the EAM are running on an IBM AIX server, neither firewall blocking nor the Check Point conduit are supported as Check Point does not currently provide OPSEC binaries for the IBM AIX platform.

- Sun Solaris 10 (SPARC)
- Microsoft Windows 2003 R2 Enterprise Edition (64-bit)

Each Sensor that reports to an EAM is located in the IT Environment. Sensors in the IT environment must be products that are supported by the TOE, in that the TOE must have the parsing logic necessary to read a given sensor's log file format. Sensors supported by the TOE will be able to communicate with the TOE via information flows to the EAM in one of the following ways:

- Syslog
- SNMP Traps
- Checkpoint OPSEC
- Cisco SDEE
- UCM Based XML

The TOE relies upon a Geoserver and trusted DNS Servers in the IT environment for implementing its geoserver functionality which provides geographical information used for locating netblocks and hosts on Map views. IBM maintains its own Geoserver which only communicates with the geoclient embedded in the TSOM TOE application. This Geoserver is part of the IT environment of the TOE and is accessed via a connection from the CMS to geoloc.ibm.com using a proprietary XML based protocol. The TOE is also dependent upon the use of trusted DNS servers in the IT environment for resolving email addresses.

2.2.2.1 Features not included in the evaluated configuration

- LDAP is an alternate method of remote authentication that is not included in the TOE. Enabling remote authentication will make any password policies set by the TOE unenforceable, since the password policy will be governed by the remote authentication server. By default, the remote authentication capability is disabled and will remain disabled in the evaluated configuration. This capability is not enabled in the TOE.
- The Host Investigative (HIT) Tools is a toolkit which includes SNMP Get, TCP Port Scan, HTTP Probe, Traceroute, UDP Port Scan and TCPDUMP among others. The HIT toolkit is an optional component that is not included with the TOE.
- The Change Control Management database (CCMDB) is an optional component that can be configured and then be used to store configuration information about hosts. The CCMDB is not within the scope of this evaluation and is not enabled in the TOE.
- The Vulnerability Import utility is a command line utility used to import vulnerability data from a vulnerability scanner. Neither this utility nor vulnerability scanners in the IT environment are within the scope of this evaluation.
- Compound threat calculation is calculated using the average of atomic threats and the threat level generated by a host for two time periods. Compound threat calculation is not within the scope of this evaluation and while the TOE generates data from this type of analysis, this data was not subject to evaluation.

2.2.3 Logical Boundary

Each of the security function descriptions is organized by the security requirements corresponding to the security function. This serves to both summarize the security functions and rationalize that the security functions are suitable to satisfy the associated requirements.

2.2.3.1 Audit Function

The TOE generates audit records which track the actions of authorized TOE users. The audit records are stored and protected in the underlying database in the IT environment of the TOE.[2] The IT environment also provides the timestamp for the audit records. Audit information may be accessed through the Event Console or the PowerGrid interface. Access to audit information is restricted to authorized administrators.

2.2.3.2 Identification and Authentication

User identification and authentication is required to access the user interface of the TOE. The user is always prompted for user name and password credentials before accessing the system. User account information is stored and protected by the database in the IT environment of the TOE. The TOE generates an MD5 hash of the user password. This hash is stored as part of the user account information in the IT environment. The user login process performs authentication as well as providing system privileges that are defined on a per-user or per-role basis. The User Interface is a Java based rich client which his launched via a browser such as Internet Explorer 6.0 or greater.

By default the Account Lockout feature is disabled. In the evaluated configuration, this feature must be enabled by checking "Enable Account Lockout". Once account lockout is enabled, the default number of authentication attempts and the default lockout time period will apply unless configured otherwise by the administrator.

2.2.3.3 User Data Protection

The TOE enforces an access control policy which defines the classes of objects that an authorized user of the TOE will have permission to manage and configure. These classes of objects includes security domains, rules that can be defined within the TOE, hosts, networks, events, tickets, and firewall rules.

2.2.3.4 Security Management

The TOE is designed to provide threat management for security incidents, which require handling many-to-one relationships. The Central Management System (CMS) in turn correlates the data, determines the threat and presents the relevant information to the authorized user through either the Event Console or the PowerGrid interface. The TOE provides the user interface utilized by the authorized administrator to manage the security and network event data collection functions and attributes.

2.2.3.5 Protection of TSF

The TOE ensures that TSF data is protected from disclosure and modification when it is transmitted between TOE components. The TOE invokes a FIPS validated module within the TOE boundary to encrypt communications between distributed parts of the TOE (UI, CMS, UCM and EAM). This module, the IBM JSSE FIPS 140-2 Cryptographic Module (Certificate#409), supports the SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA cipher suite. The TOE also ensures that all TSF data is made available to distributed parts of the TOE.

The IT environment of the TOE provides various mechanisms to ensure that the access control policy is always enforced and the data transmitted between TOE components is protected. The IT environment, specifically the underlying Operating System (OS) supports the non-bypassability of the TSP by protecting itself and the TOE from external interference and tampering. The OS maintains a security domain for its own execution and enforces the separation between the security domains of subjects in the TSC.[3]

---

[2] The Errata [4] in the IDS Analyzer PP (referenced in Section 1.2) permits software TOEs to move the FAU_STG.2 requirement to the IT environment. In these cases, the PP also mandates that OE.AUDIT_PROTECTION be added to the ST which has been done. This environment objective requires that the environment protect the audit information.

[3] The Errata [3] in the IDS Analyzer PP (referenced in Section 1.2) permits software TOEs to move the FPT_RVM requirement to the IT environment. In any case, the FPT_RVM requirement is redundant with the FDP requirements regarding access control which are claimed in this ST and enforced by the TOE.

2.2.3.6 IDS Function

The TOE provides the functions for collecting, analyzing, review and response to the events that occur at the network sensors. Some of the responses available include interfacing with other elements of the IT Environment, such as sending SNMP Traps to a Trap receiver located in the IT Environment, or emails to an SMTP server located in the IT Environment.

The TOE has the ability to acquire GPS coordinates for hosts and networks seen in the events which flow through the CMS. This is accomplished through a connection from the CMS to an IBM maintained server in the IT environment of the TOE.

3 TOE Security Environment

3.1 Threats to Security

3.1.1 Threats addressed by the TOE

The following are threats identified for the TOE and the IT System that the TOE monitors. The TOE and the IT environment are responsible for mitigating the threats. The assumed level of expertise of the attacker for all the threats is unsophisticated.

