Tenable Network Security, Inc.
Tenable Security Center 3.2 and Components

Security Target
Version 1.0

January 15, 2010

Prepared for:
Tenable Network Security, Inc.

7063 Columbia Gateway Drive, Suite 100
Columbia, MD 21046

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization.

The Target of Evaluation (TOE) is the Tenable Security Center 3.2 and Components. It consists of the Tenable Security Center 3.2 (SC3); 3D Tool 1.2 (3DT); Log Correlation Engine 2.0.2. (LCE); Passive Vulnerability Scanner 3.0 (PVS); Nessus Scanner 3.0.4. (Nessus). The TOE consists of five (5) distinct products and the evaluated configuration includes all of the Tenable products working together. Tenable's product suite provides an integrated environment for managing security events and vulnerabilities where all products tie together; the scanning products are updated with new and modified plugins as appropriate for the individual application; and, integrate with other third party products that are not part of this evaluation. The TOE facilitates administration and organization of security workflow and management that includes reporting automatic notices for affected parties; division of duties; separate access to data; and, update and tracking of vulnerability closure.

The Security Target contains the following sections:

Section 1 **Security Target Introduction**
This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization.

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 expectations of the environment, the threats that are countered by TOE and IT environment, and the organizational policy that TOE must fulfill.

Section 4 **TOE Security Objectives**
This section details the security objectives of the TOE 4.3 and IT environment.

Section 5 **IT Security Requirements**
The section presents the security functional requirements (SFR) for TOE and IT Environment that supports the TOE, and details the assurance requirements for EAL2.

Section 6 **TOE Summary Specification**
The section describes the security functions represented in the TOE that satisfy the security requirements.

Section 7 **Protection Profile Clai**ms
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.

1.1 Security Target, TOE and CC Identification

ST Title – Tenable Network Security, Inc. Tenable Security Center 3.2 and Components Security Target

ST Version – Version 1.0

ST Date – January 15, 2010

TOE Identification – Tenable Security Center 3.2 and Components. The TOE consists of: Tenable Security Center 3.2 plus Components 3D Tool 1.2 (3DT); Log Correlation Engine 2.0.2 (LCE); Passive Vulnerability Scanner 3.0 (PVS); and Nessus Scanner 3.0.4 (Nessus).

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

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
    - Part 3 Conformant
    - Assurance Level: EAL2 augmented with ALC_FLR.3 and AVA_MSU.1.
- This TOE is conformant to the following Protection Profile (PP):
    - Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006 (IDSSYPP)

1.3 Conventions and Acronyms

This section specifies the formatting conventions used in the Security Target and provides a glossary of acronyms.

1.3.1 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, a letter placed at the end of the component indicates iteration. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by bold brackets (e.g., [**assignment**]). However, the text is not bolded when a CC assignment was completed by a Protection Profile from which the SFR was drawn as part of a conformance claim, so that no assignment was exercised in writing the ST.
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by bold brackets (e.g., [***selection***]). An assignment inside a selection is indicated using bold italics surrounded by bold italics brackets surrounded by bold brackets (e.g., [***[selection]***]). However, the text is not bolded when a CC selection was completed by a Protection Profile from which the SFR was drawn as part of a conformance claim, so that no selection was exercised in writing the ST.
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Explicitly stated Security Functional Requirements (i.e., those not found in Part 2 of the CC) are identified with "**(EXP)**".
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Acronyms

3DT	3D Tool
CC	Common Criteria

CCTL	CC Testing Laboratory
CI	Configuration Item
CLI	Command Line Interface
CM	Configuration Management
CMP	Configuration Management Plan
CVE	Common Vulnerabilities and Exposures
CVS	Concurrent Versioning System
DHCP	Dynamic Host Configuration Protocol
DoD	Department of Defense
DoS	Denial of Service
EAL	Evaluation Assurance Level
EU	End User (a TOE role)
EXP	Explicitly stated SFR
FQDN	Fully Qualified Domain Name
FSP	Functional Specification
GUI	Graphical User Interface
HLD	High-level Design
HTTP	Hyper-text Transfer Protocol
ID	Identity/Identification
IDS	Intrusion Detection System
IDSSYPP	IDS System PP, Version 1.6, April 4, 2006.
IP	Internet Protocol
IT	Information Technology
ITT	Internal TOE TSF Data Transfer family of FPT
LCE	Log Correlation Engine
NASL	Nessus Attack Scripting Language
NIAP	National Information Assurance Partnership
NIDS	Network IDS
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
PKI	Public Key Infrastructure
PP	Protection Profile
PSM	Primary Security Manager (a TOE role)
PVS	Passive Vulnerability Scanner 2.2
SA	System Administrator (a TOE environment role)
SAIC	Science Applications International Corporation
SAR	Security Assurance Requirement
SC3	Security Center 3.0
SCA	Security Center Administrator (a TOE role)
SFR	Security Functional Requirement
SM	Security Manager (a TOE role)
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TASL	Tenable Application Scripting Language
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
US	United States
XML	Extensible Markup Language

2. TOE Description

The Target of Evaluation (TOE) is Tenable Security Center 3.2 (SC3) and Components: 3D Tool 1.2 (3DT); Log Correlation Engine 2.0.2 (LCE); Passive Vulnerability Scanner 3.0 (PVS); and, Nessus Scanner 3.0.4 (Nessus). The TOE consists of only these five Tenable products, as shown in the Figure 1. The configuration of the TOE subject to evaluation consists of a single SC3 and at least one instance each of the Nessus, PVS, LCE, and 3DT products. Support for other intrusion detection system (IDS) products (e.g., scanners) is provided by the product but is not part of the evaluated configuration (i.e., their security functions were not evaluated).

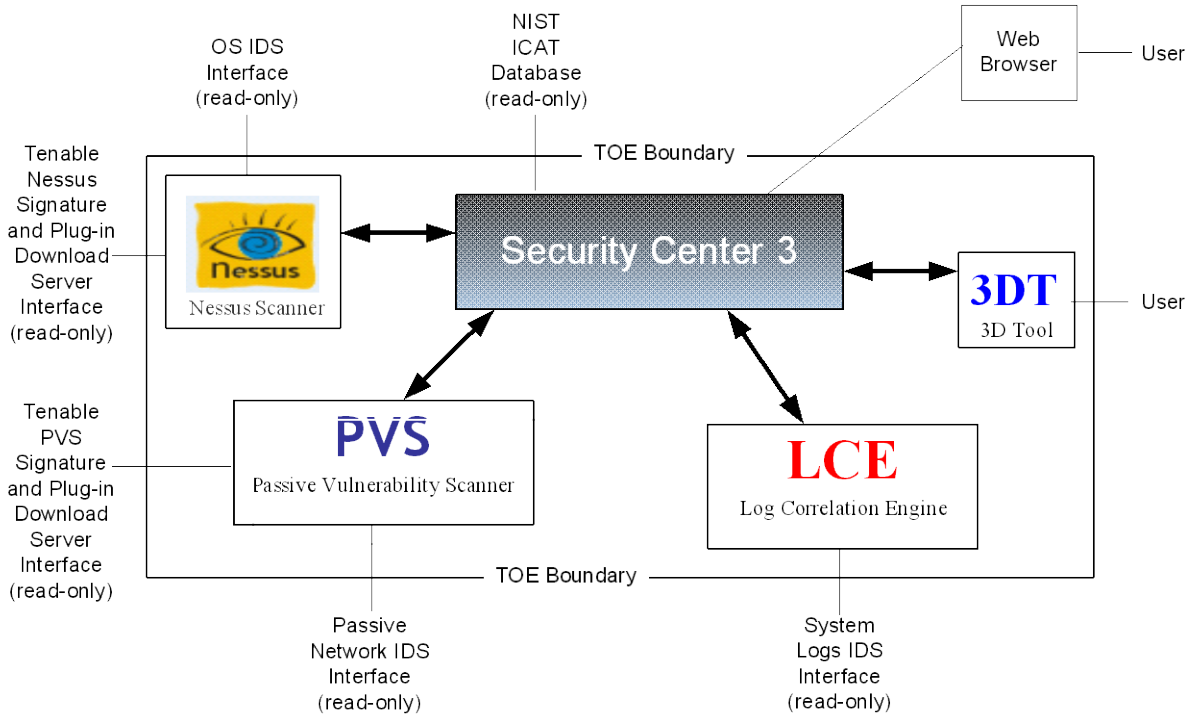

Figure 1 – The Tenable products comprising the TOE.

Figure 1 shows the external interfaces to the TOE. The TOE initiates all except the user interfaces. None are used to provide IDS information to external IT entities. The external interfaces are:

OS IDS Interface – Interface to monitored operating systems to collect IDS information.

Passive Network IDS Interface – Interface to monitored networks to collect IDS information.

System Logs (SYSLOG Server) IDS Interface – Interface to monitored servers to collect IDS information. The interface uses the SYSLOG protocol to accept events from other components of the TOE.

Tenable Nessus Signature and Plug-in Download Server – Interface to Tenable Nessus server to download signatures and NASL plug-ins that allow Nessus to detect the latest known attacks and vulnerabilities against operating systems. The downloaded signatures and plug-ins are configuration data that keep the product current with known vulnerabilities. They update the signatures and plug-ins that are shipped with the TOE.

Tenable PVS Signature and Plug-in Download Server – Interface to Tenable PVS server to download signatures and TASL plug-ins that allow PVS to detect the latest known attacks and vulnerabilities from its network perspective. The downloaded signatures and plug-ins are configuration data that keep the product current with known vulnerabilities. They update the signatures and plug-ins that are shipped with the TOE.

NIST ICAT Database – Descriptions of vulnerabilities from NIST's ICAT (now the National Vulnerability Database) are added to SC3's vulnerability descriptions when presented to users.

3DT User Interface – User interface to SC3 using 3DT for an enhanced view of the IDS scan results.

Web Browser User Interface – User interface to SC3 using a standard web browser with an SSL connection.

Note that while in theory the Nessus, PVS, and LCE components include interfaces intended for use of the component independent of the other components, it is assumed that those components will be configured and used in a manner where those interfaces would not be used. Rather, the SC3 would be used (sometimes via the 3DT component) to integrate and centralize those component capabilities.

The TOE provides administrators with tools to facilitate network security by providing the following services:

- Vulnerability discovery and management,
- Security event management and incident response,
- Measuring and demonstrating configuration management, and
- Dynamic and static asset discovery.

The TOE provides an integrated environment for managing security events and vulnerabilities. The Nessus, PVS, and LCE TOE components contain plug-ins (or scripts) that provide functionality specific to the TOE component. The TOE facilitates the administration and organization of security workflow and management tasks, including automatic reporting to affected parties; division of duties; access control for application data; and update and tracking of vulnerability closure.

Information gathered by the TOE for the above tasks is stored in a centralized database. The reporting, ticketing, user interface, and security model are designed to ensure that the right people in the organization can access the information they need to make informed network security and performance decisions.

The TOE consists of the five components shown above configured as an Intrusion and Vulnerability Detection System. The Security Center 3 component collects event and vulnerability data from one or more instances of PVS sensors and one or more instances of Nessus scanners. It analyzes the data and presents the results to its users, with the help of one or more instances of LCE and 3DT components. This fits the IDS System structure specified in the IDSSYPP, to which this ST claims conformance, as follows:

- IDS Analyzer: SC3 with LCE and 3DT.
- IDS Scanner: Nessus.
- IDS Sensor: PVS.

The TOE consists of the five software components (SC3, LCE, 3DT, Nessus, and PVS) running on hardware and operating systems that are not part of the TOE. The components do not need to all be run on the same kind of platform. The networks that connect these components are not part of the TOE.

The SC3 component is able to interface with additional 3rd party generators of IDS event data, but that capability is not tested in this evaluation. .

2.1 TOE Overview

This section describes the various TOE components and how they work together.

2.1.1 Tenable Security Center (SC3)

The Tenable Security Center provides proactive, asset-based security risk management. It unifies the process of asset discovery, vulnerability detection, event management and compliance reporting by integrating the functions of the other TOE components. The primary functions of SC3, operating in conjunction with the other TOE components further described below, include[1]:

[1] Note that since SC3 serves to consolidate and present a unified view of the available functions regardless of supporting components, there has been no attempt to specifically distinguish the functions, or aspects thereof, specifically implemented by the SC3 component from the functions made accessible via SC3.

