Tenable Network Security, Inc.
Tenable SecurityCenter 4 and Components

Security Target
Version 1.0

September 13, 2012

Prepared by:

Tenable Network Security, Inc.

7063 Columbia Gateway Drive, Suite 100
Columbia, MD 21046

Prepared For:

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 SecurityCenter 4 and Components. It consists of the Tenable SecurityCenter 4.4 (SC4), 3D Tool 2.0.1 (3DT), Log Correlation Engine 3.6.1 (LCE), Passive Vulnerability Scanner 3.6 for Linux/Unix and Windows (PVS), Nessus vulnerability scanner 5.0.1 (Nessus), and xTool 2.1. The TOE consists of six (6) distinct products and the evaluated configuration includes all of the Tenable products working in unison. 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 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 Claims**
This section presents any protection profile claims.

Section 8 **Rationale**
This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – Tenable Network Security, Inc. Tenable SecurityCenter 4 and Components Security Target

ST Version – Version 1.0

ST Date – September 13, 2012

TOE Identification – Tenable SecurityCenter 4 and Components. The TOE consists of: Tenable SecurityCenter 4.4 plus Components: 3D Tool 2.0.1 (3DT); Log Correlation Engine 3.6.1 (LCE); Passive Vulnerability Scanner 3.6 for Linux/Unix and Windows (PVS); Nessus Scanner 5.0.1 (Nessus), and xTool 2.1.

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

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 3.1 Revision 3, July 2009.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 3.1 Revision 3, July 2009.
  - Part 3 Conformant
  - Assurance Level: EAL2 augmented with ALC_FLR.2.
- This TOE is conformant to the following Protection Profile (PP):
  - Intrusion Detection System System Protection Profile (IDSSYPP), Version 1.7, July 25, 2007

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 are applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that can be applied to functional requirements: assignment, selection and refinement.
  - 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 "**(EXT)**".
- 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 2.0.1
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 1.7, July 25, 2007.
IP	Internet Protocol
IT	Information Technology
ITT	Internal TOE TSF Data Transfer family of FPT
LCE	Log Correlation Engine 3.6.1
MGR	Manager (a TOE role)
NASL	Nessus Attack Scripting Language
NIAP	National Information Assurance Partnership
NIDS	Network IDS
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OH	Organizational Head (a TOE role)
OS	Operating System
PKI	Public Key Infrastructure
PP	Protection Profile
PVS	Passive Vulnerability Scanner 3.6 for Linux/Unix and Windows
SA	System Administrator (a TOE environment role)
SAIC	Science Applications International Corporation
SAR	Security Assurance Requirement
SC4	Security Center 4.4
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 Overview

The Target of Evaluation (TOE) is Tenable SecurityCenter 4 (SC4) and Components: SecurityCenter 4.4, 3D Tool 2.0.1 (3DT), Log Correlation Engine 3.6.1 (LCE), Passive Vulnerability Scanner 3.6 for Linux / Unix and Windows (PVS), Nessus scanner 5.0.1 (Nessus), and xTool 2.1. The TOE consists of only these six Tenable products, as shown in the Figure 1. The configuration of the TOE subject to evaluation consists of a single SC4 and at least one instance each of the Nessus, PVS, LCE, 3DT and xTool 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).