T.COMDIS	An unauthorized person may attempt to disclose the data analyzed and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.IMPCON	The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential intrusions to go undetected.
T.LOSSOF	An unauthorized person may attempt to remove or destroy data analyzed and produced by the TOE.
T.NOHALT	An unauthorized person may attempt to compromise the continuity of the TOE's analysis functionality by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

3.2 Secure Usage Assumptions

This section describes the security aspects of the environment in which the TOE will be utilized. This includes information about the physical, personnel, and logical aspects of the environment.

3.2.1 Physical Assumptions

A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

3.2.2 Personnel Assumptions

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.

3.2.3 Intended Usage Assumptions

A.ACCESS	The TOE has access to all the trusted IT System resources necessary to perform its functions and these resources are set up in such a manner that the TOE can perform its functions securely.

3.3 Organizational Security Polices

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs.

P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.ACCESS	The data analyzed and generated by the TOE shall only be used for authorized purposes.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to network data and appropriate response actions taken.
P.AVAILABLE	The TOE shall make available the data that is transmitted between TOE components.
P.INTGTY	Data analyzed and generated by the TOE shall be protected from modification.
P.MANAGE	The TOE shall only be managed by authorized users.
P. PROTCT	The TOE shall be protected from unauthorized accesses of analysis and response activities.
P.TRANSPRT	The TOE shall protect the data transmitted between the TOE components

4 Security Objectives

This section defines the security objectives for the TOE and its supporting environment. Security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to counter identified threats, address assumptions, and/or comply with any organizational security policies identified.

4.1 Security Objectives of the TOE

The following security objectives are intended to be satisfied by the TOE.

O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the Analyzer functions.
O.AVAILABLE	The TOE must ensure the availability of IDS data between TOE components.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDACTS	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.
O.INTEGR	The TOE must ensure the integrity of all audit and Analyzer data.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.EXPORT	The TOE must ensure the confidentiality of the IDS data between TOE components.

4.2 Security Objective of the IT Environment

The following security objective for the IT environment of the TOE must be satisfied in order for the TOE to fulfill its own security objectives.

OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering.
OE.TIME	The IT environment will provide reliable timestamps to the TOE

4.3 Security Objective of the Non - IT Environment

The following are the non-IT security objectives, which are to be satisfied without imposing technical requirements on the TOE. That is, they will be satisfied largely through application of procedural or administrative measures.

OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed,

	managed, and operated in a manner which is consistent with IT security.
OE.INTROP	The TOE is interoperable with the IT Systems that it monitors and other IDS components within its IDS, all of which are carefully configured in order to ensure that the TOE functions are performed securely.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the Analyzer.
OE. PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

5 IT Security Requirements

This section of the ST details the security functional requirements (SFRs) for the TOE and the IT Environment that will support the TOE. The SFRs are a combination of the SFRs drawn from the CC Part 2 and explicitly stated requirements that define functionality not modeled by the CC.

The following table lists the security functional requirements for the TOE and the IT environment.

Security Functional Class	Security Functional Requirements
TOE Requirements	
Security Audit	FAU_GEN.1 Audit data generation
	FAU_SAR.1 Audit review
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
User Data Protection (FDP)	FDP_ACC.1 Subset Access Control
	FDP_ACF.1 Security Attribute-based Access Control
Identification and Authentication (FIA)	FIA_AFL.1 Authentication failure handling
	FIA_ATD.1 User Attribute Definition
	FIA_UAU.1 User authentication before any action
	FIA_UID.1 User identification before any action
Security management (FMT)	FMT_MOF.1 Management of security functions behaviour
	FMT_MSA.1 Management of Security Attributes
	FMT_MTD.1 Management of TSF data
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles
Protection of the TSF (FPT)	FPT_ITT.1 Basic internal TSF data transfer protection
	FPT_ITA_(EXP).1 Basic TSF data availability
IDS Component Requirements (IDS)	IDS_NDC.1 Network Event Data Collection
	IDS_ANL.1 Network Analyzer analysis
	IDS_RCT.1 Analyser React
	IDS_RDR.1 Restricted Data Review
IT Environment Requirements	
Security Audit (FAU)	FAU_STG.2 Guarantees of audit data availability
Protection of the TSF (FPT)	FPT_RVM.1 Non-bypassability of the TSP
	FPT_SEP.1 TSF domain separation
	FPT_STM.1 Reliable time stamps

Table 1: Security Functional Requirements

5.1 TOE Security Functional Requirements

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 Audit data generation

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

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

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

c) **the auditable events identified in Table 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 ST, [**no additional information**].

Component	**Event**
FAU_GEN.1	Start up and shutdown of audit functions
FIA_UAU.1	All use of the authentication mechanism
FIA_UID.1	All use of the user identification mechanism

Table 2: Auditable Events

5.1.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [the authorized administrator] with the capability to read [all audit trail data] from the audit records.

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

5.1.1.3 FAU_SAR.2 Restricted audit review

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

5.1.1.4 FAU_SAR.3(a) Selectable audit review (Sorting)

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

5.1.1.5 FAU_SAR.3(b) Selectable audit review (Searches)

FAU_SAR.3.1 The TSF shall provide the ability to perform [***searches***] of audit data based on [**date and time.**]

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the [**Access Control Security Policy**] on [

subjects: users;

objects: security domain, infrastructure, rules, event classification, tickets, Knowledge Base, Reports, and firewall rules; and,

operations: read, write, execute].

5.1.2.2 FDP_ACF.1 Security Attribute-based Access Control

FDP_ACF.1.1 The TSF shall enforce the [**Access Control Security Policy**] to objects based on the following: [

subject: users

- **Permissions**
- **Group membership**

object:

- **Domain associated with the object**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**the subject is granted the ability to perform an operation on an object if the subject's group membership permits access to the domain associated with the object and if the subject's permissions permit the operation.**]

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the: [**no explicit denial access rules**].

Application Note: *The objects defined in FDP_ACC.1 are actually "classes" of objects. The group membership assigned to a user identifies what security domains the user has access to. The role of the user identifies what permissions that user has to the domain objects (read, write, execute). Therefore, the attributes that the access decision is based upon are those of the user and not the object. This is captured in the FDP_ACF requirement and elaborated upon in Section 6.*

5.1.3 Identification and Authentication (FIA)

5.1.3.1 Authentication failure handling (FIA_AFL.1)

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

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**lock the user account for a period of time that is set by the administrator**].

5.1.3.2 FIA_ATD.1 User attribute definition

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

individual users:

a) **User identity;**

b) **Authentication data;**

c) **Authorisations (permissions);**

d) **[Role and group membership.**].

5.1.3.3 FIA_UAU.1 Timing of authentication

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

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

5.1.3.4 FIA_UID.1 Timing of identification

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

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

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behaviour of the functions **of analysis and reaction** to **authorized administrators and authorised Analyser administrators**.[4]

5.1.4.2 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [**Access Control Security Policy**] to restrict the ability to [**enable, disable**] the security attributes [**permissions**] to [**authorized administrator**].