- ***Risk management:*** SC3 supports risk management through the use of periodic Nessus vulnerability scanning; continuous passive PVS vulnerability scanning; automated custom administrator notification; and vulnerability projection onto network topology

- ***Threat management:*** SC3 performs real-time IDS event aggregation and distribution; real-time IDS and vulnerability correlation; automated alerting[2] of affected administrators; and projection of IDS events onto network topology.

- ***Asset discovery and management****:* SC3 allows combining the knowledge of existing asset inventories with the vulnerability and compliance information discovered by Nessus and the Passive Vulnerability Scanner. SC3 performs asset discovery with active and passive vulnerability scanners. Resources are classified on type, location and description. It also performs vulnerability reporting, remediation and false positive management by asset type.

- ***Workflow management:*** SC3 includes a ticketing and workflow system. Vulnerability and compliance issues can have a ticket opened against them. Tickets can be applied to just the vulnerable system, any system having a vulnerability, or any vulnerable system in an asset group. Administrators can accept the risk on one or more vulnerabilities or raise or lower its severity level. SC3 also determines which users should receive notification of new tickets.

- ***Executive reporting****:* SC3 provides several methods to report and visualize vulnerability, compliance and event data: asset lists, 3D visualization using 3DT, and user customizable reports. Managers can view security threats, risks and workflows for each business unit and group of business units. Trending reports are provided for vulnerabilities and intrusion events. Resource allocation tracking is per business unit. The security of various business units can be compared.

- ***Minimal resource impact****:* SC3 configuration requirements are minimal, requiring shallow learning curves and minimal training requirements. The full-time passive scanning has no direct network visibility though the impact on network performance will vary depending on the extent of configured scans. Distributed active scanning has minimal network impact. Users interact with the TOE via a web interface and all data stays within the host network boundaries.

The SC3 TOE component can manage one or more Nessus and PVS network scanners. Scans can discover new hosts, new applications and new vulnerabilities or verify policy compliance. Nessus scans can be scheduled and automatically distributed to multiple scanners. SC3 manages the Nessus scanners and determines which are best suited to scan a particular host. It can use a remote Nessus scanner to simulate what an external attacker might see from outside the network. SC3 can manage user credentials for access control. Note that while access management may be linked to an external LDAP or Windows Domain, this use of third party authentication is not included in the scope of this evaluation.

SC3 receives Intrusion Detection System (IDS) events from multiple sources. It analyzes the event data against its vulnerability database to determine whether the target of an event is vulnerable to the attack. If it is, it reports the information to the relevant system administrators and (optionally) to users via e-mail. SC3 includes a set of common audit guides implemented by Tenable for use in various government, financial, and health care compliance audits. SC3 captures the time that system components and vulnerabilities were first discovered and when they were last seen. This allows users to demonstrate to auditors when security issues were first identified, what was done to inform system owners of their required actions (i.e., such as disabling an unauthorized service), and how long it took to close an issue.

SC3 performs IDS event correlation. It can send alerts to designated, authorized SC3 users to indicate that a protected system is being attacked, and it can be configured to only send that alert if the subject system is vulnerable

[2] Note that each component generates alerts independently relative to the events they process. For the most part Nessus and PVS just present their results to the other TOE components. LCE TASL scripts can be defined to issue alerts and SC3 can issue alerts based on normalized data that it receives.

to that specific attack. Further, PVS can be configured to detect both encrypted and clear interactive sessions and to identify these sessions by IP address, port and network protocol. It can recognize when any system inside the protected network begins to launch port scans or network sweeps.

For more accurate vulnerability to IDS event correlation, the SC3 should be configured to synchronize with the latest rules engine (as described in Appendix 1 of the Security Center 3.2 Documentation) and have the latest vulnerability information as possible. If scans are only being performed once in a great while, performing correlation on them could be of marginal value. Using daily scans or implementing passive network monitoring can greatly increase the accuracy of the correlated events.

SC3 uses five daemons (*lightningd*, *lightning-proxy*, *importd*, *logd* and *maild*) to perform communications, importation of security data, and user alerting. *lightningd* conducts all scheduled events such as launching vulnerability scans and downloading new IDS signatures and Nessus plugins. The *lightning-proxy* simulates a Nessus daemon and a Nessus client so that when a scan is launched by the Security Center, it can perform all the functions necessary for distributing the scan parameters and aggregating the results. *lightning-proxy* also pushes new vulnerability information out to the remote scanners. *importd* formats and imports raw vulnerability scan data into the Security Center's database. *logd* listens for SNMP traps and SYSLOG messages. *maild* is a dedicated outbound email tool that the Security Center uses instead of sendmail.

An Apache web server is included in the product distribution but is not part of the TOE. It can be used in the TOE environment to provide secure user and administration interfaces.

The SC3 stores all configuration data including customer, user, vulnerability and intrusion data in an embedded database that is optimized for data storage and indexing. SC3 uses Secure Shell (SSH) to make LCE queries. All reporting and data analysis is performed remotely by the LCE and presented to the user by the SC3. If the LCE discovers an anomaly or a specific type of event correlation it sends an alert to the SC3, which treats it as if it came from an IDS device.

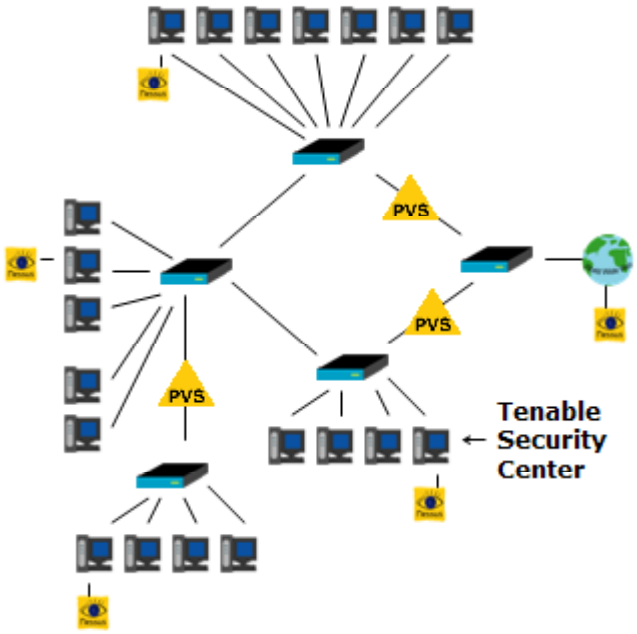

Figure 2. An example network showing the placement of Nessus scanners (yellow eyes). The routers (blue boxes) isolate local traffic on subnets, so full coverage requires a scanner on each subnet. The scanner on the external connection allows scanning traffic at the enterprise boundary. The figure also shows one Tenable SC3 component collecting and reporting events from all of the scanners and three PVSs (yellow triangles).

SC3 can receive trap analysis events directly from IDS sensors using SYSLOG and Simple Network Management Protocol (SNMP) protocols. SC3 is configured to receive IDS signature updates via direct or proxy access to the Internet. It can access the support sites or management consoles of the various IDS solutions it supports in order to build an up-to-date reference model of all the signature events it might find in logs from those IDS solutions. Correlation of event signatures from the various sensors is done by matching Common Vulnerabilities and Exposures (CVE) (http://cve.mitre.org) and bugtraq (http://www.securityfocus.com) IDs with Tenable Nessus and PVS plug-in information. SC3 also provides optional web-based reporting and analytical functions. 3DT can also be used for some analytical and presentation activities. SC3 uses the collected scan data to build dynamic asset lists of system vulnerability and configuration information using dynamic rules. These lists include account addresses, open ports numbers, specific vulnerabilities, IDs, and descriptions of discovered vulnerabilities from the know bug databases. Dynamic asset lists can be augmented with existing static asset lists collected externally to the SC3.

Although the TOE also supports a single scanner configuration (i.e., SC3 and Nessus), the evaluated configuration of the TOE is for multiple scanner configurations. Figure 2 depicts SC3 deployed on a server (lower right) and multiple Nessus scanners deployed across the small network. The triangle icons show three PVSs deployed on various network links.

2.1.2 3D Tool (3DT)

3DT is a 3D Visualization tool that runs on a user workstation and displays network topology and the relative distribution of security information in three dimensions. It runs on Windows and requires a Security Center account to access the data. It's only form of communication with the Security Center is via an SSL communication path. Users launch the 3DT tool, establish an SSL connection with the Security Center and then authenticate to the Security Center. It supports two reporting modes: network topology and a hosts-to-vulnerabilities trend comparison matrix. 3DT users can make one or more queries to populate the 3DTdata sets and the tool plots topology data for discovered routing and devices, interconnections and correspondence among network servers and clients. Two data sets can be compared using this tool. 3DT plots and explores the results of one query against another and allows the browsing of data (events) and topology. It also provides rapid visual feedback about event frequency.

2.1.3 Log Correlation Engine (LCE)

LCE aggregates, normalizes, correlates and analyzes event log data from the various devices within the network infrastructure. It is closely integrated with the Security Center, allowing the centralization of log analysis and vulnerability management.

Each Security Center can manage multiple LCEs and each LCE can receive system logs, netflows, IDS events, firewall events, honeypot events, and other types of records from multiple sources. Only Nessus Scanner and PVS IDS sources are included in the evaluated configuration, however. Security Center users see only the LCE events they are authorized to see.

The LCE implements a SYSLOG interface that it exports to clients for the purpose of accepting events to analyze and correlate. While LCE could potentially accept SYSLOGs from multiple sources, the TOE includes LCE agents for specific OSs (including the TOE component hosts) that serve to monitor those systems and generate SYSLOG findings to LCE. When an LCE receives an event, it can save the raw event data, and it can also perform customized analysis on it. When an event is to be sent to SC3, the data is normalized and forwarded. LCE enables the Security Center to perform high-speed analysis and reporting for many types of events.

The LCE includes an event scripting language, based on Tenable Nessus' NASL language, known as Tenable Application Scripting Language (TASL) that can be used to specify complex correlation tasks for execution in real time. TASL scripts can be written or installed by any of the system administrator roles, but can be executed only on the network segments to which each system administrator has access.

LCE allows SC3 functionality to be expanded to any log device, where the primary focus is to offload aggregation, normalization, analysis and reporting of security events to one or more servers other than the SC3. SC3 can be extended with one or more LCEs. The LCE runs on a separate server from the SC3. LCE can collect events using a SYSLOG interface and can make use of other generic protocols for behavioral and event correlation and can send the alerts to the SC3.

LCE includes client agents for Unix, Windows, netflow, OPSEC, RDEP and network sniffing that can be used to log a variety of network traffic. LCE clients can be placed on key servers and at network choke points to aggregate as many logs as possible. LCE implements a mode for each monitored host that includes: client or server behavior; inbound, outbound and Internet connection rates; and per event rates.

Although the TOE can be configured to accept IDS events from other sources, the evaluated configuration only includes the Tenable IDS event sources that are part of the TOE. This restriction is enforced by the ability to filter event sources based on IP Address.

2.1.4 Passive Vulnerability Scanner (PVS)

PVS continuously monitors network traffic, searching for vulnerable systems, watching for potential application compromises, observing client and server trust relationships, and tracking open or browsed network protocols in use. PVS monitors network traffic for a variety of security related information including:

- Client and server application vulnerabilities
- Detection of compromised or subverted applications
- Detecting when new hosts are added to the network
- Detecting when an internal system begins to port scan other systems
- Highlighting all interactive and encrypted network sessions
- Tracking exactly which systems communicate with other internal systems
- Detecting which ports are served and which ports are browsed for each individual system
- Passively determining the type of operating system of each active host

SC3 fuses this information with the active or credentialed scan results from Tenable Nessus. Note that the period of PVS logging is configured and SC3 gets the available data when it connects for that purpose. As such, PVS and SC3 should be coordinated appropriately. SC3 communication is facilitated via a proxy enabling the use of web-based SSL interactions When a credential scan is performed the credentials are protected by the SSL channel.

PVS is not a typical Network IDS (NIDS) in that it does not run large signature sets of known network attack or probe activity. Instead, as the PVS learns about a network's applications, it looks for compromise events in traffic originating from those systems. PVS detects when systems are compromised based on application intrusion detection; selectable rule libraries and filtering rules to look for overflows, web attacks, etc., and sniffs out vulnerabilities from network session traffic. Most protocols carry internal version and identity information.

PVS uses its own signatures and plugins for passive analysis (i.e. it does not have an agent on any of its targets). It can collect information about client-side and server-side vulnerabilities, detect rogue and non-routable hosts, discover network assets by active IP address, detect TCP SYN packets (indicating client-side usage and providing passive OS fingerprinting), TCP SYN-ACK (open services and "show-connections"). PVS is constantly updating its model of the networks it is monitoring, noting which hosts are active; which ports are open; and which plugins have matched on particular IP address.