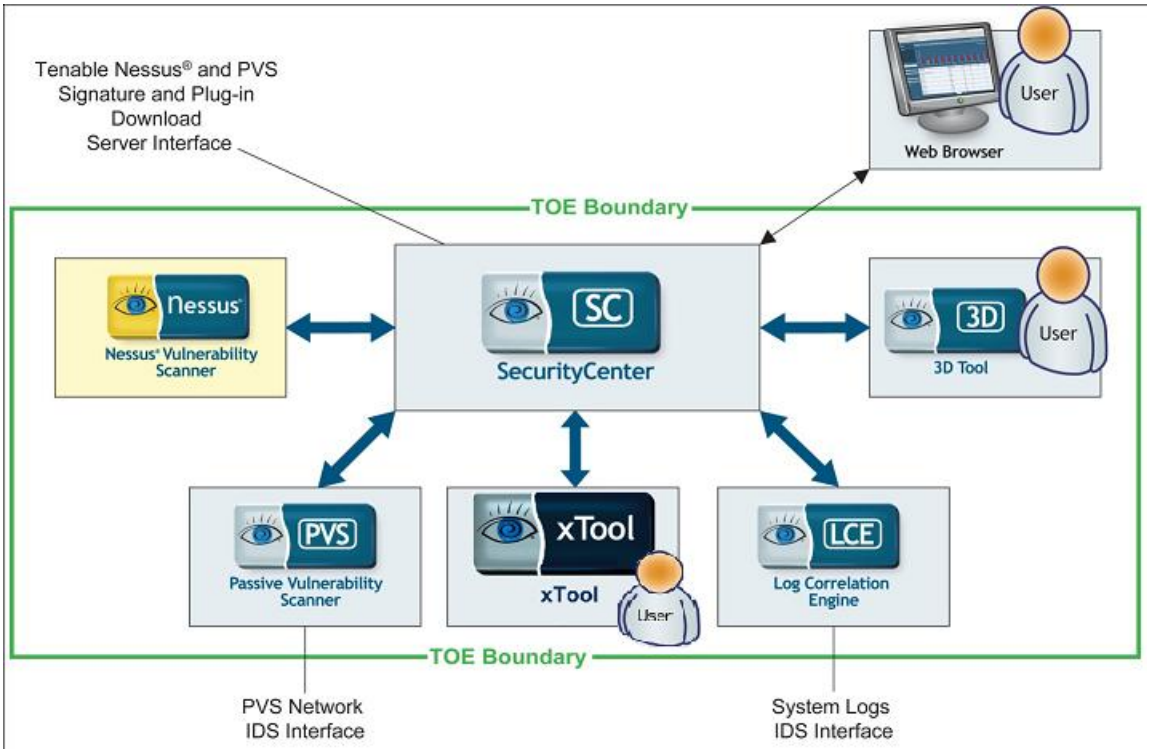

Tenable Nessus® and PVS Signature and Plug-in Download Server Interface
User
Web Browser
TOE Boundary
Nessus
Nessus® Vulnerability Scanner
SC
SecurityCenter
3D
User
3D Tool
PVS
Passive Vulnerability Scanner
xTool
xTool
User
LCE
Log Correlation Engine
TOE Boundary
PVS Network IDS Interface
System Logs IDS Interface

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:

Passive Network IDS Interface – Interface to monitored networks to passively collect vulnerability 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.

Nessus Scanner Interface – Interface to monitored networks to actively collect vulnerability information.

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

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

3DT User Interface – User interface to SC4 using 3DT for an enhanced view of topology and vulnerability data.

xTool User Interface – User interface to xTool for conversion of XML data files to .audit file formats used by SC4.

Web Browser User Interface – User interface to SC4 using a standard web browser with an SSL connection.

Note that in theory, Nessus can be used independently of SC. The other components, including PVS and LCE, are also optional components to the SC. It is assumed that all components will be configured and managed by SC and any independent interfaces would not be used. Rather, SC4 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
- 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 plugins (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 databases used by SC and the LCE. 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 six components shown above configured as an intrusion and vulnerability detection system. The SC4 component collects 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. The xTool has the ability to produce audit files for use by SC4 via Nessus scanning. This fits the IDS System structure specified in the IDSSYPP, to which this ST claims conformance, as follows:

- IDS Analyzer: SC4 with LCE and 3DT.
- IDS Scanner: Nessus.
- IDS Sensor: PVS.

xTool audit files are generated for use by SecurityCenter, but the underlying operating system on which the xTool runs is responsible for the audit file upload function. xTool is able to query repositories and scan results in SC4; to do so, it authenticates to SecurityCenter over SSL on TCP port 443 using valid SecurityCenter user credentials with permissions to perform such queries.

The TOE consists of the six software components (SC4, LCE, PVS, 3DT, Nessus, and xTool) 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 SC4 component is able to interface with additional third-party generators of IDS event data, but that capability is not tested in this evaluation.

2.1 TOE Description

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

2.1.1 Tenable SecurityCenter (SC4)

Tenable's SecurityCenter 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 SC4, operating in conjunction with the other TOE components further described below, include[1]:

- ***Risk management:*** SC4 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:*** LCE 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****:* SC4 allows combining the knowledge of existing asset inventories with the vulnerability and compliance information discovered by Nessus and the PVS. SC4 performs asset discovery with active and passive vulnerability scanners. Resources are classified by type, location and description. It also performs vulnerability reporting, remediation and false positive management by asset type.

- ***Workflow management:*** SC4 includes a ticketing and workflow system. Vulnerability and compliance issues can have a ticket opened against them. Tickets can be opened for 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 their severity level. SC4 also determines what users should receive notification of new tickets.

- ***Executive reporting****:* SC4 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****:* SC4 configuration requirements are minimal, requiring slight learning curves and simple training requirements. Full-time passive scanning by the PVS has no direct network visibility though the impact on network performance. Distributed active scanning by Nessus has minimal network impact. Users interact with the TOE via a web interface and all data stays within the host network boundaries.