5.1.4.3 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to query **and add Analyser and audit data, and shall restrict the ability to query and modify all other TOE data** to [**authorized administrators who can perform all functions and authorized Analyzer administrator who can perform all functions except those assigned as Administrator privileges]**.

5.1.4.4 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**manage the access control policy, determine and modify the**

[4] This refinement has been made to identify the roles supported by this TOE in Section 5.1.4.6.

behaviour of the event rule function, query the event data, create, modify, and delete the user account, manage the audit function].

5.1.4.5 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the **following** roles: **authorized administrator, authorized Analyser administrators, and [no other role**].

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

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [***disclosure and modification***] when it is transmitted between separate parts of the TOE.

Application Note: *The TSF uses SSL to achieve the protection of communication paths between separate parts of the TOE. Please refer to Section 6.1.5 for further detail.*

5.1.5.2 FPT_ITA_(EXP).1 Basic TSF data availability

FPT_ITA_(EXP).1.1 The TSF shall ensure the availability of all TSF data transmitted between distributed parts of the TOE under normal TOE operating conditions.

5.1.6 IDS Components Requirements (IDS)

5.1.6.1 IDS_NDC.1 Network Event Data Collection (EXP)

IDS_NDC.1.1 The TSF shall be able to collect network event data from the network Sensors.

IDS_NDC.1.2 The TSF shall collect and record within each event at least the following information: date and time of the event, event type, Sensor identity, protocol, and presumed source and destination IP Addresses and ports.

5.1.6.2 IDS_ANL.1 Analyzer analysis (EXP)

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

[**geographical correlation and atomic threat calculation**].

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

a) Date and time of the result, type of result, identification of data source and
b) [**no other attributes**].

5.1.6.3 IDS_RCT.1 Analyser react (EXP)

IDS_RCT.1.1 The TSF shall send an alarm to [**authorized administrators and authorized Analyzer administrators**] and take [**at least one of the following actions:**

a) **Create ticket;**

b) **Send email;**

c) **Send Trap;**

d) **Generate Meta Event;**

e) **Execute Script**

f) **Perform an OPSEC SAM function on a firewall**] when an intrusion is detected.

5.1.6.4 IDS_RDR.1 Restricted Data Review (EXP)

IDS_RDR.1.1 The TSF shall provide [**authorized administrator and authorized Analyzer administrator**] with the capability to read [**all applicable information**] from the **correlated** Analyser data.

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

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

5.2 IT Environment Security Functional Requirements

5.2.1 Security Audit

5.2.1.1 FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1 The ~~TSF~~ **IT Environment** shall protect the stored audit records **and IDS data** from unauthorised deletion.

FAU_STG.2.2 The ~~TSF~~ **IT Environment** shall be able to detect modifications to the audit records **and IDS data**.

FAU_STG.2.3 The ~~TSF~~ **IT Environment** shall ensure that [**all**] audit records will be maintained when the following conditions occur: [***audit storage exhaustion***]

5.2.2 Protection of the TSF (FPT)

5.2.2.1 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The ~~TSF~~ **IT Environment** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2.2.2 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The ~~TSF~~ **IT Environment** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The ~~TSF~~ **IT Environment** shall enforce separation between the security domains of subjects in the TSC.

5.2.2.3 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for its own use **and for use by the TSF**.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the components included in Evaluation Assurance Level (EAL) 3 as specified in Part 3 of Common Criteria.

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_CAP.3 Authorisation controls
	ACM_SCP.1 TOE CM coverage
Delivery and Operation (ADO)	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1 Informal functional specification
	ADV_HLD.2 Security enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life cycle support (ALC)	ALC_DVS.1 Identification of security measures
Tests (ATE)	ATE_COV.2 Analysis of Coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment (AVA)	AVA_MSU.1 Examination of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Table 3: Assurance Components for EAL3

5.3.1 Configuration management (ACM)

5.3.1.1 Authorisation controls (ACM_CAP.3)

ACM_CAP.3.1d The developer shall provide a reference for the TOE.
ACM_CAP.3.2d The developer shall use a CM system.
ACM_CAP.3.3d The developer shall provide CM documentation.
ACM_CAP.3.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.3.2c The TOE shall be labelled with its reference.
ACM_CAP.3.3c The CM documentation shall include a configuration list and a CM plan.
ACM_CAP.3.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.5c The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.6c The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.
ACM_CAP.3.7c The CM system shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.8c The CM plan shall describe how the CM system is used.
ACM_CAP.3.9c The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.3.10c The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.3.11c The CM system shall provide measures such that only authorised changes are made to the configuration items.
ACM_CAP.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 TOE CM coverage (ACM_SCP.1)

ACM_SCP.1.1d The developer shall provide a list of configuration items for the TOE.
ACM_SCP.1.1c The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.
ACM_SCP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.
ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2c The functional specification shall be internally consistent.
ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4c The functional specification shall completely represent the TSF.
ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1d The developer shall provide the high-level design of the TSF.
ADV_HLD.2.1c The presentation of the high-level design shall be informal.
ADV_HLD.2.2c The high-level design shall be internally consistent.
ADV_HLD.2.3c The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.2.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.2.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.2.6c The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.2.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.2.8c The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.
ADV_HLD.2.9c The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.
ADV_HLD.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.2.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.
ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.
ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.
AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.
AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Life cycle support (ALC)

5.3.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.

ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2c The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

5.3.6 Tests (ATE)

5.3.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.

ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2c The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

ATE_COV.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1d The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1c The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

ATE_DPT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability assessment (AVA)

5.3.7.1 Examination of guidance (AVA_MSU.1)

AVA_MSU.1.1d The developer shall provide guidance documentation.
AVA_MSU.1.1c The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AVA_MSU.1.2c The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.1.3c The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.1.4c The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.1.2e The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.1.3e The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.3.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.7.3 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.

AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6 TOE Summary Specification

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is presented by describing how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the associated requirements.