Note that while the PVS could be configured to share its scanned data with alternate or multiple clients, the evaluated configuration restricts its sharing to other TOE components, specifically the SC3. Similarly, while the PVS can be configured to forward vulnerability and alert data via SYSLOG to other components, this capability is disabled in the evaluated configuration.

Furthermore, PVS can be configured to take actions to mitigate some IDS-related events. For example, it can send TCP resets when disallowed traffic is detected. However, given that the enforcement of such directives is outside the control of the TOE this feature has not been subject to security claims and as such has not been evaluated in this regard.

2.1.5 Nessus Scanner (Nessus)

Nessus is an active scanner that provides agent-less host auditing of both UNIX and Windows servers. It features network node discovery, asset profiling, and vulnerability analysis. Nessus scanners can be distributed throughout a large network, on DMZs, and across distributed networks. It can be used for ad-hoc scanning, daily scans, and quick-response audits. When managed with SC3, vulnerability recommendations can be sent to responsible parties, remediation can be tracked, and security patches can be audited.

Nessus discovery scans include ARP ping, Syn ping, ICMP ping, TCP CONNECT (full TCP handshake), TCP SYN. OS detection methods include port scanners that send packets in a specific way and listen for minute changes that would identify the type of server responding. Service detection scanning identifies servers by the banners they present and how they respond to probes. Vulnerability analysis scans servers for known vulnerabilities using the information about the server resulting from the port scanner, OS detection and banner detection routines. The Nessus client/server architecture has the flexibility to deploy the scanner and the Graphical User Interface (GUI) in

multiple configurations and with various reports to reflect the risk level of each security vulnerability found (i.e., from Low to High) and provides guidance on how to prevent them from being exploited.

Scan types include:

- ***Local (credentialed):*** Nessus scans the local host for security vulnerabilities, identifying missing security patches, checks client software versions, and audits policy compliance using a valid logon on the target machine. A local scan is less intrusive than a network scan and can provide information about installed software.
- ***Remote (network):*** Nessus scans remotely for vulnerabilities using its standard methodology of port scans followed up by vulnerability scans. It can identify open ports, recognize underlying OSs, and discover vulnerabilities in network services.
- ***Hybrid (both network and credentialed):*** A combination of local and remote scans that provides the most comprehensive scan of a network host.

Nessus contains service specific plugins that determine the services that are running behind specified ports, based on defined parameters. This minimizes the impact of security scans on printers and other devices that cannot support multiple open ports simultaneously. Nessus contains more than 11,000 plugins, each of which checks for one or more unique vulnerabilities. Plugins are organized into Families.

The administrator can opt to enable all security checks or to enable all security checks except the checks that are potentially harmful. (Unsafe checks are not supported in the evaluated configuration.) Administrators also have options to define new security check policies and to activate a pre-defined policy.

Nessus reporting focuses on the severity of vulnerabilities. Warnings are mild flaws or vulnerabilities that may increase the severity of other vulnerabilities. Holes are severe flaws or vulnerabilities that may have a major impact on host or network security. Nessus security reports automatically pop up as a new instance of Microsoft Internet Explorer. All reports are archived and available for later viewing and printing.

Nessus saves all of its vulnerability data in various file formats (notably XML and “nbe” which is a custom file format). The Nessus scanner includes the Nessus Attack Scripting Language (NASL) designed to allow the development of new security tests easily and quickly. NASL scripts can be written or installed by any of the system administrator roles, but can be executed only on the network segments to which each system administrator has access.

Nessus can be invoked as a command in a host system shell. This command line interface (CLI) support allows arguments on the command line so that scans can be launched via batch files or scripts. This provides support for concurrent scanning because each CLI runs as a separate process. CLI reports can be saved as NBE, NSR, XML and TXT formats. The CLI supports UNIX and some Windows functionality.

In the evaluated configuration, Nessus is configured such that it is used only via the SC3. As such, SC3 utilizes the Nessus CLI and references to the administrator, above, apply to the SC3 administrator and not a Nessus-specific role. While Nessus could be configured for multiple means of user authentication, the evaluated configuration includes only the use of passwords for authentication. This account information is configured within the SC3 for the purpose of interacting with the Nessus component(s).

2.2 TOE Architecture

This section describes the TOE physical and logical boundaries.

2.2.1 TOE Physical Boundaries

The TOE physical boundary includes the following components:

- SC3 – Tenable Security Center 3.2
- 3DT – 3D Tool 1.2
- LCE – Log Correlation Engine 2.0.2
- PVS – Passive Vulnerability Scanner 3.0
- Nessus – Nessus Scanner 3.0.4

Each bulleted item is licensed separately. The following sub-sections describe the platforms supported for each of the TOE components. These platforms are part of the TOE environment, not part of the TOE. Each system must be dedicated to the appropriate Tenable applications (Security Center, Nessus, LCE or PVS) and contain no other applications except what is required to operate the system in a secure manner. Tenable applications can co-exist on the same host.

2.2.1.1 SC3

SC3 consists of the Tenable Security Center 3.2 software component.

SC3 is supported on the following platforms: Red Hat Enterprise Server 3 and Enterprise Server 4. It must be configured with a Fully Qualified Domain Name (FQDN).

SC3 installation requirements:

Scenario	Recommended Hardware
SC3 and Nessus Scanner 3.0 managing 500 to 2,500 active IPs	Single P4 3 GHz CPU, 1 GB memory, 40 GB hard drive
SC3 managing 2,500 to 10,000 active Ips	Single P4 3 GHz CPU, 2 GB memory, 60 GB hard drive
SC3 managing more than 10,000 IPs	Single P4 3 GHz CPU, 4 GB memory, 80 GB hard drive

2.2.1.2 3DT

3DT consists of the Tenable 3D Tool 1.2 software component.

3DT supported platforms: Windows XP Professional with Service Pack 3.

2.2.1.3 PVS

PVS is the Tenable Passive Vulnerability Scanner 3.0 software component, which can be installed on Windows Server 2003 SP2, Windows XP Professional SP3, Red Hat Linux ES3 and ES4. It can be deployed on existing network IDS devices, firewalls, e-mail servers, Dynamic Host Configuration Protocol (DHCP) servers, etc. without effecting the underlying system's operation. It can also be deployed as a stand-alone device for dedicated monitoring.

PVS hardware guidelines are depicted in the following table:

Network Profile	Required Hardware
Less than 50 Mb/s	P3 1 GHz CPU
50 Mb/s to 100 Mb/s	P3/P4 1.5 GHz
More than 100 Mb/s	P4 2.0 GHz
Less than 10,000 hosts	512 MB memory
10,000 to 25,000 hosts	1 GB memory
More than 25, 000 hosts	2 GB memory

2.2.1.4 LCE

LCE consists of the Tenable Log Correlation Engine 2.0 software component. It is supported on the following platforms: Red Hat Linux Enterprise Server 3 and Enterprise Server 4.

2.2.1.5 Nessus

Nessus server includes the Nessus Scanner 3.0 software component. It is supported on the following Windows, Unix, and Unix-like systems:

- Windows: Windows Server 2003 SP2, Windows XP Professional SP3 and Windows Server 2000 SP4.
- Unix: FreeBSD 5 and 6
- Unix-like: Red Hat Linux Enterprise Server 3 and Enterprise Server 4; Debian Linux 3; SuSE 9 and 10; Solaris 10 Sparc; and Mac OS X 10.4

2.2.2 TOE Logical Boundaries

This section identifies the security functions that the Tenable TOE provides.

The following features are not included in the TOE evaluated configuration:

- The evaluated configuration requires at least one instance of each identified TOE component.
- Use of Nessus, PVS, or LCE components directly rather than via the SC3 interfaces is excluded from the evaluated configuration.
- Use of third party authentication servers, such as LDAP, is not allowed in the evaluated configuration.
- Exporting data (from any TOE component) via SYSLOG outside the TOE is not allowed in the evaluated configuration.
- The LCE clients that operate within non-TOE components have not been subject to the evaluation. *However, while their impact on their respective hosts is uncertain, they cannot impact the security claims in this ST and as such are not forbidden in the evaluated configuration.*
- The PVS ability to interfere with network traffic has not been subject to the evaluation. *Note that while this function simply has not been subject to specific evaluation claims, it does not interfere with the security of the TOE or its claimed functions and therefore can be used in the evaluated configuration. This function simply has been evaluated only to the extent that it doesn't interfere with other functions and not relative to explicit security claims of its own.*

2.2.2.1 Security Audit

The TOE generates audit events for the basic level of audit. (Note that the IDS_SDC.1 (EXP) and IDS_ANL.1 (EXP) requirements address a different audit mechanism that records the results from IDS scanning, sensing, and analyzing tasks. This is not that mechanism.) The TOE provides a SC3 GUI that is used by authorized system administrators to read the audit trail, and to sort audit data. The TOE audit events can be included in or excluded from reports based on event type. The TOE restricts access to the audit trail to authorized system administrators. The events that are audited are fixed and no event can be masked so that it is not entered into the audit trail.

The TOE administrator guidance advises the systems administrator how to configure and manage the TOE security audit storage so that storage exhaustion is prevented. If audit trail storage becomes exhausted, the TOE will overwrite the oldest record and send an alarm.

2.2.2.2 Identification and Authentication

TOE users are required to login with a unique name and password in order to access the TOE. Only systems administrators have access to security management functions. The TOE maintains user identities, authentication data, authorization information and role association. The SC3 provides a web-based logon and users must be successfully identified and authenticated prior to accessing the reports.

2.2.2.3 Security Management

The Security Center restricts the ability to manage functions based on the user role. The roles supported by the Security Center are Security Center Administrator (SCA), Primary Security Manager (PSM), Security Manager (SM) and End User (EU), (which collectively conform to the IDSSYPP Authorized Systems Administrator role). A Systems Administrator (which conforms to the IDSSYPP Authorized Administrator role) manages the environment. It is up to the TOE user organization to appropriately assign people to roles.

Small organizations may assign all roles to the same person. Larger organizations may assign roles based on their organizational structure. For example, a large organization might give responsibility for all Security Center Administration functions and any activity that requires administrative (privileged) access to the Operating System to the Information Technology group, responsibility for enterprise management of security functions throughout the business units, including the performance of all Security Center administration tasks to the Information Security group. If the business unit is a Primary Security Manager or Customer, an Information Security Officer in the business unit may be responsible for all security functions within that unit and would serve as the Security Manager for that business unit. A large organization might have multiple Primary Security Managers.

Within the business units End Users may be designated. These End Users are managed by the unit's Security Manager and are responsible for a particular network segment.

User access is restricted by the role to which the user is assigned and the assets to which the user has been granted access. The role indicates what functionality (i.e., which menu options) the TOE presents to each user. The assets are the machines for which the user can launch IDS scans and access IDS audit records. The SC3 component provides the tools necessary to define users and configure access. SC3 stores each customer's data in a separate directory so access is enforced by separating user data into separate directories. The underlying operating system limits access to the tenable user but the SC3 product actually performs access control on its users.

A description of the roles supported by the Security Center follows:

Security Center Administrator (SCA)

The Security Center Administrator role is able to configure and manage the Security Center application. No access to the underlying operating system platform is required. All functions can be performed through the Security Center GUI. The Security Center Administrator defines and manages customers, specifying which network ranges within which network traffic may be monitored for each customer. Each customer has a unique name and serial number. There are three Customer roles: the Primary Security Manager, Security Manager and End User.

The Security Center Administrator's role includes performing the following functions:

- Manage the Security Center
- Managing Security Center Customer Accounts
- Managing Security Center Components
- Monitoring Security Center Audit Logs

The Security Center Administrator (SCA) cannot access customer data nor initiate IDS scans.

Primary Security Manager (PSM)

The Primary Security Manager has full rights for the entire network space of a customer and cannot be deleted without removing the entire customer entry. The Primary Security Manager may define additional users for the address space as either Security Managers or End Users. The Primary Security Manager is typically the security representative for the customer organization and is responsible for its overall security posture.

A Primary Security Manager (PSM) can access only one customer's data and can initiate IDS scans on only one customer's network.

Security Manager (SM)

The Security Manager has the same rights as the Primary Security Manager. There can be many Security Managers for a customer, but only one Primary Security Manager.

A Security Manager (SM) can access only one customer's data and can initiate IDS scans for only one customer.