The SC4 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. SC4 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. SC4 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.

The LCE receives Intrusion Detection System (IDS) events from multiple sources. It analyzes the event data against the SC4 vulnerability database to determine whether the target of an event is vulnerable to the attack. If it is, SC4 reports the information to the relevant system administrators and (optionally) to users via e-mail. SC4 includes a set of common audit guides created by Tenable for use in various government, financial and health care compliance audits. SC4 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

[1] Note that since SC4 serves to consolidate and present a unified view of the available functions regardless of supporting components, there has been no attempt to distinguish the functions, or aspects thereof, specifically implemented by the SC4 component from the functions made accessible via SC4.

[2] Note that each component generates alerts independently relative to the events they process. For the most part, Nessus and PVS present their results to the other TOE components. LCE TASL scripts can be defined to issue alerts and SC4 can issue alerts based on normalized data that it receives.

inform system owners of their required actions (i.e., disabling an unauthorized service) and how long it took to close an issue.

The LCE performs IDS event correlation. It can send alerts to designated, authorized SC4 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 to that specific attack. Further, PVS can be configured to detect both an encrypted or cleartext interactive session and to identify sessions by IP address, port and network protocol.

For more accurate vulnerability to IDS event correlation , SC4 should be configured to synchronize with the latest rules engine (as described on pages 15 and 16 of the SecurityCenter 4.4 Administration Guide) and have the latest vulnerability information as possible. If scans are not being performed often enough, 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.

SecurityCenter stores all of its vulnerability and intrusion data into highly optimized, proprietary-format binary files. Other data, such as organization and user data, are stored in an indexed SQLite format. SC operates one daemon, **Jobd** (Job Scheduler), and issues commands via XML-RPC over SSL to Nessus scanners. When SC launches a scan, the XML-RPC commands perform the necessary functions for scan distribution and results aggregation. When new vulnerability checks are available, XML-RPC commands are also used to determine if scanner plugins are updated and initiate a "push" of updates from SecurityCenter out to the remote scanners. In addition to Nessus, commands are also used via SSL to connect to one or more Tenable PVS servers.

The **Jobd** process manages the scheduling of all system tasks such as launching vulnerability scans, sending email, importing vulnerability information, generating reports and new IDS signature and Nessus plugin downloads.

SC sends all email through an external SMTP server. The administrator user configures the desired SMTP settings including hostname, port, authentication method, secure connection and return address and the **Jobd** scheduler kicks off the email process as necessary. Multiple forms of authenticated email are supported and many types of emails can be sent such as attack alerts, text results of new vulnerability scans and scheduled PDF reports. The SC does not have a daemon listening for incoming email.

An Apache web server is included in the product distribution but is not part of the TOE. Only the version of Apache provided with the SecurityCenter product installation is supported by Tenable and must be used in the TOE environment to provide and protect secure user and administration interfaces.