6.1.1 Audit Function

The TOE tracks and records the actions of authorized TOE users. The TOE generates and stores audit records for the following auditable events:

- Start-up and shutdown of the audit functions
- The actions identified in Table 2: Auditable Events, as reproduced below:

Component	Event
FAU_GEN.1	Start up and shutdown of audit functions
FIA_UAU.1	All use of the authentication mechanism
FIA_UID.1	All use of the user identification mechanism

Each audit record contains, at a minimum, the following information: the subject identity, date/time of when the action occurred, the event type and the outcome of the action. (FAU_GEN.1)

The User Interface (UI) provides the Event Console and the PowerGrid interfaces which both display the audit records in a format understandable to the user and can be used by the authorized administrator to review the audit records. The PowerGrid interface provides the ability for the authorized administrator to read, search and filter the audit records by the date/time and the ability to order the audit records based upon the available displayed attributes. These attributes include the date/time, subject identity and the event type. The PowerGrid interface allows the administrator to order the audit record by moving the display columns. The user is able to reorder the columns so that the audit records will be sorted in accordance to the first column in the display. (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3)

The audit records are stored in the log event table of the database in the IT environment of the TOE. Data partitioning at the database level is used to ensure quick access to the data in the database.

The Audit Function demonstrates the implementation of the following security functional requirements: FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, and FAU_SAR.3.

6.1.2 Identification and Authentication

The TOE requires users to be successfully identified and authenticated before they are granted access to the TOE and any of its functions. TOE users are required to login using their user id and password before they may perform any other action not associated with the collection of network, application, host or other event data. The UI which is used to access the CMS is a JAVA based rich-client. Login occurs via this JAVA client application which is launched via a web browser in the IT environment. There is no other purpose for the browser other than for viewing the reports portal.

The TOE has a password policy that defines the required password length, determines the required character types, prevents password reuse for a specific period of time and sets the password expiration parameters. The TOE requires that passwords meet the following:

- The TOE enforces minimum password lengths of eight (8) characters. Note that the maximum password length is 20 characters.
- Composition can include all upper and lower case alphabetic letters (52);
- At least one special characters (i.e., ~ ! @ # $ % ^ & * ( ) _ + ` - = { } : “ < > ? | [ ] ; ‘ , . / \) or

number (0 1 2 3 4 5 6 7 8 9 0) must be used (42)

- The TOE disallows reuse of the last three (3) passwords.

The TOE has the capability to set password expiration that, when enabled, determines that the period in days that a password may be used before it expires is the default of 90 days. Also, when password expiration is enabled, the TOE will prompt the user for a new password 10 days prior to expiration and will send an expiration reminder to the user.

The TOE detects when an administrator configurable number of unsuccessful user authentication attempts has occurred and will lock out the user account for an administrator specified period. By default, the number of unsuccessful user authentication attempts that will trigger the user lockout period is 3, and the lockout period is for 3 hours. The administrator can configure the number of attempts to be between 1 and 10 and can also specify the user lockout time period (FIA_AFL.1).[5] Upon successful verification of the entered identification and authentication information, the user is given access to the interfaces of the TOE. (FIA_UAU.1, FIA_UID.1)

The TOE defines user account information which is used to identify the user's TOE security role, the user's privileges, unique user name, authentication data (password), user groups and user role which defines the access control permissions (authorizations) (FIA_ATD.1). The user account information is stored in the database in the IT environment of the TOE. The TOE generates an MD5 hash of the user password. This hash is stored as part of the user account information in the IT environment.

The Identification and Authentication function demonstrates the implementation of the following security functional requirements: FIA_ATD.1, FIA_UAU.1, and FIA_UID.1.

6.1.3 User Data Protection

The TOE enforces the Access Control SFP with the association of user roles to user accounts. The user roles define the TOE object classes or categories that the user will have access to and the type of operation (read, write or execute) that they will be able to perform (FDP_ACC.1, FDP_ACF.1). The TOE object classes are as follows:

- Security domain - A hierarchical, logical grouping of devices, networks, hosts and their associated data used to compartmentalize information, and define an individual or group's access. Watch lists, which simply create a label for hosts and networks, can be created within security domains.
- Infrastructure – hosts and networks.
- Rules -- rules evaluate all of the events within a security domain using a user-defined filter and respond to those events by triggering a response or action.
- Event classification – event classes provide the capability of grouping event types by abstracting the common elements of different types of events into a single classification.
- Tickets - used to assign and track work associated with event response and resolution.
- Firewall Rules – firewall configuration rules
- Reports -- provide information regarding the security posture of the enterprise
- Knowledge Base – user defined entries containing articles that can be linked to various objects in the system.

Individual users can access information associated with a security domain based on their group membership. User Groups act as a bridge connecting user accounts with security domains. User Groups allow for the group assignment of users to security domains, which in turn determine the visibility of events

[5] By default the Account Lockout feature is disabled. In the evaluated configuration, this feature must be enabled by checking "Enable Account Lockout". Once account lockout is enabled, the default number of authentication attempts and the default lockout time period will apply unless configured otherwise by the administrator.

collected by the system. Users assigned to a user group have access into any security domain with which that user group is associated.

Roles provide a means of managing the permissions assigned to an individual user or group of users. By assigning a user to a role, the group of permissions granted to the role is inherited by the user. The user's role is used to assign Read, Write and Execute permissions to objects.

- Read – permission to view an object. .
- Write -- permission to create, add or delete an object.
- Execute -- permission to execute a function associated with an object. This permission applies to Reports and Firewall Rules.

By default, with the creation of each user account, the user has no access to any of the TOE objects, until the user account is associated to a user role by the authorized administrator. The user roles are modified by the authorized administrator. (FMT_MSA.1)

The User Data Protection function demonstrates the implementation of the following security functional requirements: FDP_ACC.1, FDP_ACF.1 and FMT_MSA.1.

6.1.4 Security Management

The TOE defines the security roles of authorized administrator and authorized Analyzer administrator. The authorized administrator security role is a default administrative role with the username of 'admin'. The authorized administrator is a member of the Administrator user group and has access to all security management functions of the TOE. This role cannot be deleted or modified and is not subject to Security Domain restrictions. The authorized Analyzer administrator security role may perform all security management functions of the TOE except for those assigned as Administrator privileges including the modifying of users, groups and roles and the ability to perform administrative tasks on the system such as the configuration of EAMs, sensors and event classes.

The TOE provides the authorized administrator with the ability to manage the audit function, manage user accounts (create, modify and delete) and manage the access control policy (enable and disable permissions).Authorized administrators and Analyzer administrators can both query the event data and manage the event rule function, the behavior of the analysis and reaction functions, and the data collected and generated by the TOE. (FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_MSA.1)

The authorized administrators and authorized Analyzer administrators are assigned permissions to the objects managed by the TOE. The access rights are divided into object permissions, action permissions and Host Investigative Toolkit (HIT)[6] permissions. The object permissions permit the right to view, add, change, and/or delete the various objects managed by the TOE. The action permissions permit the ability to run reports, import vulnerability information from the Nessus open-source vulnerability scanner, and the system administration. The HIT permissions permit the administrator the right to use particular tools provided by the TOE.