The term "(Primary) Security Manager" is used to refer to both the Primary Security Manager and Security Manager roles.

End User (EU)

The End User is typically a system or network engineer who has responsibility for running a network. The Security Manager and End User roles are limited in several ways:

- Each can only see vulnerabilities, IDS events, and logs for a specific range of IP addresses, determined by the particular asset lists a user has access to.
- Security Managers can add, edit, and delete new users, which may be either security managers or end users.
- Each type of user may be able to conduct vulnerability scanning of their networks, but both types of accounts can also be "locked out" from scanning either manually or when the threshold for failed login attempts is reached.
- Security Managers can open tickets for which vulnerabilities need to be mitigated and end users can close tickets by marking them as fixed. Opening and closing tickets is not a security function.

An End User (EU) can initiate IDS scans on only a part of one customer's network and can access only the data relevant to that part of the one customer's network.

System Administrator (Environmental Role)

The System Administrator manages the TOE environment and is the person responsible for installing and maintaining the platform Operating System on which the Security Center runs. The Systems Administrator has administrative ("root") access to the underlying operating system, but does not have access to any Security Center user accounts. System Administrator is not a TOE role, but because the System Administrator has root access to the operating system, that role is capable of accessing and changing anything in the TOE, including audit data. This role includes all standard System Administration duties, such as the following:

- Operating System Installation
- System Security Hardening
- System Configuration
- Installation of Supporting Applications
- Managing User Access to the OS platform
- Installation of the Security Center Software
- Installation of the Security Center Components (Nessus, PVS, LCE, etc)
- Installation of Client Applications
- OS System Monitoring
- Security Administration of the System
- System Backups
- Generate SSH keys on remote hosts for credential scans

The following table summarizes the TOE roles and the security functions they can perform. The Authorized Administrator and Authorized System Administrator roles are required by the IDSSYPP.

Security Function	Authorized	Authorized	Customer Accounts

	Administrator[4]	System Administrator[5]	(Primary) Security Manager	End User
Install and configure SC3[1]	X			
Manage customer accounts[2]		X		
Manage user accounts[2]			X	
Manage SC3 components[2]		X		
Monitor SC3 logs[3]			X	X
Manage audit functions[2]		X		
Monitor audit data[3]		X	X	

[1] Maps to the IDSSYPP "Query and modify all other TOE data" function.
[2] Maps to the IDSSYPP "Modify Behavior of system data collection, analysis, and reaction" function.
[3] Maps to the IDSSYPP "Query and add system and audit data" function.
[4] This role is required by the IDSSYPP to administer the platforms that support the TOE. It is a role supported by the environment here.
[5] This role is required by the IDSSYPP to administer the IDS. It is equivalent to the SC3 "Security Center Administrator" role.

2.2.2.4 Protection of the TSF

The TOE protects itself and ensures that its policies are enforced in a number of ways. While there is dependence on the underlying operating system to separate its process constructs, enforce file access restrictions, and to provide communication services, the TOE protects itself by keeping its context separate from that of its users and also by making effective use of the operating system mechanisms to ensure that memory and files used by the TOE have the appropriate access settings. Furthermore, the TOE interacts with users through well-defined interfaces designed to ensure that its security policies are always enforced.

2.2.2.5 Intrusion Detection System

The TOE collects network traffic data for use in scanning, sensing and analyzing functions with the SC3. The TOE performs signature analysis on collected network traffic data and records corresponding network traffic event data. Reports are generated using a web-based interface to LCE that provides the ability to examine analytical conclusions drawn by the TOE that describe the conclusion and identifies the information used to reach the conclusion. Note that users can only access reports via a web browser where access to TOE data is based on identification and authentication. The TOE provides the ability to generate alarms and notify an systems administrator using a configured notification mechanism when an intrusion is detected.

2.3 TOE Environment

The TOE relies on the environment to provide the following security functionality:

2.3.1 Protection of TOE communication

The environment must protect the communication among TOE components. The TOE is shipped with an implementation of OpenSSLv 0.9.8g. For most communication paths, the TOE should be configured to use the SSL protections provided in OpenSSL to protect network traffic between TOE components from disclosure and modification. The one exception is that communication between the SC3 and the LCE is performed using SSH. The SSH encryption is also supported using the OpenSSL module.

2.3.2 Non-bypassability of the TSP

The TOE should be deployed on a network in such a way that it can monitor all potentially malicious traffic, including any network traffic used to administer the TOE itself. It should ensure that no traffic can circumvent the TOE's monitoring functions and thus escape being monitored for malicious content.

2.3.3 Domain Separation

The TOE components run as separate processes in one or more operating systems. However, this separation is not used to separate users with different access rights. Users of the TOE are not provided access to operating system shells nor are they able to run arbitrary programs on the operating system as a result of their TOE access. The TOE controls user access through the functionality provided on its user interfaces.

2.3.4 Reliable Time Stamps

The TOE environment provides a source of reliable time stamps, which the TOE uses in its audit function. The system administrator needs to be aware that a network time protocol should be used to ensure consistent time across the different components and associated events.

2.3.5 Trusted Path

The TOE environment supports HTTPS sessions for remote users that protect user authentication and other information from disclosure.

2.4 TOE Documentation

Tenable offers a series of documents that describe the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features. Refer to section 5.2 for information about these and other documentation associated with the TOE.

3. Security Environment

This section summarizes the threats addressed by the TOE (often with help from its environment) and assumptions about the intended environment of the TOE. Note that while the identified threats are mitigated by the security functions implemented in the TOE, the overall assurance level (EAL2 augmented with ALC_FLR.3 and AVA_MSU.1) also serves as an indicator of whether the TOE would be suitable for a given environment.

3.1 Threats

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

3.1.1 TOE Threats

T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions 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
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.

3.1.2 IT System Threats

The following identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the Intrusion Detection System System Protection Profile.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

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

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

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

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

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

3.3 Secure Usage Assumptions

3.3.1 Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.WKSTN All desktop systems used to access security center data (either through the web GUI or through 3D Tool) must be secured, patched and have the latest anti-virus software installed.

A.OS The operating system for each component, Security Center, Nessus, LCE, and PVS, must be dedicated to the associated application and configured in a secure manner to ensure the security controls cannot be bypassed.

3.3.2 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.

3.3.3 Personnel Assumptions

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

A.NOEVIL	The authorized administrators are not willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation and that of its environment.
A.NOTRST	The TOE can only be accessed by authorized users.

4. Security Objectives

This section summarizes the security objectives for the TOE and its environment.

4.1 Security Objectives for the TOE

O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.IDSCAN	The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
O.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.IDANLZ	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.RESPON	The TOE must respond appropriately to analytical conclusions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.

4.2 Security Objectives for the Environment

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.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE and its environment critical to security policy are protected from any physical attack.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner that is consistent with IT security.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
OE.PROTECT	The IT Environment will protect itself and the TOE from external interference or tampering.
OE.INTROP	The monitored IT System is interoperable with the TOE.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE and its environment.
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.SYSTEM_PROTECTION	The IT Environment will provide the capability to protect System (i.e., IDS) information.

OE.WKSTN_PROT	Those responsible for the administrative destops will ensure they are secured, patched and have the latest anti-virus software installed.
OE.DEDICATED	The operating systems for the TOE components will be dedicated to the associated TOE component.

5. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for the TOE and associated environment components.

The TOE also satisfies a minimum strength of function: 'SOF-basic'. The only applicable (i.e., probabilistic or permutational) security functions are FIA_UAU.2, which is levied on the TOE.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are candidates to be satisfied by the TOE. These are conformant to the IDSSYPP:

Requirement Class	Requirement Component
FAU: 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
	FAU_SEL.1: Selective audit
	FAU_STG.2a: Guarantees of audit data availability
	FAU_STG.4: Prevention of audit data loss
FIA: Identification and Authentication	FIA_AFL.1: Authentication failure handling
	FIA_ATD.1: User attribute definition
	FIA_UAU.2: User authentication before any action
	FIA_UID.2: User identification before any action
FMT: Security Management	FMT_MOF.1: Management of security functions behavior
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of management functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data protection
	FPT_RVM.1a: Non-bypassability of the TSP
	FPT_SEP.1a: TSF domain separation
IDS: Intrusion Detection System	IDS_ANL.1 (EXP): Analyzer analysis
	IDS_RCT.1 (EXP): Analyzer react
	IDS_RDR.1 (EXP): Restricted data review
	IDS_SDC.1 (EXP): System data collection
	IDS_STG.1a (EXP): Guarantee of system data availability
	IDS_STG.2 (EXP): Prevention of system data loss

Table 1 TOE Security Functional Components

5.1.1 FAU - Security Audit

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 *[basic]* level of audit; and c) [Access to the System and access to the TOE and System data].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [the additional information specified in the Details column of Table 2 Auditable Events].

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System data	Object IDS, requested access
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FIA_UAU.2	All use of the authentication mechanism	User identity, location
FIA_UID.2	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MDT.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Figure 2: Auditable Events

FAU_SAR.1 - Audit Review

FAU_SAR.1.1 The TSF shall provide [**authorized systems administrator**] with the capability to read [**all audit information**] 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.

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.

FAU_SAR.3 - Selectable Audit Review

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

FAU_SEL.1 - Selective Audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: a) [*event type*] b) [**no additional attributes**].

FAU_STG.2a - Guarantees of Audit Data Availability

FAU_STG.2a.1 The TSF shall protect the stored audit records from unauthorized deletion.
FAU_STG.2a.2 The TSF shall be able to [*detect*] modifications to the audit records.
FAU_STG.2a.3 The TSF shall ensure that [**the most recent, limited by available System data storage**] audit records will be maintained when the following conditions occur: [***audit storage exhaustion***].

FAU_STG.4 - Prevention of Audit Data Loss

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

5.1.2 FIA - Identification and Authentication

FIA_AFL.1 - Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [a settable, non-zero number] of unsuccessful authentication attempts occur related to [external IT products attempting to authenticate].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offending external IT product from successfully authenticating until an authorized administrator takes some action to make authentication possible for the external IT product in question].

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) Authorizations; and d) [**Roles.**]].

FIA_UAU.2 – User Authentication before any Action

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

FIA_UID.2 – User Identification before any Action

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

5.1.3 FMT - Security Management

FMT_MOF.1 - Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [*modify the behavior of*] the functions of System data collection, analysis and reaction to [authorized System administrators].

FMT_MTD.1 - Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [*query and add*] [System and audit data], and shall restrict the ability to [*query and modify*] [all other TOE data] to [**authorized System administrators (to query and add system and audit data) and the authorized administrators (to query and modify all other TOE data)**].

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**Management of Analyzer data, Management of Audit functions, Management of user accounts**].

FMT_SMR.1 - Security Roles

FMT_SMR.1.1 The TSF shall maintain the following roles: authorized administrator, authorized System administrators, and [**no other roles**].
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Note: *The roles in this requirement are copied from directly from the pp. The TOE realizes these roles in the following manner. The Authorized Administrator role is a TOE environmental role and is realized by the Systems Administrator role in the TOE. The Authorized System Administrator role is realized by four roles in the TOE. Those roles are: Security Center Administrator, Primary Security Manager, Security Manager, and End User. More information is provided in Section 6.1.3.*

5.1.4 FPT – Protection of the TSF

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.

FPT_RVM.1a - Non-bypassability of the TSP

FPT_RVM.1a.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1a - TSF domain separation

FPT_SEP.1a.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1a.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.5 IDS – Intrusion Detection System

IDS_ANL.1 (EXP) - Analyzer analysis

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received: [***signature, statistical, integrity***]; and [**no other analytical functions**]. (EXP)
IDS_ANL.1.2 The System 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. [**location and description**]. (EXP)

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

IDS_RCT.1 (EXP) - Analyzer react

IDS_RCT.1.1 The System shall send an alarm to [**authorized system administrator**] and take [**no other action**] when an intrusion is detected. (EXP)

IDS_RDR.1 (EXP) - Restricted Data Review

IDS_RDR.1.1 The System shall provide [**authorized system administrators**] with the capability to read [**all data**] from the System data. (EXP)

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information. (EXP)

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

IDS_SDC.1 (EXP) - System Data Collection

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s): a) [***identification and authentication events; data accesses; service requests; network traffic; security configuration changes; data introduction; detected malicious code; access control configuration; service configuration; authentication configuration; accountability policy configuration; detected known vulnerabilities***]; and b) [**no other specifically defined events**]. (EXP)

IDS_SDC.1.2 At a minimum, the System shall collect and record 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) The additional information specified in the Details column of the following Table 3 System Events. (EXP).