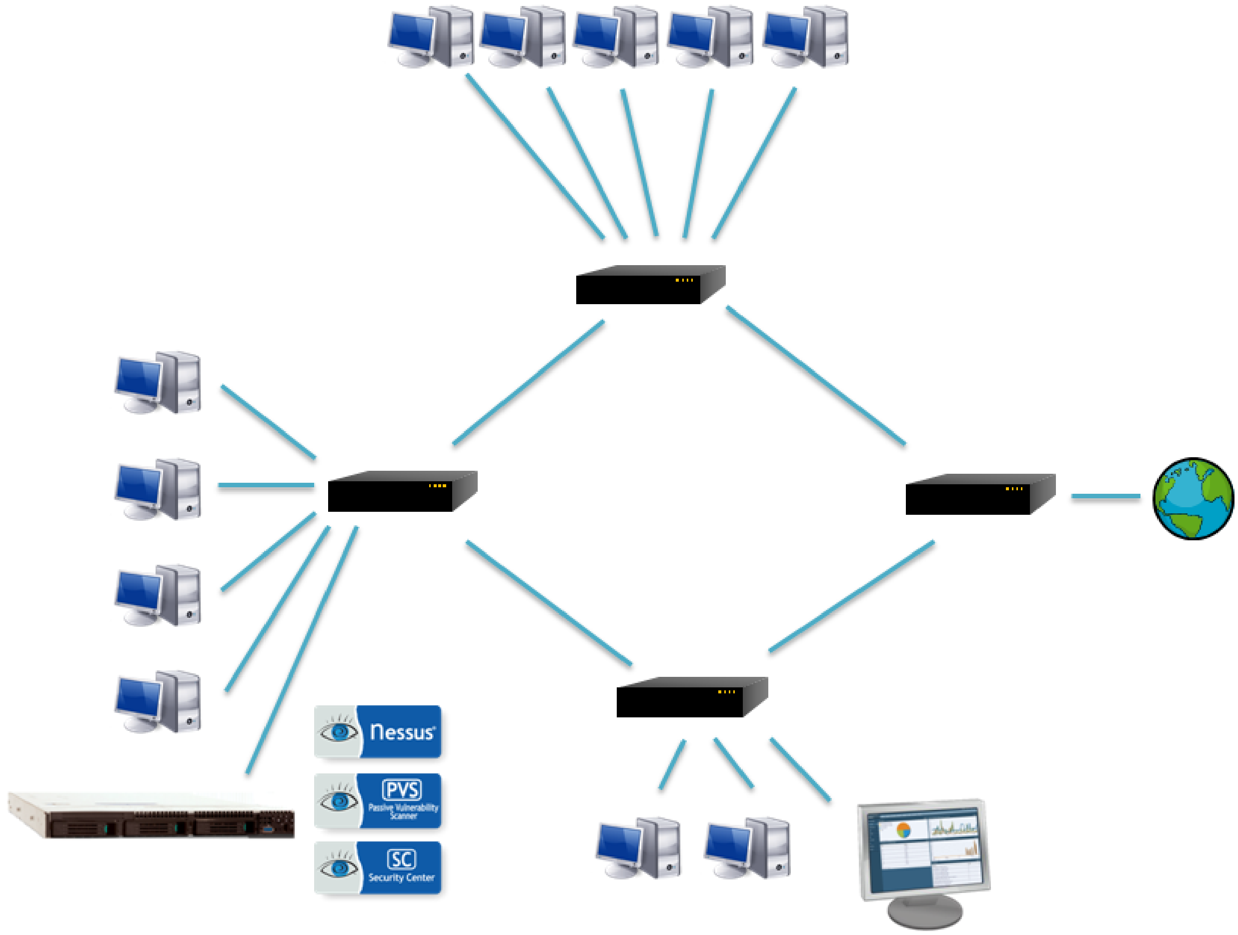
SC4 stores vulnerability data in proprietary format binary files, while organization and user data is stored in SQLite database files. SC4 uses Secure Shell (SSH) to make LCE queries and Secure Copy (SCP) to transfer raw log files from the LCE to SC4. All reporting and data analysis is performed remotely by the LCE and presented to the user by the SC4. If the LCE discovers an anomaly or a specific type of event correlation, it sends an alert to the SC4.

The LCE can receive events directly from IDS sensors using SYSLOG and Simple Network Management Protocol (SNMP) protocols. SC4 is configured to receive IDS signature updates via direct or proxied 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. These signatures are pushed out to the corresponding LCE servers for IDS event correlation. Correlation of event signatures from the various sensors is performed by matching Common Vulnerabilities and Exposures (CVE) (http://cve.mitre.org/) and Bugtraq (http://www.securityfocus.com/bid/) IDs with Tenable Nessus and PVS plugin information. SC4 also provides optional web-based reporting and analytical functions. SC4 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 several known vulnerability databases. Dynamic asset lists can be augmented with existing static asset lists collected externally to the SC4.

Although the TOE also supports a single scanner configuration (i.e., SC4 and Nessus), the evaluated configuration of the TOE is for a multiple scanner configuration.

For small networks (e.g., a few Class C networks), all of the vulnerability assessment components of the SecurityCenter can be installed on a single server. When installed on a single server, the primary processes that will be running and active include **`nessusd`** (Nessus), **`pvs`**, **`pvs-proxy`**, and **`pvs-proxy-service.exe`** (PVS), **`Jobd`** (SC) and **`httpd`** (SC). These processes are "always-on", while there are others that run "on demand" at various times.

XML-RPC commands from SC manage the results from the Nessus daemon. The Nessus server runs the Nessus daemon on TCP port 8834. The server will also typically run the Apache web server on TCP port 443, as well as SSH on TCP port 22.



SecurityCenter, Nessus and PVS installed on a single server

This configuration supports multiple organizations and can conduct and store scans for a fairly large group of users. It does not, however, take advantage of more than one Nessus or passive scanner. In addition, it does not make use of the event processing of the LCE.

Depending on the size of the scanned network, it may suffer performance problems while conducting a scan. For example, when no scans are occurring, the Apache web server has a majority of the system resources to provide fast responses to user queries about the current network vulnerabilities. However, when a scan is occurring, the scan daemon will consume a noticeable amount of system resources. A dual CPU system will help, but placing the scan daemon(s) on a separate system is the best way to limit the impact to SecurityCenter.