The Security Management function demonstrates the implementation of the following security functional requirements: FMT_MOF.1, FMT_MTD.1, FMT_MSA.1, FMT_SMF.1, and FMT_SMR.1.

6.1.5 Protection of TSF

The TOE invokes a FIPS validated module to encrypt communications between distributed parts of the TOE (UI, CMS, EAM, and UCM). This module, the IBM JSSE FIPS 140-2 Cryptographic Module (Certificate#409), supports the SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA cipher suite and is used to encrypt TCP/IP communications between the UI and the CMS and between the CMS and the EAM. It is also used to encrypt communications between the UCM and the EAM via an SSL mechanism which uses the SSLContext class. The UCM conduit on the EAM generates a certificate to be used by the UCM to create a connection with the EAM. The UCM conduit will reject an invalid certificate used by the UCM and the UCM will be required to request a new certificate.

[6] As noted in Section 2, the HIT Tools are not included in the TOE.

The EAM Connection Manager (EAM CM) assists in managing the communications and transmission of event data from the EAM to the CMS. Specifically, the EAM CM, reads event data from the event database, performs filtering and batching, responds to messages from the CMS, and transmits event data using the encrypted TCP/IP connection to the EAM Manager on the CMS. The EAM CM assigns the data a unique event id, and then transmits the data via the TCP/IP connection to the CMS. The CMS correlates the event data and caches a running subset of the correlated event data for real time display while directing the correlated event data stream to the event database for persistent storage. The CMS then sends an acknowledgement back to the EAM CM to verify delivery of the events to the CMS. Event data is also protected from modification as the TOE does not make any methods available for users to modify event data. (FPT_ITT.1)

The IT environment of the TOE also provides various mechanisms to ensure that the access control policy is always enforced and the data transmitted between TOE components is protected. The IT environment, specifically the underlying Operating System (OS) supports the non-bypassability of the TSP by protecting itself and the TOE from external interference and tampering. The OS maintains a security domain for its own execution and enforces the separation between the security domains of subjects in the TSC.[7]

The TOE ensures that all TSF data is made available to distributed parts of the TOE under normal TOE operating conditions where there is connectivity between the TOE and its components and the TOE is operating within its specified parameters. The TOE's response time is dependent upon system use as well as the complexity of the user's query. (FPT_ITA_ (EXP).1)

The Protection of the TSF demonstrates the implementation of the following security functional requirement: FPT_ITT.1 and FPT_ITA_ (EXP).1

6.1.6 IDS Function

The EAM and UCM perform the task of collecting the network event data from the various Sensors. The UCM collects the data from the Sensors which resides on platforms that cannot support an EAM and transfers the data collected to the EAM. The EAM normalizes the data into a common event format. The format includes at least the following fields: date and time of the event (from the Sensors as applicable and assigned timestamp from the EAM), the event type, Sensor identity, protocol, IP addresses and ports of the source and destination. (IDS_NDC.1) The EAM filters the network data to exclude false positives and other routine events from the data and batches low priority events.

The EAM transmits the data to the CMS where the data is correlated and analyzed. The CMS performs Deterministic Threat Analysis, calculating the threat posed to the destination by the event, and applies the rules configured in the Stateful Rules Engine to the event stream, allowing the TOE to respond to specific attack signatures and events of interest. Specifically, the TOE performs the following analysis functions:

- Geographical correlation –geographically places hosts associated with the events
- Atomic threat calculation – comprised of the source threat and destination threat values and calculated from configured event type, host and netblock[8] parameters. (IDS_ANL.1)

Event correlation and threat determination involves a programmed logic aiding in the analysis of the event data stream. This programmed logic performs many of the routine tasks currently performed by security analysts; sorting and determining the relationship between events; assigning a weighted threat value to each event; and associating each event to its source and destination hosts.

[7] As noted in Section 2, the Errata [3] in the IDS Analyzer PP (referenced in Section 1.2) permits software TOEs to move the FPT_RVM requirement to the IT environment. In any case, the FPT_RVM requirement is redundant with the FDP requirements regarding access control which are claimed in this ST and enforced by the TOE.

[8] Netblocks are created during initial deployment to support the addition of networks to the system in order to segment the network into smaller networks based on IP address ranges. The netblock definition includes a description of the network, the netblock watchlist membership, a percentage threat weighting assigned to the netblock as a source of events and an asset criticality weighting assigned to the netblock as a target of events.

The CMS provides the ability to configure stateless and stateful rules that can be applied to the data. The configurable rules provide a concurrent approach to threat determination. By applying stateless and stateful rules, the CMS screens the event stream against configurable enterprise-level attack signatures, and triggers responses based on these signatures. The types of responses that can be initiated by a rule are:

- **Create ticket --** generates a ticket with the event information in the ticket and assigns the ticket to the user or group defined in the action.
- **Send email** -- sends an e-mail to the user or group defined in the action. An administrator can configure this functionality to send an email to a configured user or external email address including email-enabled pagers.
- **Send Trap** -- allows the user to define the specific details of the trap to send to pre-configured SNMP receivers.
- **Generate Meta Event --** creates a system event that captures event information defined within the action, allowing for the assignment of the event sequence that triggered the rule to a more descriptive event classification. Examples of meta events are: real-time alerts, sending another event to respond to a group of IDS events and dropping an event when a potential network event is detected.
- **Execute Script** -- executes the defined script when the events triggering the associated rule are detected.
- **Perform an OPSEC SAM function on a firewall --** performs the defined OPSEC SAM function on a firewall defined for Firewall Blocking. (ie, reconfigure a checkpoint firewall). The TOE stores a passphrase to authenticate with the OPSEC SAM firewall and must be configured to identify the firewall, provide connection information, and perform a certificate exchange before communication can occur.

The TOE depends on the functionality provided by SNMP and SMTP servers in the IT environment to send the notifications via email, pager (only if email enabled) and SNMP traps. (IDS_RCT.1)

The TOE has the ability to acquire GPS coordinates for hosts and networks seen in the events which flow through the CMS. The TOE's geographical correlation 'Geoserver' feature allows it to connect to an IBM GeoServer in order to query public allocation registries to determine the ownership and geographic location of a given address range. The IBM Geoserver only communicates with the geoclient embedded in the TSOM TOE application. This Geoserver is part of the IT environment of the TOE and is accessed via a connection from the CMS to *geoloc.ibm.com* using a proprietary XML based protocol. The TOE is also dependent upon the use of trusted DNS servers in the IT environment as part of this process.