Event	Details
Identification and authentication events	User identity, location, source address, destination address
Data accesses	Object IDS, requested access, source address, destination address
Service requests	Specific service, source address, destination address
Network traffic	Protocol, source address, destination address
Security configuration changes	Source address, destination address
Data introduction	Object IDS, location of object, source address, destination address
Detected malicious code	Location, identification of code
Access control configuration	Location, access settings
Service configuration	Service identification (name or port), interface, protocols
Authentication configuration	Account names for cracked passwords, account policy parameters
Accountability policy configuration	Accountability policy configuration parameters
Detected known vulnerabilities	Identification of the known vulnerability

Table 2: System Events

IDS_STG.1a (EXP) - Guarantee of System Data Availability

IDS_STG.1a.1 The System shall protect the stored System data from unauthorized deletion. (EXP)

IDS_STG.1a.2 The System shall protect the stored System data from modification. (EXP)

IDS_STG.1a.3 The System shall ensure that [**the most recent, limited by available System data storage**] System data will be maintained when the following conditions occur: [***System data storage exhaustion***]. (EXP)

IDS_STG.2 (EXP) - Prevention of System data loss

IDS_STG.2.1 The System shall [***overwrite the oldest stored System data***] and send an alarm if the storage capacity has been reached. (EXP)

5.2 IT Environment Security Functional Requirements

Since the TOE is software only, the following SFRs are assessed to the IT environment, as authorized by IDSSYPP:

Requirement Class	Requirement Component
FAU: Security Audit	FAU_STG.2b: Guarantees of audit data availability
FPT: Protection of the TOE Security Functions	FPT_RVM.1b: Non-bypassability of the TSP
	FPT_SEP.1b: TSF domain separation
	FPT_STM.1: Reliable time stamps
FTP: Trusted path/channels	FTP_TRP.1: Trusted path
IDS: Intrusion Detection System	IDS_STG.1b (EXP): Guarantee of system data availability

5.2.1 FAU - Security Audit

FAU_STG.2b - Guarantees of Audit Data Availability

FAU_STG.2b.1 The ~~TSF~~ **IT environment** shall protect the stored audit records from unauthorized deletion.
FAU_STG.2b.2 The ~~TSF~~ **IT environment** shall be able to [*protect*] modifications to the audit records.
FAU_STG.2b.3 The ~~TSF~~ **IT environment** shall ensure that [**the most recent, limited by available System data storage**] audit records will be maintained when the following conditions occur: [***audit storage exhaustion***].

5.2.2 FPT - Protection of the TOE Security Functions

FPT_RVM.1b - Non-bypassability of the TSP

FPT_RVM.1b.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.

FPT_SEP.1b - TSF domain separation

FPT_SEP.1b.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.1b.2 The ~~TSF~~ **IT environment** shall enforce separation between the security domains of subjects in the TSC.

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 **and TOE** use.

5.2.3 FTP – Trusted path/channels

FTP_TRP.1 – Trusted path

FTP_TRP.1.1 The ~~TSF~~ **IT environment** shall provide a communication path between itself and **[*remote*]** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The ~~TSF~~ **IT environment** shall permit **[*remote users*]** to initiate communication via the trusted path.

FTP_TRP.1.3 The ~~TSF~~ **IT environment** shall require the use of the trusted path for ***[initial user authentication, [and protection of user sessions from disclosure]]***.

5.2.4 IDS – Intrusion Detection System

IDS_STG.1b (EXP) - Guarantee of System Data Availability

IDS_STG.1b.1 The IT environment shall protect the stored System data from unauthorized deletion. (EXP)
IDS_STG.1b.2 The IT environment shall protect the stored System data from modification. (EXP)
IDS_STG.1b.3 The IT environment shall ensure that [**the most recent, limited by available System data storage**] System data will be maintained when the following conditions occur: [***System data storage exhaustion***]. (EXP)

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL2 augmented with ALC_FLR.3 and AVA_MSU.1 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.2: Configuration items
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.1: Descriptive high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life cycle support	ALC_FLR.3: Systematic flaw remediation
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1: Examination of guidance
	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 4: EAL 2 augmented with ALC_FLR.3 and AVA_MSU.1 Assurance Components

5.3.1 ACM - Configuration management

5.3.1.1 ACM_CAP.2 - Configuration items

ACM_CAP.2.1d The developer shall provide a reference for the TOE.

ACM_CAP.2.2d The developer shall use a CM system.

ACM_CAP.2.3d The developer shall provide CM documentation.

ACM_CAP.2.1c The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2c The TOE shall be labeled with its reference.

ACM_CAP.2.3c The CM documentation shall include a configuration list.

ACM_CAP.2.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.5c The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.6c The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.7c The CM system shall uniquely identify all configuration items.

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

5.3.2 ADO - Delivery and operation

5.3.2.1 ADO_DEL.1 - Delivery procedures

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 ADO_IGS.1 - Installation, generation, and start-up procedures

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 ADV - Development

5.3.3.1 ADV_FSP.1 - Informal functional specification

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 ADV_HLD.1 - Descriptive high-level design

ADV_HLD.1.1d The developer shall provide the high-level design of the TSF.

ADV_HLD.1.1c The presentation of the high-level design shall be informal.

ADV_HLD.1.2c The high-level design shall be internally consistent.

ADV_HLD.1.3c The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5c 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.1.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

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

ADV_HLD.1.2e 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 ADV_RCR.1 - Informal correspondence demonstration

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 AGD - Guidance documents

5.3.4.1 AGD_ADM.1 - Administrator guidance

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 behavior 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 AGD_USR.1 - User guidance

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 behavior 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 ALC - Life cycle support

5.3.5.1 ALC_FLR.3 - Systematic flaw remediation

ALC_FLR.3.1d The developer shall provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.3.2d The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.3.3d The developer shall provide flaw remediation guidance addressed to TOE users.

ALC_FLR.3.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.3.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.3.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.3.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.3.5c The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.3.6c The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.3.7c The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.3.8c The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

ALC_FLR.3.9c The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.

ALC_FLR.3.10c The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.

ALC_FLR.3.11c The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.

ALC_FLR.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6 ATE - Tests

5.3.6.1 ATE_COV.1 - Evidence of coverage

ATE_COV.1.1d The developer shall provide evidence of the test coverage.

ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

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

5.3.6.2 ATE_FUN.1 - Functional testing

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.

5.3.6.3 ATE_IND.2 - Independent testing - sample

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 AVA - Vulnerability assessment

5.3.7.1 AVA_MSU.1 - Examination of guidance

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 AVA_SOF.1 - Strength of TOE security function evaluation

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 AVA_VLA.1 - Developer vulnerability analysis

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

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security Audit

The TOE generates audit records for at least the basic level of audit, including the following events.

- Start-up and shutdown the SC3 component. If the SC3 component is enabled, then auditing is turned in and cannot be turned off.
- Access to the system by TOE users
- Access to the TOE and system data by other system components
- Successful and unsuccessful attempts to read from the audit trail
- Successful and unsuccessful attempts to launch scans
- Modifications to the audit configuration
- Successful and unsuccessful attempts at user identification and authentication
- Modifications to the TSF configuration and data
- Modifications to the TOE users role assignments.

Each audit record contains at least the following information: date and time of the event, event type, subject identity, and event success or failure.

TOE security audit records are stored in flat files that can grow to use all the space in the file system. A new file is started at the beginning of each month. These files are small compared to the IDS data and are only constrained in size by the size of their disk partition. The vendor provides guidance to administrators and users on how to configure audit storage to prevent it from becoming exhausted. The systems administrator configures and manages the audit storage, but the admin is the only role that the TOE authorizes to access the audit records.

The SC3 provides a web based interface for viewing audit records. The admin user is the only role authorized access the audit records. There is no configuration option to enable another user to view the audit logs or to turn off the audit function. The audit functionality is built-in to the application and there are no options available to disable it. The web interface allows the admin user to search the audit date based on keyword or keyword combination searches. The current month's audit file is searched by default but other files can be specified.

TOE security audit records are stored in flat files that can grow to use all the space in the file system. A new file is started at the beginning of each month. These files are small compared to the IDS data and are only constrained in size by the size of their disk partition. The vendor provides guidance to administrators and users on how to configure audit storage to prevent it from becoming exhausted. Note that the TOE can be configured to monitor the disk usage on each component and issue an alarm via the SC3 and also send an e-mail to a configured user (Primary Security manager by default) should the available disk space drop below a limit (the default is 15%) defined by the administrator when configuring the function. The authorized administrator configures and manages the audit storage, but the authorized system administrator (the SCA) is the only role that the TOE authorizes to access the audit records.

The Security Audit function satisfies the following security functional requirements:

- FAU_GEN.1: Audit data generation
- FAU_SAR.1: Audit review
- FAU_SAR.2: Restricted audit review
- FAU_SAR.3: Selectable audit review
- FAU_SEL.1: Selective audit
- FAU_STG.2a: Audit data availability
- FAU_STG.4: Prevention of audit data loss

6.1.2 Identification and Authentication

The SC3 TOE component provides an HTTP-based GUI logon interface. TOE users are required to login to the SC3 TOE component with a unique name and password before access to the TOE is granted. The TOE maintains user identities, authentication data, authorization information and role association information for each user. Users must be successfully identified and authenticated prior to accessing any reports.

The Security Center Administrator can configure the TOE to lock a specific account after a configurable number of consecutive unsuccessful login attempts occur. It is up to users to contact a Security Center Administrator to request that a locked account be unlocked.

When using the 3DT client, users must still authenticate successfully to the SC3. The 3DT client is simply an application that makes visualization more pleasant for the administrator. The 3DT application will pass authentication credentials to the SC3 to perform authentication before any TOE information can be displayed to the end user. .

The Identification and Authentication function satisfies the following security functional requirements:

- FIA_AFL.1: Authentication failure handling
- FIA_ATD.1: User attribute definition
- FIA_UAU.2: User authentication before any action
- FIA_UID.2: User identification before any action

6.1.3 Security Management

The IDSSYPP defines two roles: Authorized Administrator and Authorized System Administrator. The Authorized Administrator role is a TOE environmental role and is realized by the Systems Administrator role in the TOE. The Authorized System Administrator role is realized by four roles in the TOE. Those roles are: Security Center Administrator, Primary Security Manager, Security Manager, and End User. The term "TOE users" will be used when referring to all four of the TOE roles, since only the four administrative roles are allowed access by the TOE. The term "(Primary) Security Managers" will be used to refer to both Primary Security Managers and Security Managers. Otherwise, each role will be identified specifically. The TOE restricts the ability to manage functions related to audit and system data to Security Center Administrators. They are able to query and add system and audit data; and query and modify all other TOE data. Scanning, sensing and analyzing tasks are restricted to (Primary) Security Managers and End Users, who can modify the behavior of system data collection, analysis and reaction. The environment supports the Authorized Administrator role. Authorized Administrators manage the operating systems, and install and configure the TOE.

(Primary) Security Managers, and End Users operate the IDS system on specific parts of the network domain space called a customer. A customer is made up of one or more managers who perform actions for the customer. The managers are expected to work together for a customer. (Primary) Security Managers administer a customer network and are able to initiate customer analyzer IDS audit functions, access IDS audit data, and manage user accounts. Only Primary Security Managers are able to add new IDS sources. End Users administer a specific sub-network within a customer network. Depending on the size of the organization, some or all of these roles may be assigned to one individual.

The Primary Security Manager is the first account created for a TOE customer. If the Primary Security Manager account is deleted, the customer is also deleted, even if other Security Manager accounts are active at the time.

The TOE maintains a directory structure in the host file system to hold data for specific customers. Subdirectories can be created to further subdivide customer data according to sub-networks. The Security Center Administrator creates this structure in the course of configuring customers and gives access to the Customer's Primary Security Manager, who may then create other Security Managers and End Users. The (Primary) Security Managers can restrict the access that End Users have within the customer structure and thus restrict them to operating the IDS on specific subsets of the customer network.

The TOE offers access by (Primary) Security Managers and End Users via these directories, according to the scope of their authority. (Primary) Security Managers can access customer directories. End Users can access only specific subdirectories within a Customer directory. This access is determined by the TOE. When a Primary Security Manager account is deleted, the corresponding Customer directory is also deleted.

User access is restricted by the role to which the user is assigned and the assets to which the user has been granted access. All SC3 functions are controlled by asset lists. Individual Security Center users are assigned one or more asset lists. These lists can be either static or dynamic. Users who have the ability to scan can only scan hosts in their asset lists. Similarly, users can only see vulnerability, compliance, intrusion detection, and normalized logs for systems within their asset groups. The role indicates what functionality (i.e., which menu options) the TOE presents to each user. The assets are the machines for which the user can launch IDS scans and access IDS audit records.

The Authorized Administrator environmental role is implemented by the underlying operating system, where it is called System Administrator or Administrator or Root. It has full access to the underlying operating system and, by implication, the entire TOE.

The Security Management function satisfies the following security functional requirements:

- FMT_MOF.1: Management of security functions behavior
- FMT_MTD.1: Management of TSF data
- FMT_SMF.1: Specification of management functions
- FMT_SMR.1: Security roles

6.1.4 Protection of the TSF

The TOE uses the SSH and SSL capabilities of its environment when communicating among its distributed parts to protect transferred data from disclosure and modification. SSH is used between the SC3 and the LCE. In all other instances, SSL is used. The cryptographic keys necessary to support this use of SSH and SSL are created or installed during the installation or administration of the operating systems that run under the TOE components. TOE administrator guidance documents include advice on administering the SSH and SSL mechanisms in the environment.

Note that SSH and SSL are fully implemented within the hosts of the TOE applications. Though the guidance documents refer to configuring SSH and SSL for use by the components, this is done within the host operating systems and not via TOE functions. While there is an expectation that the environment will provide SSH and SSL services that can be used by the TOE, the TOE has not specific requirements about the implementation of SSH and SSL (e.g., its algorithm). As such, this ST does not define specific cryptographic requirements for itself nor for its environment.

The TOE instantiates itself as a process provided by the underlying operating system. The TOE protects its files using features provided by the underlying operating system. Specifically, it ensures that the security properties of those objects do not allow access by other operating system processes. This serves to both protect the TOE itself as well as to ensure that any attempts to access the data collected by the TOE must be made through the TOE. Furthermore, the TOE has been carefully designed to offer well-defined interfaces that ensure that access to protected resources is subject to the applicable TOE security policies.

- FPT_ITT.1: Basic internal TSF data transfer protection
- FPT_RVM.1a: Non-bypassability of the TSP
- FPT_SEP.1a: TSF domain separation

6.1.5 Intrusion Detection System

The TOE collects and records network traffic data for use by the scanning, sensing and analyzing functions with the SC3. The following event types are collected:

- Identification and authentication
- Data accesses
- Service Requests
- Network Traffic
- Security Configuration Changes
- Data Introduction
- Detected Malicious Code
- Access Control Configuration
- Service Configuration
- Authentication Configuration
- Accountability Policy Configuration

For each event the TOE records at least the following information: date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

The Security Center Administrator can specify the types of events that will be audited by configuring the various PVC and Nessus scanners deployed in the monitored system. The TOE comes with several pre-configured audit configuration files that were derived from NSA and other guidelines for the configuration of Unix and Windows systems.

The TOE performs analysis on all signature, statistical and integrity data. Signature analysis involves identifying deviations from normal patterns of behavior (e.g., it may use mean frequencies and measures of variability to identify abnormal usage). Statistical analysis involves identifying patterns of usage that correspond to known attacks or misuses of the system (e.g., patters of system settings and user activity can be compared against a database of known attacks). Integrity analysis involves comparing system settings or user activity at some point in time with that at another point in time to detect (possibly unauthorized) differences. When analysis identifies an anomaly the TOE records an analytical result that contains at least the date and time of the result, type of result, identification of data source, location, and description.

Reports are generated using a web-based interface to SC3 that provides access to the LCE, allowing users to examine analytical conclusions and the information used to reach those conclusions in an intuitive way.

TOE users access reports via a web browser. The Security Center Administrator controls access to the reports based on userid and role.

When an intrusion is detected, the TOE can generate alarms and notify anyone, using a notification mechanism, such as e-mail, that is configured by the Security Center Administrator.

LCE stores events into one or more silos (there can be up to 255). Each silo consists of an index file and a data file. When a silo is filled (determined by the maximum silo size), the next silo is written to. When the last silo is filled, the first silo is overwritten. The silo mechanism and the large maximum disk space supported by the TOE allows the system to be configured with enough storage so that filled silos can be copied to long term storage and returned to use before all of the disk space is consumed and before any IDS data are overwritten. However, if the system is not provided with adequate silo storage space or silo maintenance is neglected, IDS data can be lost. With sufficient neglect, the maximum number of lost IDS data is unbounded. In order to mitigate overflow of storage, the LCE and SC3 components both support filtering of inputs based on IP address.

Each silo has a maximum file size specified in MB or GB. The maximum file size for a silo is 4 GB. With 255 potential silos, that is approximately 1.5 terabytes of potential IDS data storage. In practice, the vendor recommends that the LCE servers be tuned to handle up to 250 million events. Assuming roughly 300 bytes per record, this will require approximately 75 GBs. However, some organizations will have shorter or longer messages.

In the evaluated configuration, the TOE is configured to periodically download updated signature files and plugins from Tenable servers over the Internet. Connection is made to the download server using https, which serves to authenticate the server to the TOE. The TOE authenticates itself to the server by providing a Nessus Plugin Subscription Activation Code that is distributed with the product and entered during product installation. The PVS component does encrypt the plugins. Nessus does not encrypt the plugins it distributes rather it has a two-tiered approach: regular and 'trusted'. Trusted plugins must be signed by Tenable, or a user can create / sign a plugin as well. The signature tells Nessus that the plugin is trusted and allows it to perform more operations at a lower level to the machine. .

The environment is responsible to restrict access to IDS data via its interfaces so that in effect the TOE controls access to that data.

The Intrusion Detection System function satisfies the following security functional requirements:

- IDS_ANL.1 (EXP): Analyzer analysis
- IDS_RCT.1 (EXP): Analyzer react
- IDS_RDR.1 (EXP): Restricted data review
- IDS_SDC.1 (EXP): System data collection
- IDS_STG.1a (EXP): Guarantee of system data availability
- IDS_STG.2 (EXP): Prevention of system data loss

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The Tenable Configuration Management Plan (CMP) identifies the measures applied by Tenable to ensure that configuration items are uniquely identified and that documented procedures are used to control and track changes that are made to the TOE. Tenable uses the Concurrent Versioning System (CVS) to ensure that changes to the implementation representation are controlled. Tenable performs configuration management on the TOE, which consists of the implementation representation (source code), design documentation, and user and administrator guidance.

These activities are documented in:

- Version Management at Tenable, Revision 1, August 24, 2007

The Configuration management assurance measure satisfies the following EAL2 augmented with ALC_FLR.3 and AVA_MSU.1 assurance requirements:

- ACM_CAP.2

6.2.2 Delivery and operation

Tenable's delivery documentation identifies the TOE and explains how the TOE is delivered, the carriers utilized, and the procedures and processes implemented to maintain security when the TOE is distributed to the user's site. It documents their system control and distribution facilities.

Tenable's Installation, generation, and start-up procedures explain how the TOE is installed, generated, and started up in a secure manner, as intended by Tenable. They show a secure transition from the TOE's implementation representation, under configuration control, to its initial operation in the customer environment.

These activities are documented in:

- Security Center 3.2 Documentation (Revision 55)
- Tenable Nessus 3.0 Installation Guide (Revision 14)
- Security Center 3.2 Quick Start Guide (Revision 16)
- Tenable Product Delivery Process, May 1, 2007 (Revision 1)

The Delivery and operation assurance measure satisfies the following EAL2 augmented with ALC_FLR.3 and AVA_MSU.1 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

Tenable documents describing the design of the TOE include a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; and correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the subsystems.

These activities are documented in:

- Tenable Network Security, Security Center 3.2 Functional Overview, March 25, 2008, Revision 4

The Development assurance measure satisfies the following EAL2 augmented with ALC_FLR.3 and AVA_MSU.1 assurance requirements:

- ADV_FSP.1
- ADV_HLD.1

- ADV_RCR.1

6.2.4 Guidance documents

Tenable guidance documentation describes the product in a way that ensures that all administrators, managers, and users understand the operation environment. They provide detailed, accurate information on how to administer the TOE in a secure manner and how to make effective use of the TSF privileges and protection functions.

These activities are documented in:

Security Center

- Security Center 3.2 Documentation (Revision 55)
- Security Center 3.2 Quick Start Guide (Revision 16)
- 3D Tool 1.0 User Guide (Revision 5)

Nessus

- Tenable Nessus 3.0 Installation Guide (Revision 14)
- Nessus 3.0 Advanced User Guide (Revision 8)
- Nessus Credential Checks for Unix and Windows (Revision 17)
- Nessus Compliance Checks (Revision 27)

LCE (Thunder):

- Log Correlation Engine 2.0 Administration and User Guide (Revision 25)
- Log Correlation Engine 2.0 Client Guide (Revision 18)
- Log Correlation Engine 2.0 Log Analysis Guide (Revision 7)
- TASL Reference Guide (Revision 14)
- Log Correlation Engine 2.0 Statistics Daemon Guide (Revision 13)

Passive Vulnerability Scanner

- Passive Vulnerability Scanner 3.0 User Guide (Revision 11)

The Tenable guidance documents satisfy the following EAL2 augmented with ALC_FLR.3 and AVA_MSU.1 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life cycle support

Tenable provides documents describing their established procedures and methods for tracking security flaws, identifying corrective actions, and the automatic distribution of corrective action information to TOE users in a timely fashion. TOE users, developers and engineers can report flaws at any time during the TOE's life cycle.

These activities are documented in:

- Tenable Network Security Quality Assurance: Mantis Use at Tenable, October 1, 2007, Revision 4 (revision unchanged)
- Customer Support: Cerberus Helpdesk Use at Tenable, October 1, 2007, Revision 2

The Life cycle support assurance measure satisfies the following EAL2 augmented with ALC_FLR.3 and AVA_MSU.1 assurance requirements:

- ALC_FLR.3

6.2.6 Tests

Tenable has test suites to test the functions of the TOE, although exhaustive specification testing of the interfaces is not required. It shows that each security function has been sufficiently tested against the behavioral claims in the functional specification.

These activities will be documented in:

- SC3 Test Plan v1.2
- SC3 Test Cases v1.2
- Mantis Use at Tenable (Oct 2007 Revision 4)
- Tenable Network Security Help Desk (Cerberus)

The Tests assurance measure satisfies the following EAL2 augmented with ALC_FLR.3 and AVA_MSU.1 assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.7 Vulnerability assessment

Tenable Vulnerability Assessment documents the existence and exploitability of flaws or weaknesses in the TOE in the intended environment. It describes a systematic search for vulnerabilities in the TOE (including the misuse of TOE guidance documents), provides an assessment of vulnerabilities found, and indicates their relevance to the intended environment for the TOE.

Tenable Strength of Function (SOF) analysis shows that the SOF claims made in the ST for all probabilistic or permutational mechanisms are supported by an analysis.

The strength of function claim is: SOF-Basic, based on the identification and authentication security function FIA_UAU.2 (User Authentication before any Action).

These activities are documented in:

- Tenable Security Center 3.20 Vulnerability Analysis
- Tenable 3D Tool 1.20; Log Correlation Engine 2.0.2 (LCE) Vulnerability Analysis
- Tenable Passive Vulnerability Scanner 3.02.2 Vulnerability Analysis
- Tenable Nessus Scanner 3.0.4 Vulnerability Analysis

The Vulnerability assessment assurance measure satisfies the following EAL2 augmented with ALC_FLR.3 and AVA_MSU.1 assurance requirements:

- AVA_MSU.1
- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

The TOE conforms to the US Government Intrusion Detection System System Protection Profile (IDSSYPP), Version 1.6, April 4, 2006.

This Security Target includes all of the Security Functional and Security Assurance Requirements from the PP, except as noted below. The following are PP conformance issues raised in the PP Errata:

- FPT_STM.1 was moved to the environment, as allowed in the IDSSYPP Errata for TOEs that do not include hardware.
- FPT_SEP.1 and FPT_RVM.1 were iterated in the environment, as allowed in the PP Errata for TOEs that do not include hardware.
- FAU_STG.2b and IDS_STG.1b were added to the environment to better explain how the entire product protects the audit and IDS data. This is permitted in the PP Errata for TOEs that do not include hardware.
- The TOE relies on its host operating systems for audit storage, so FAU_STG.2 is replicated for the TOE and its environment and OE.AUDIT_PROTECTION is included. Similarly, IDS_STG.1 has been replicated for the TOE and its environment and a new objective (OE.SYSTEM_PROTECTION) has been added for the environment..
- The TOE provides its own audit record sorting mechanism, so FAU_SAR.3 remains a TOE SFR and OE.AUDIT_SORT is not included.