The CMS directs the correlated event data-stream to the archiver (ie. database) for persistent storage, while a running subset of the event data is directed to the Event Console for real-time display. The event data can also be viewed using the PowerGrid interface. Both the real-time and persistent data is used in presenting relevant information through the user interface and advanced analytics module. The TOE restricts the ability to read all correlated event data to the authorized administrator and authorized Analyzer administrator. (IDS_RDR.1)

The event data is stored in the log event table of the database in the IT environment of the TOE. Multiple table names are not used as data partitioning at the database level is employed to ensure quick access to the event data. Event data is protected from modification as the TOE does not make any methods available for users to modify event data.

The IDS function demonstrates the implementation of the following security functional requirements: IDS_SDC.1, IDS_ANL.1, IDS_RDR.1, and IDS_RCT.1.

6.2 Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL3 assurance requirements:

- Configuration Management;
- Delivery and Guidance;
- Design Documentation;
- Tests; and
- Vulnerability Assessment.

6.2.1 Configuration Management

The configuration management measures applied by IBM ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. IBM ensures changes to the implementation representation are controlled and that TOE associated configuration item modifications are properly controlled. IBM performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, lifecycle support, vulnerability analysis, delivery and operations and the configuration management documentation. These activities are documented in:

- IBM Tivoli Security Operations Manager Configuration Management Plan

The configuration management documentation satisfies the ACM_CAP.3 and ACM_SCP.1 assurance requirements.

6.2.2 Delivery and Guidance

6.2.2.1 Delivery and Installation

IBM provides documentation that explains how the TOE is delivered, the carriers utilized and the procedures to be able to detect any unauthorized modifications that may be made to the TOE. IBM's installation procedures describe the steps used for the secure installation, generation, and start-up of the TOE along with configuration settings to secure the TOE privileges and functions.

The delivery and installation process is documented in:

- IBM Tivoli Security Operations Manager Delivery and Operation Guide;
- IBM Tivoli Security Operations Manager Installation Guide
- IBM Tivoli Security Operations Manager Common Criteria Guide

The delivery and installation documentation satisfies the assurance requirements: ADO_DEL.1, and ADO_IGS.1.

6.2.2.2 Administrative and User Guidance

IBM provides administrator guidance on how to utilize the TOE security functions, other administrative functions and warnings to authorized administrators about actions that can compromise the security of the TOE. The procedures, included in the administrator guidance, describe the steps necessary to operate the TOE in accordance with the evaluated configuration, detailing how to establish and maintain the secure configuration. The only users of the TOE are authorized system administrators and administrators, thus only administrator guidance is provided.

The administrator guidance is documented in:

- IBM Tivoli Security Operations Manager Common Criteria (CC) Configuration Requirements
- IBM Tivoli Security Operations Manager Administration Guide

- IBM Tivoli Security Operations Manager User Guide

The administrator's guide satisfies the assurance requirements: AGD_ADM.1, and AGD_USR.1.

6.2.3 Development

The design documentation serves to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST).

The development evidence is documented in:

- IBM Tivoli Security Operations Manager Functional Specification
- IBM Tivoli Security Operations Manager High Level Design

The design documentation satisfies the security assurance requirements: ADV_FSP.1, ADV_HLD.2; and, ADV_RCR.1.

6.2.4 Life cycle support

IBM ensures the adequacy of the procedures used during the development and maintenance of the TOE through its life-cycle. IBM includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. .

These activities are documented in:

- IBM Tivoli Security Operations Manager Lifecycle Support

The Life cycle support document satisfies the assurance requirements: ALC_DVS.1.

6.2.5 Tests

The test documentation is found in the following documents:

- IBM Common Criteria Test Plan TSOM 4.1.1
- IBM Tivoli Security Operations Manager Test Spreadsheets

These documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the security functions described in the functional specification and the high-level design are appropriately tested.

The test documentation satisfies the following assurance requirements: ATE_COV.2, ATE_DPT.1, ATE_FUN.1 and, ATE_IND.2.

6.2.6 Vulnerability Assessment

The TOE administrator and user guidance documents describe the operation of TSOM and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references.

IBM performed a vulnerability analysis of the TOE to identify weaknesses that can be exploited in the TOE and a strength of function analysis of the password mechanism. The vulnerability analysis and the strength of function analysis are documented in:

- IBM Tivoli Security Operations Manager Vulnerability Assessment

The vulnerability analysis documentation satisfies the assurance requirements: AVA_MSU.1, AVA_SOF.1; and, AVA_VLA.1.

7 Protection Profile Claim

There are no Protection Profile claims in this Security Target.

8 Rationale

This section provides the rationale for completeness and consistency of this Security Target.

8.1 Security Objectives Rationale

This section provides a rationale for each threat, assumption and organizational security policy. This section includes the table that illustrates the mapping of the threats, assumptions, and policies to the security objectives. The following discussions detail the coverage of each assumption, threat, and organizational policy.

Security Environment	Security Objectives
A.ACCESS	OE.INTROP
A.LOCATE	OE.PHYCAL
A.MANAGE	OE.PERSON
A.NOEVIL	OE.INSTAL OE.PHYCAL OE.CREDEN
A.NOTRST	OE.PHYCAL OE.CREDEN
A.PROTCT	OE.PHYCAL
P.ACCESS	O.IDAUTH O.ACCESS O.PROTCT OE.AUDIT_PROTECTION
P.ACCACT	O.AUDITS O.IDAUTH OE.TIME
P.ANALYZ	O.IDACTS
P.AVAILABLE	O.AVAILABLE
P.INTGTY	O.INTEGR
P.MANAGE	OE.PERSON OE.EADMIN OE.INSTAL O.IDAUTH O.ACCESS OE.CREDEN O.PROTCT
P.PROTCT	OE.PHYCAL OE.PROTECT

P.TRANSPRT	O.EXPORT
T.COMDIS	O.IDAUTH O.ACCESS O.EXPORT O.PROTCT OE.PROTECT
T.COMINT	O.IDAUTH O.ACCESS O.INTEGR O.PROTCT OE.PROTECT
T.FALACT	O.RESPON
T.FALASC	O.IDACTS
T.FALREC	O.IDACTS
T.IMPCON	OE.INSTAL O.EADMIN O.IDAUTH O.ACCESS
T.LOSSOF	O.IDAUTH O.ACCESS O.INTEGR O.PROTCT
T.NOHALT	O.IDAUTH O.ACCESS O.IDACTS
T.PRIVIL	O.IDAUTH O.ACCESS O.PROTCT

Table 4: Security Environment vs. Security Objectives

A.ACCESS *The TOE has access to all the trusted IT System resources necessary to perform its functions and these resources are set up in such a manner that the TOE can perform its functions securely.*

The OE.INTROP objective ensures the TOE has the needed access and that all IT Systems are configured in order for the TOE to perform its functions securely.