This Security Target includes all of the assumptions and threats statements described in the PP, verbatim. None were added. However, the assumptions regarding competent and non-malicious administrators have been extended to include the environment as well as the TOE itself.

This Security Target includes all of the Security Objectives from the PP, verbatim. None were added except as allowed in the IDSSYPP Errata, as noted below. However, the environment objective for physical protection of the TOE has been extended to address components in the environment also critical to the secure operation of the TOE.

Section 5 of this Security Target specifically identifies each of the operations that have been performed on requirements drawn from the PP. Note that operations already performed in the PP have not been identified in this Security Target.

The following SFRs from the PP have not been included in this ST: FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1. They were dropped because the TOE has no communications with external IT products, making these SFRs unnecessary. To further support the exclusion of these SFRs, PD-0097 (http://niap.nist.gov/cc-scheme/PD/0097.html) states the inter-TSF related requirements (FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1) were erroneously included in the PP. PD-0097 also states the O.EXPORT objective was erroneously replicated into the system PP. This ST has deleted the O.EXPORT objective to be consistent with PD-0097. Additionally, PD-0097 also indicates that FPT_ITT.1 should be included when the TOE is a distributed TOE. The IDS system described herein is a distributed TOE so FPT_ITT.1 has been included.

FIA_UID.1 and FIA_UAU.1 in the IDSSYPP were upgraded to FIA_UID.2 and FIA_UAU.2 in the ST to accurately reflect what the TOE does. They are both hierarchical to the corresponding SFRs in the PP.

The objectives OE.TIME and OE.PROTECT specified in the PP errata were added to the ST and mapped according to the PP errata guidance.

A.NOEVIL was modified to remove the “careless” component that was included in the assumption in the PP, since carelessness does not necessarily derive from evil motives.

A.OS and A.WKSTN (and associated environmental objectives) were added to address the protection of the component workstations.

FMT_SMF.1 was added to capture the security function management capabilities of the TOE.

The Tenable product suite provides the specified level of audit to satisfy the IDSSYPP.

Interpretations

The following International Interpretations have been incorporated into the PP requirements by using CC 2.3 for the ST: RI #003, RI #051, RI #094, and RI #141.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

8.1.1 Complete Coverage – Environmental Assumptions

This section shows coverage of the Non-IT security objectives by the environmental assumptions. The following table shows this assumption to objective mapping.

		OE.INSTAL	OE.PHCYAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.WKSTN_PROT	OE.DEDICATED
Intended usage assumptions	A.ACCESS					X		
	A.ASCOPE					X		
	A.DYNMIC				X	X		
	A.WKSTN						X	
	A.OS							X
Physical assumptions	A.LOCATE		X					
	A.PROTCT		X					
Personnel assumptions	A.MANAGE				X			
	A.NOEVIL	X	X	X				
	A.NOTRST		X	X				

8.1.1.1 A.ACCESS

The TOE has access to all the IT System data it needs to perform its functions.

This Assumption is satisfied by ensuring that:

- OE.INTROP: The OE.INTROP objective ensures the TOE can get the IT system data that it needs to perform its intrusion detection function.

8.1.1.2 A.ASCOPE

The TOE is appropriately scalable to the IT System the TOE monitors.

This Assumption is satisfied by ensuring that:

- OE.INTROP: The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

8.1.1.3 A.DYNMIC

The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

This Assumption is satisfied by ensuring that:

- OE.INTROP: The OE.INTROP objective ensures the TOE has the proper access to the IT System.
- OE.PERSON: The OE.PERSON objective ensures that the TOE will be managed appropriately.

8.1.1.4 A.LOCATE

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

This Assumption is satisfied by ensuring that:

- OE.PHYCAL: The TOE is protected from any physical attack.

8.1.1.5 A.PROTCT

The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

This Assumption is satisfied by ensuring that:

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

8.1.1.6 A.MANAGE

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

This Assumption is satisfied by ensuring that:

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

8.1.1.7 A.NOEVIL

The authorized administrators are not willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation and that of its environment.

This Assumption is satisfied by ensuring that:

- OE.INSTALL: The OE.INSTAL objective ensures that the TOE is properly installed and operated.
- OE.PHYCAL: The OE.PHYCAL objective provides for physical protection of the TOE and its environment by authorized administrators.

- OE.CREDEN: The OE.CREDEN objective supports this assumption by requiring protection of all authentication data

This assumption requires the TOE to prevent attackers from becoming authorized administrators by obtaining and using administrator credentials. This requires the TOE to be physically protected, to be properly installed and operated, and that the administration credentials be adequately protected. This assumption also requires administrators who might be willfully negligent or hostile to be avoided and that administrators be trained and motivated to manage the TOE according to the TOE documentation.

8.1.1.8 A.NOTRST

The TOE can only be accessed by authorized users.

This Assumption is satisfied by ensuring that:

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

8.1.1.9 A.WKSTN

All desktop systems used to access security center data (either through the web GUI or through 3D Tool) must be secured, patched and have the latest anti-virus software installed.

This Assumption is satisfied by ensuring that:

- OE.WKSTN_PROT: The OE.WKSTN_PROT objective ensure the administrator responsible for the workstation with the administrator tools will be secured, patched with the latest updates and will be running the latest anti-virus software.

8.1.1.10 A.OS

The operating system for each component, Security Center, Nessus, LCE, and PVS, must be dedicated to the associated application and configured in a secure manner to ensure the security controls cannot be bypassed

This Assumption is satisfied by ensuring that:

- OE.DECICATED: The OE.DEDICATED objective ensures the platform for each TOE component is dedicated to the components and managed in a secure manner.

8.1.2 Complete Coverage – Organizational Security Policies

This section shows that all organizational security policies are completely covered by the TOE security objectives and that each objective counters or addresses at least one policy.

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	OE.INSTAL	OE.PHCYAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME	OE.PROTECT	OE.AUDIT_PROTECTION	OE.SYSTEM_PROTECTIO
P.DETECT		X	X							X						X	X			
P.ANALYZ				X	X															
P.MANAGE	X					X	X	X				X		X	X					
P.ACCESS	X						X	X												
P.ACCACT								X		X							X			
P.INTGTY											X									
P.PROTCT								X	X				X					X		

8.1.2.1 P.DETECT

Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

This Policy is satisfied by ensuring that:

- O.AUDITS: the required system audit data is collected.
- O.IDSENS: the required sensor data regarding system security events is collected.
- O.IDSCAN: the required scanner data regarding system configuration is collected.

- OE.INTROP: the monitored IT System is interoperable with the TOE.
- OE.TIME: the time dependent security monitoring functions have a reliable source of time.

8.1.2.2 P.ANALYZ

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

This Policy is satisfied by ensuring that:

- O.IDANLZ: analytical processes are applied to data collected from Sensors and Scanners.
- O.RESPON: the TOE responds appropriately to analytical conclusions.

8.1.2.3 P.MANAGE

The TOE shall only be managed by authorized users.

This Policy is satisfied by ensuring that:

- O.PERSON: competent administrators will manage the TOE.
- O.EADMIN: there is a set of functions for administrators to use to manage the TOE.

- O.INSTAL: administrators follow all provided documentation and maintain the security policy.
- O.IDAUTH: users are identified and authenticated prior to accessing any TOE functions.
- O.ACCESS: only authorized users are allowed access to TOE functions and data.
- O.CREDEN: administrators protect all authentication data.
- O.PROTCT: the TOE protects itself from unauthorized access or modification.

8.1.2.4 P.ACCESS

All data collected and produced by the TOE shall only be used for authorized purposes.

This Policy is satisfied by ensuring that:

- O.IDAUTH: users are identified and authenticated prior to accessing any TOE functions.
- O.ACCESS: only authorized users are allowed access to TOE functions and data.
- O.PROTCT: the TOE protects itself from unauthorized access or modification.
- OE.AUDIT_PROTECTION: the IT environment supports this objective by limiting access to audit data.
- OE.SYSTEM_PROTECTION: the IT environment supports this objective by limiting access to IDS system data.

8.1.2.5 P.ACCACT

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

This Policy is satisfied by ensuring that:

- O.AUDITS: all data accesses and uses of TOE functions are audited.
- O.IDAUTH: users are identified and authenticated prior to accessing any TOE functions.
- OE.TIME: user accountability functions that are time dependent have a reliable source of time.

8.1.2.6 P.INTGTY

Data collected and produced by the TOE shall be protected from modification.

This Policy is satisfied by ensuring that:

- O.INTEGR: the integrity of audit and system data is ensured.

8.1.2.7 P. PROTCT

The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

This Policy is satisfied by ensuring that:

- O.OFLOWS: potential audit and system data storage overflows are appropriately handled.
- O.IDAUTH: users are identified and authenticated prior to accessing any TOE functions.
- OE.PHYCAL: the TOE is protected from physical attack.
- OE.PROTECT: the TOE is protected from external interference or tampering.

8.1.3 Complete Coverage – Threats

This section shows that all threats are completely covered by the TOE security objectives and that each objective counters or addresses at least one threat.

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	OE.INSTAL	OE.PHCYAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME	OE.PROTECT
T.COMINT	X						X	X			X							X
T.COMDIS	X						X	X										X
T.LOSSOF	X						X	X			X							
T.NOHALT		X	X	X			X	X										
T.PRIVIL	X						X	X										
T.IMPCON						X	X	X				X						
T.INFLUX									X									
T.FACCNT										X								
T.SCNCFG		X														X		
T.SCNMLC		X																
T.SCNVUL		X																
T.FALACT					X													
T.FALREC				X														
T.FALASC				X														
T.MISUSE			X							X								
T.INADVE			X							X								
T.MISACT			X							X								

8.1.3.1 T.COMINT

An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

This Threat is satisfied by ensuring that:

- O.IDAUTH: users are identified and authenticated prior to accessing any TOE functions.
- O.ACCESS: only authorized users are allowed access to TOE functions and data.
- O.INTEGR: the integrity of audit and system data is ensured.
- O.PROTCT: the TOE protects itself from unauthorized access or modification.
- OE.PROTECT: keeps the TOE security mechanisms from being bypassed.

8.1.3.2 T.COMDIS

An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

This Threat is satisfied by ensuring that:

- O.IDAUTH: users are identified and authenticated prior to accessing any TOE functions.
- O.ACCESS: only authorized users are allowed access to TOE functions and data.
- O.PROTCT: the TOE protects itself from unauthorized access or modification.
- OE.PROTECT: keeps the TOE security mechanisms from being bypassed.

8.1.3.3 T.LOSSOF

An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

This Threat is satisfied by ensuring that:

- O.IDAUTH: users are identified and authenticated prior to accessing any TOE functions.
- O.ACCESS: only authorized users are allowed access to TOE functions and data.
- O.INTEGR: the integrity of audit and system data is ensured.
- O.PROTCT: the TOE protects itself from unauthorized access or modification.

8.1.3.4 T.NOHALT

An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

This Threat is satisfied by ensuring that:

- O.IDAUTH: users are identified and authenticated prior to accessing any TOE functions.
- O.ACCESS: only authorized users are allowed access to TOE functions and data.
- O.IDSCAN, O.IDSENS, and O.IDANLZ: the TOE collect and analyze System data, which includes attempts to halt the TOE.

8.1.3.5 T.PRIVIL

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

This Threat is satisfied by ensuring that:

- O.IDAUTH: users are identified and authenticated prior to accessing any TOE functions.
- O.ACCESS: only authorized users are allowed access to TOE functions and data.
- O.PROTCT: the TOE protects itself from unauthorized access or modification.

8.1.3.6 T.IMPCON

An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

This Threat is satisfied by ensuring that:

- O.EADMIN: the TOE has all the necessary administrator functions to manage the product.
- O.IDAUTH: users are identified and authenticated prior to accessing any TOE functions.
- O.ACCESS: only authorized users are allowed access to TOE functions and data.
- OE.INSTAL: the administrators configure the TOE properly.

8.1.3.7 T.INFLUX

An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

This Threat is satisfied by ensuring that:

- O.OFLOWS: potential audit and system data storage overflows are appropriately handled.

8.1.3.8 T.FACCNT

Unauthorized attempts to access TOE data or security functions may go undetected.

This Threat is satisfied by ensuring that:

- O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.