A.LOCATE *The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.*

The OE.PHYCAL provides for the physical protection of the TOE.

A.MANAGE *There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.*

The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

A.NOEVIL *The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.*

The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.NOTRST *The TOE can only be accessed by authorized users.*

The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.PROTCT *The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.*

The OE.PHYCAL provides for the physical protection of the TOE hardware and software.

P.ACCESS *The data analyzed and generated by the TOE shall only be used for authorized purposes.*

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective provides for TOE self-protection. The OE.AUDIT_PROTECTION objective provides protection of the audit records from unauthorized deletion and modifications by the IT environment.

P.ACCACT *Users of the TOE shall be accountable for their actions within the IDS.*

The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The OE.PROTECT objective enforces this policy by ensuring the security functions of the TOE are invoked before proceeding and the TOE is protected from tampering.

P.ANALYZ *Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to network data and appropriate response actions taken.*

The O.IDACTS objective requires analytical processes be applied to data collected from Sensors and Scanners.

P.AVAILABLE *The TOE shall make available the data that is transmitted between TOE components.*

The O.AVAILABLE objective ensures the availability of data.

P.INTGTY *Data analyzed and generated by the TOE shall be protected from modification.*

The O.INTEGR objective ensures the protection of data from modification..

P.MANAGE *The TOE shall only be managed by authorized users.*

The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective provides for TOE self-protection.

P. PROTCT *The TOE shall be protected from unauthorized accesses of analysis and response activities.*

The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

P.TRANSPRT *The TOE shall protect the data transmitted between the TOE components*

The O.EXPORT objective ensures that confidentiality of TOE data will be maintained during transmission between TOE components.

T.COMDIS *An unauthorized person may attempt to disclose the data analyzed and produced by the TOE by bypassing a security mechanism.*

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.EXPORT objective ensures that confidentiality of TOE data will be maintained. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective addresses this threat by ensuring that the underlying OS protects the TOE from external interference and tampering.

T.COMINT *An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.*

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective addresses this threat by ensuring that the underlying OS protects the TOE from external interference and tampering.

T.FALACT *The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.*

The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

T.FALASC *The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.*

The O.IDACTS objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

T.FALREC *The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.*

The O.IDACTS objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.

T.IMPCON *The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential intrusions to go undetected.*

The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.

T.LOSSOF *An unauthorized person may attempt to remove or destroy data analyzed and produced by the TOE.*

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.NOHALT *An unauthorized person may attempt to compromise the continuity of the TOE's analysis functionality by halting execution of the TOE.*

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDACTS objective addresses this threat by requiring the TOE to collect all events, including those attempts to halt the TOE.

T.PRIVIL *An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.*

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.

8.2 Security Requirements Rationale

This section demonstrates that the security requirements selected provides complete coverage for the security objectives defined in this Security Target. The mapping of the requirements to the security objectives is illustrated in the table below:

	O.ACCESS	O.AUDITS	O.AVAILABLE	O.EADMIN	O.IDAUTH	O.IDACTS	O.INTEGR	O.PROTCT	O.RESPON	O.EXPORT	OE.AUDIT_PROTECTION	OE.PROTECT	OE.TIME
FAU_GEN.1		X											
FAU_SAR.1		X		X									
FAU_SAR.2	X	X			X								
FAU_SAR.3		X		X									
FDP_ACC.1	X							X					
FDP_ACF.1	X							X					
FIA_AFL.1	X							X					
FIA_ATD.1					X								
FIA_UAU.1	X				X			X					
FIA_UID.1	X				X			X					
FMT_MOF.1	X			X				X					
FMT_MSA.1	X			X									
FMT_MTD.1	X			X			X	X					
FMT_SMF.1				X									
FMT_SMR.1					X								
FPT_ITA_(EXP).1			X										

	O.ACCESS	O.AUDITS	O.AVAILABLE	O.EADMIN	O.IDAUTH	O.IDACTS	O.INTEGR	O.PROTCT	O.RESPON	O.EXPORT	OE.AUDIT_PROTECTION	OE.PROTECT	OE.TIME
FPT_ITT.1										X			
FPT_RVM.1												X	
FPT_STM.1													X
FPT_SEP.1												X	
IDS_SDC.1						X							
IDS_ANL.1						X							
IDS_RDR.1	X			X	X								
IDS_RCT.1									X				

Table 5: Security Functional Requirements vs. Security Objectives

O.ACCESS *The TOE must allow authorized users to access only appropriate TOE functions and data.*

The TOE must restrict access to the TOE objects by the permission associated to the authorized users [FDP_ACC.1, FDP_ACF.1]. The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The Analyzer is required to restrict the review of Analyzer data to those granted with explicit read access [IDS_RDR.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE detects when an administrator configurable number of failed authentication attempts occurs and will lock out the user account [FIA_AFL.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the Analyzer may query and add Analyzer and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1], and enable and disable the permissions associated with the access control policy [FMT_MSA.1].

O.EADMIN *The TOE must include a set of functions that allow effective management of its functions and data.*

The TOE must provide the ability to review and manage the audit trail of an Analyzer [FAU_SAR.1, FAU_SAR.3]. The Analyzer must provide the ability for authorized administrators to view the Analyzer data [IDS_RDR.1].

The TOE must provide the interfaces to manage the TOE and its data [FMT_SMF.1]. The Analyzer must provide the ability to determine and modify the behavior of the rule function, [FMT_MOF.1], the enable and disable permission associated with the access control policy, [FMT_MSA.1], and the ability to manage TOE data to the authorized administrator and/or authorized Analyzer administrator [FMT_MTD.1]. The TOE must provide the ability for

authorized administrators to view the correlated Analyser data [IDS_RDR.1].

O.AUDITS *The TOE must record audit records for data accesses and use of the Analyzer functions.*

Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the ability for the authorized administrator to review the audit records [FAU_SAR.1, FAU_SAR.2, FAU_SAR.3].

O.AVAILABLE *The TOE must ensure the availability of IDS data between TOE components.*

Under normal operating conditions where there is connectivity between the TOE and its components, and the TOE is operating within specified parameters, the TOE ensures that data is made available to distributed parts of the TOE (FPT_ITA.1)

O.IDACTS *The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).*

The TOE collects the network event data from the Sensors on the IT System [IDS_SDC.1]. The Analyser is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].

O.IDAUTH *The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.*

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The Analyzer is required to restrict the review of collected Analyzer data to those granted with explicit read-access [IDS_RDR.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the Analyzer may query and add Analyzer and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1].