8.1.3.9 T.SCNCFG

Improper security configuration settings may exist in the IT System the TOE monitors.

This Threat is satisfied by ensuring that:

- O.IDSCAN: the TOE collect and store static configuration information, which could detect a configuration setting change.
- OE.INTROP: the monitored IT System in interoperable with the TOE.

8.1.3.10 T.SCNMLC

Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

This Threat is satisfied by ensuring that:

- O.IDSCAN: the TOE collect and store static configuration information, which could detect the presence of malicious code.

8.1.3.11 T.SCNVUL

Vulnerabilities may exist in the IT System the TOE monitors.

This Threat is satisfied by ensuring that:

- O.IDSCAN: the TOE collect and store static configuration information, which could detect the presence of system vulnerability.

8.1.3.12 T.FALACT

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

This Threat is satisfied by ensuring that:

- O.RESPON: the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

8.1.3.13 T.FALREC

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

This Threat is satisfied by ensuring that:

- O.IDANLZ: the TOE will recognize vulnerabilities or inappropriate activity from a data source.

8.1.3.14 T.FALASC

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

This Threat is satisfied by ensuring that:

- O. IDANLZ: the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

8.1.3.15 T.MISUSE

Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

This Threat is satisfied by ensuring that:

- O.AUDITS and O.IDSENS: the TOE collects audit and sensor data.

8.1.3.16 T.INADVE

Inadvertent activity and access may occur on an IT System the TOE monitors.

This Threat is satisfied by ensuring that:

- O.AUDITS and O.IDSENS: the TOE collects audit and sensor data.

8.1.3.17 T.MISACT

Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

This Threat is satisfied by ensuring that:

- O.AUDITS and O.IDSENS: the TOE collects audit and sensor data.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 3** indicates the requirements that effectively satisfy the individual objectives.

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective(s) that it is intended to satisfy.

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	OE.INSTAL	OE.INTROP	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.TIME	OE.PROTECT	OE.AUDIT_PROTECTION	OE.SYSTEM_PROTECTION
FAU_GEN.1										X										
FAU_SAR.1						X														
FAU_SAR.2							X	X												
FAU_SAR.3						X														
FAU_SEL.1						X				X										

FAU_STG.2a	X						X	X	X		X								
FAU_STG.4									X	X									
FIA_AFL.1								X											
FIA_ATD.1								X											
FIA_UAU.2							X	X											
FIA_UID.2							X	X											
FMT_MOF.1	X						X	X											
FMT_MTD.1	X						X	X			X								
FMT_SMF.1		X	X	X			X	X		X	X								
FMT_SMR.1								X											
FPT_ITT.1	X										X								
FPT_RVM.1a	X																		
FPT_SEP.1a	X																		
IDS_ANL.1 (EXP)				X															
IDS_RCT.1 (EXP)					X														
IDS_RDR.1 (EXP)						X	X	X											
IDS_SDC.1 (EXP)		X	X																
IDS_STG.1a (EXP)	X						X	X	X		X								
IDS_STG.2 (EXP)									X										
IT Environment Security Functional Requirements																			
FAU_STG.2b																		X	
FPT_RVM.1b																	X		
FPT_SEP.1b																	X		
FPT_STM.1																X			
FTP_TRP.1																	X		
IDS_STG.1b (EXP)																			X

Table 3 Objective to Requirement Correspondence

8.2.1.1 O.PROTCT

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

This TOE Security Objective is satisfied by ensuring that:

- The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2a].
- The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1a (EXP)].
- 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 System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1].
- Communications among distributed TOE components is protected from disclosure and modification. [FPT_ITT.1]
- The TOE ensures that the TOE functions cannot be bypassed [FPT_RVM.1a]
- The TOE runs in a process eparate from other user processes and does not provide access to its code and data [FPT_SEP.1a].

8.2.1.2 O.IDSCAN

The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.

This TOE Security Objective is satisfied by ensuring that:

- A System containing a Scanner is required to collect and store static configuration information of an IT System. The type of configuration information collected must be defined in the ST [IDS_SDC.1 (EXP)].
- A System provides functions to allow the management of analyzer data. [FMT_SMF.1].

8.2.1.3 O.IDSENS

The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

This TOE Security Objective is satisfied by ensuring that:

- A System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. These events must be defined in the ST [IDS_SDC.1 (EXP).
- A System provides functions to allow the management of analyzer data and audit functions. [FMT_SMF.1].

8.2.1.4 O.IDANLZ

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).

This TOE Security Objective is satisfied by ensuring that:

- The Analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL.1 (EXP)].
- A System provides functions to allow the management of analyzer data. [FMT_SMF.1].

8.2.1.5 O.RESPON

The TOE must respond appropriately to analytical conclusions.

This TOE Security Objective is satisfied by ensuring that:

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

8.2.1.6 O.EADMIN

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

This TOE Security Objective is satisfied by ensuring that:

- The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1, FAU_SAR.3, FAU_SEL.1].
- The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1 (EXP)].

8.2.1.7 O.ACCESS

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

This TOE Security Objective is satisfied by ensuring that:

- The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2].
- The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1 (EXP)].

- The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2a].
- The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1a (EXP)].
- Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2, FIA_UAU.2].
- 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 System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1].
- A System provides functions to allow the management of audit functions and user accounts. [FMT_SMF.1].

8.2.1.8 O.IDAUTH

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

This TOE Security Objective is satisfied by ensuring that:

- The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2].
- The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1 (EXP)].
- The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2a].
- The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1a (EXP).
- The TOE detects when the configured (non-zero) number of authentication failures occurs and lock the account until cleared by an administrator. [FIA_AFL.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.2, FIA_UAU.2].
- 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 System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1].
- A System provides functions to allow the management of audit functions and user accounts. [FMT_SMF.1].
- The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1].

8.2.1.9 O.OFLOWS

The TOE must appropriately handle potential audit and System data storage overflows.

This TOE Security Objective is satisfied by ensuring that:

- The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2a].
- The TOE must prevent the loss of audit data in the event that its audit trail is full [FAU_STG.4]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1a (EXP)].
- The System must prevent the loss of audit data in the event the its audit trail is full [IDS_STG.2 (EXP)].

8.2.1.10 O.AUDITS

The TOE must record audit records for data accesses and use of the System functions.

This TOE Security Objective is satisfied by ensuring that:

- Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1].
- The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1].
- The TOE must prevent the loss of collected data in the event the its audit trail is full [FAU_STG.4].
- A System provides functions to allow the management of audit functions and user accounts. [FMT_SMF.1].

8.2.1.11 O.INTEGR

The TOE must ensure the integrity of all audit and System data.

This TOE Security Objective is satisfied by ensuring that:

- The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2a].
- The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1a (EXP)].
- Only authorized administrators of the System may query or add audit and System data [FMT_MTD.1].
- A System provides functions to allow the management of audit functions and user accounts. [FMT_SMF.1].
- Communications among distributed TOE components is protected from disclosure and modification. [FPT_ITT.1]

8.2.1.12 OE.TIME

The IT Environment will provide reliable timestamps to the TOE.

This Environment Security Objective is satisfied by ensuring that:

- The TOE IT environment provides a reliable time stamp. [FPT_STM.1]

8.2.1.13 OE.PROTECT

The IT Environment will protect itself and the TOE from external interference or tampering.

This Environment Security Objective is satisfied by ensuring that:

- The TOE IT environment must ensure that communication among TOE components through the environment cannot be disclosed to or modified by unauthorized persons. [FTP_ITT.1]
- The TOE IT environment must ensure that attackers cannot bypass its protections. [FPT_RVM.1b]
- The TOE IT environment must ensure that the TOE is protected from interference and tampering. This can be accomplished by employing the OpenSSL package shipped with the TOE to provide FIPS 140-2 certified SSL protection to network communications among the various parts of the TOE. [FPT_SEP.1b]
- The TOE IT environment must ensure that user authentication data and other TOE data is protected from disclosure during users sessions over uncontrolled networks. [FTP_TRP.1]

8.2.1.14 OE.AUDIT_PROTECTION

The IT Environment will provide the capability to protect audit information.

This Environment Security Objective is satisfied by ensuring that:

- The TOE IT environment is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack from any interfaces made available from the IT environment [FAU_STG.2b].

8.2.1.15 OE.SYSTEM_PROTECTION

The IT Environment will provide the capability to protect System (i.e., IDS) information.

This Environment Security Objective is satisfied by ensuring that:

- The TOE IT environment is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack from any interfaces made available from the IT environment [IDS_STG.1b (EXP)].

8.3 Security Assurance Requirements Rationale

The selected security assurance level is EAL2 augmented with ALC_FLR.3 and AVA_MSU.1.

EAL2 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 System 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.

The base assurance level was augmented with ALC_FLR.3 because flaw remediation procedures provide greater assurance that security-related defects will be fixed. This is an important assurance measure for a widely distributed commercial product.

The base assurance level was augmented with AVA_MSU.1 because clear and complete documentation of all modes of operation of the TOE and the assumptions and requirements for the TOE environment allows the user to deploy the TOE securely and in a manner that best achieves the goals of the organization.

8.4 Strength of Functions Rationale

The TOE minimum strength of function is SOF-basic. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information. This security function is in turn consistent with the security objectives described in Section 4.

8.5 Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satisfied and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1 (IT environment)
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1 and FMT_MTD.1	FAU_GEN.1 and FMT_MTD.1
FAU_STG.2a	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.2a (Hierarchical to FAU_STG.1)
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 (Hierarchical to FIA_UAU.1)
FIA_ATD.1	None	None

FIA_UAU.2	FIA_UID.1	FIA_UID.2 (Hierarchical to FIA_UID.1)
FIA_UID.2	None	None
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2 (Hierarchical to FIA_UID.1)
FPT_ITT.1	None	None
FPT_RVM.1a	None	None
FPT_SEP.1a	None	None
IDS_ANL.1 (EXP)	None	None
IDS_RCT.1 (EXP)	None	None
IDS_RDR.1 (EXP)	None	None
IDS_SDC.1 (EXP)	None	None
IDS_STG.1a (EXP)	None	None
IDS_STG.2 (EXP)	None	None
IT Environment Security Functional Requirements		
FAU_STG.2b	FAU_GEN.1	FAU_GEN.1
FPT_RVM.1b	None	None
FPT_SEP.1b	None	None
FPT_STM.1	None	None
FTP_TRP.1	None	None
IDS_STG.1b (EXP)	None	None

The EAL2 assurance package is defined in the CC to be internally consistent. The dependencies of the EAL2 augmentations specified in this ST (ALC_FLR.3 and AVA_MSU.1) are met as follows:

- ALC_FLR.3 has no dependencies.
- AVA_MSU.1 has dependencies on ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, and AGD_USR.1, all of which are included in the EAL2 assurance package, so they and their indirect dependencies are met.

8.6 Explicitly Stated Requirements Rationale

The IDS class of explicitly stated security functional requirements captures the TOE's basic functionality for collecting system data (IDS_SDC.1 (EXP)), analyzing that data for evidence of intrusions (IDS_ANL.1 (ESP)), reacting and reporting on the analysis results (IDS_RCT.1 (EXP)), and protecting the availability (IDS_STG.1a (EXP)), integrity and confidentiality (IDS_STG.2 (EXP)) of the results. It captures the unique nature of IDS data and provides requirements for collecting, reviewing and managing the data.

The CC contains no security functional requirements that fully describe these requirements, although the audit family of the CC (FAU) was used as a model.

These explicit requirements are specified in the IDSSYPP, to which this ST claims conformance.

These requirements have no dependencies since the stated requirements embody all the necessary security functions.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function, demonstrating that the set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

	Security audit	Identification and authentication	Security management	Protection of the TSF	Intrusion detection system
FAU_GEN.1	X				
FAU_SAR.1	X				
FAU_SAR.2	X				
FAU_SAR.3	X				
FAU_SEL.1	X				
FAU_STG.2a	X				
FAU_STG.4	X				
FIA_AFL.1		X			
FIA_ATD.1		X			
FIA_UAU.2		X			
FIA_UID.2		X			
FMT_MOF.1			X		
FMT_MTD.1			X		
FMT_SMF.1			X		
FMT_SMR.1			X		
FPT_ITT.1				X	
FPT_RVM.1a				X	
FPT_SEP.1a				X	
IDS_ANL.1 (EXP)					X
IDS_RCT.1 (EXP)					X
IDS_RDR.1 (EXP)					X
IDS_SDC.1 (EXP)					X
IDS_STG.1a (EXP)					X
IDS_STG.2 (EXP)					X

Table 4 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.