O.INTEGR *The TOE must ensure the integrity of all audit and Analyzer data.*

Only authorized administrators of the Analyzer may query or add audit and Analyzer data [FMT_MTD.1]. The Analyzer must protect the collected data from disclosure and modification to ensure its integrity when the data is transmitted to TOE components [FPT_ITT.1].

O.PROTCT *The TOE must protect itself from unauthorized modifications and access to its functions and data.*

The TOE must restrict access to the TOE objects by the permission associated to

the authorized users [FDP_ACC.1, FDP_ACF.1]. Security attributes of subjects use to enforce the authentication policy and the access control policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE detects when an administrator configurable number of failed authentication attempts occurs and will lock out the user account [FIA_AFL.1].

The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the Analyzer may query and add Analyzer and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1].

O.RESPON *The TOE must respond appropriately to network event data and analytical conclusions.*

The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1]

O.EXPORT *The TOE must ensure the confidentiality of the IDS data between TOE components.*

The TOE must protect the IDS data from disclosure and modification in order to ensure its integrity when the data is transmitted between TOE components. [FPT_ITT.1].

OE.AUDIT_ PROTECTION *The IT Environment will provide the capability to protect audit information.*

The IT environment must protect the audit records and IDS data from unauthorized deletion.[FAU_STG.2].

OE.PROTECT *The IT environment will protect itself and the TOE from external interference or tampering.*

The underlying OS must protect the TOE from interference that would prevent it from performing its functions [FPT_SEP.1, FPT_RVM.1]

OE.TIME *The IT environment will provide reliable timestamps to the TOE.*

The underlying OS must provide the reliable time stamp to associate with an audit record, network event data, and the Analyzer data. [FPT_STM.1].

8.2.1 Explicitly Stated Requirements Rationale

A family of IDS requirements was created to specifically address the data collected and analyzed by the TOE. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of the network data and provide for requirements about collecting, reviewing and managing the data.

In response to PD-0127, the FPT_ITA_(EXP).1 requirement was added to address the availability of TOE data.

All of the explicitly stated requirements are self-contained and do not introduce any new dependencies.

8.2.2 Security Functional Requirement Dependency Rationale

This section demonstrates the dependencies of the TOE security functional requirements. The table maps the TOE security functional requirements to the security functional requirements they depend upon, illustrating that TOE security functional requirement dependencies are met within the ST.

Note: The table assumes that requirement iteration have the same dependencies, thus the iterations are not individually identified in the table (e.g FMT_MTD.1(a)).

Dependency / Requirements	FAU_GEN.1	FAU_SAR.1	FDP_ACC.1	FDP_ACF.1	FIA_UAU.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FAU_GEN.1												X
FAU_SAR.1	X											
FAU_SAR.2		X										
FAU_SAR.3		X										
FDP_ACC.1				X								
FDP_ACF.1 (**see note below**)			X					X				
FIA_AFL.1					X							
FIA_UAU.1						X						
FMT_MOF.1										X	X	
FMT_MSA.1			X							X	X	
FMT_MTD.1										X	X	
FMT_SMR.1						X						

Table 5: Security Functional Requirements Dependencies

Note: The TOE does not provide default values for security attributes used to enforce the SFP, therefore FMT_MSA.3 has not been included as a security requirement in this ST and the dependency that FDP_ACF.1 has on FMT_MSA.3 is considered satisfied.

8.2.3 Security Assurance Requirements Rationale

EAL3 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL3, the TOE will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

8.3 TOE Summary Specification Rationale

This section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions and security assurance measures are suitable to meet the TOE security requirements. The collection of security functions work together to implement the security requirements. The security

functions described in the TOE summary specification and indicated in Table 6: Security Functional Requirements vs. Security Functions are all necessary for the required functionalities in the TSF.

Table 7: Security Assurance Requirements vs. Assurance Measures provides a mapping of TOE security assurance functions to those security assurance measures that have been implemented by the developer to ensure that the TOE meets the requirements specified by CC EAL3.

	AUDIT FUNCTION	USER DATA PROTECTION	IDENTIFICATION AND AUTHENTICATON	SECURITY MANAGEMENT	PROTECTION OF THE TSF	TOE ACCESS	IDS FUNCTION
FAU_GEN.1	X						
FAU_SAR.1	X						
FAU_SAR.2	X						
FAU_SAR.3	X						
FDP_ACC.1		X					
FDP_ACF.1		X					
FIA_AFL.1			X				
FIA_ATD.1			X				
FIA_UAU.1			X				
FIA_UID.1			X				
FMT_MOF.1				X			
FMT_MSA.1		X					
FMT_MTD.1				X			
FMT_SMF.1				X			
FMT_SMR.1				X			
FPT_ITA_(EXP).1					X		
FPT_ITT.1					X		
IDS_NDC.1							X
IDS_ANL.1							X
IDS_RDR.1							X
IDS_RCT.1							X

Table 6: Security Functional Requirements vs. Security Functions

	CONFIGURATION MANAGEMENT	DELIVERY AND GUIDANCE	DEVELOPMENT	TESTS	VULNERABILITY ASSESSMENT
ACM_CAP.3	X				
ACM_SCP.1	X				
ADO_DEL.1		X			
ADO_IGS.1		X			
ADV_FSP.1			X		
ADV_HLD.2			X		
ADV_RCR.1			X		
AGD_ADM.1		X			
AGD_USR.1		X			
ATE_COV.2				X	
ATE_DPT.1					
ATE_FUN.1				X	
ATE_IND.2				X	
AVA_MSU.1					**X**
AVA_SOF.1					X
AVA_VLA.1					X

Table 7: Security Assurance Requirements vs. Assurance Measures

8.4 Strength of Function Rationale

A strength of function rating of SOF-basic was designated for this TOE. The rationale for the chosen level is based on the low attack potential of the threat agents identified in this ST. The TOE includes a password mechanism used to login the users of the TOE. The strength of function of SOF-basic is associated to this mechanism. The password mechanism is enforced with the security function, Identification and Authentication, and implements FIA_UAU.1.

8.5 Internal Consistency and Support

The selected functional requirements for the TOE and IT Environment are internally consistent. All the operations performed are in accordance with the CC. The ST does not include any instances of a requirement that conflicts with or contradicts another requirement. In instances where multiple requirements apply to the same functions, the requirements and their operations do not cause a conflict between each other.

The selected requirements are mutually supportive by supporting the dependencies listed in Section 5. Section 8.2 justifies the lack of any dependency, provides the rationale for the suitability of the requirements to meet the objectives; and for the inclusion of architectural IT environment requirements, FPT_RVM.1 and FPT_SEP.1, to protect the TOE. It also provides the rationale for the inclusion of

management requirements to provide a means to properly configure and manage the other security requirements.