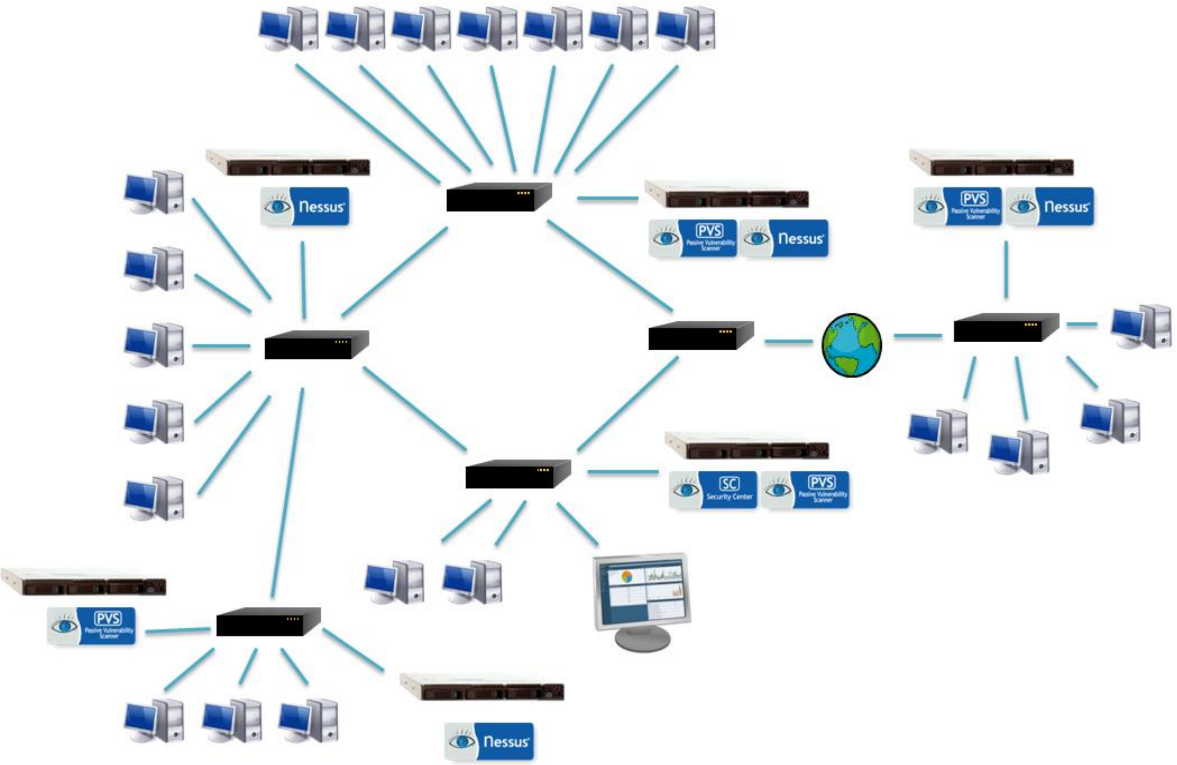
All functionality of SecurityCenter is available, even though only one server is being used. Nessus network scans can be scheduled as often as desired, with or without credentials. One or more SecurityCenter users can be created, each with different roles and data access. Reports can be scheduled and so on. The only functionality lost with a single server architecture is load balanced scanning or any type of scan that required multiple scanners.

SecurityCenter users employ their web browser to access their security information. These users can be within the network, coming across a VPN or anywhere else they have network access.

Multiple Scanner Architecture

Expanding the above architecture, multiple Nessus and PVS systems can be added for each Class C subnet to be scanned. To add these devices to SecurityCenter, they should first be installed in their desired locations and then entered into the SecurityCenter configuration by the administrator.

In the diagram below, SecurityCenter is deployed on a server in the lower right and multiple Nessus scanners are deployed across the small network. The icons show four PVS systems deployed on various network links.


Nessus
PVS Passive Vulnerability Scanner
Nessus
PVS Passive Vulnerability Scanner
Nessus
SC Security Center
PVS Passive Vulnerability Scanner
PVS Passive Vulnerability Scanner
Nessus

SecurityCenter and multiple Nessus/Passive Vulnerability scanners

In this configuration, when an active scan occurs, the targets get split up between the active scanners. During active scans, the CPU usage on the SecurityCenter server is very minimal. When all scanning is performed by remote Nessus scanners, the overhead from using XML-RPC commands to the Nessus scanners is minimal.

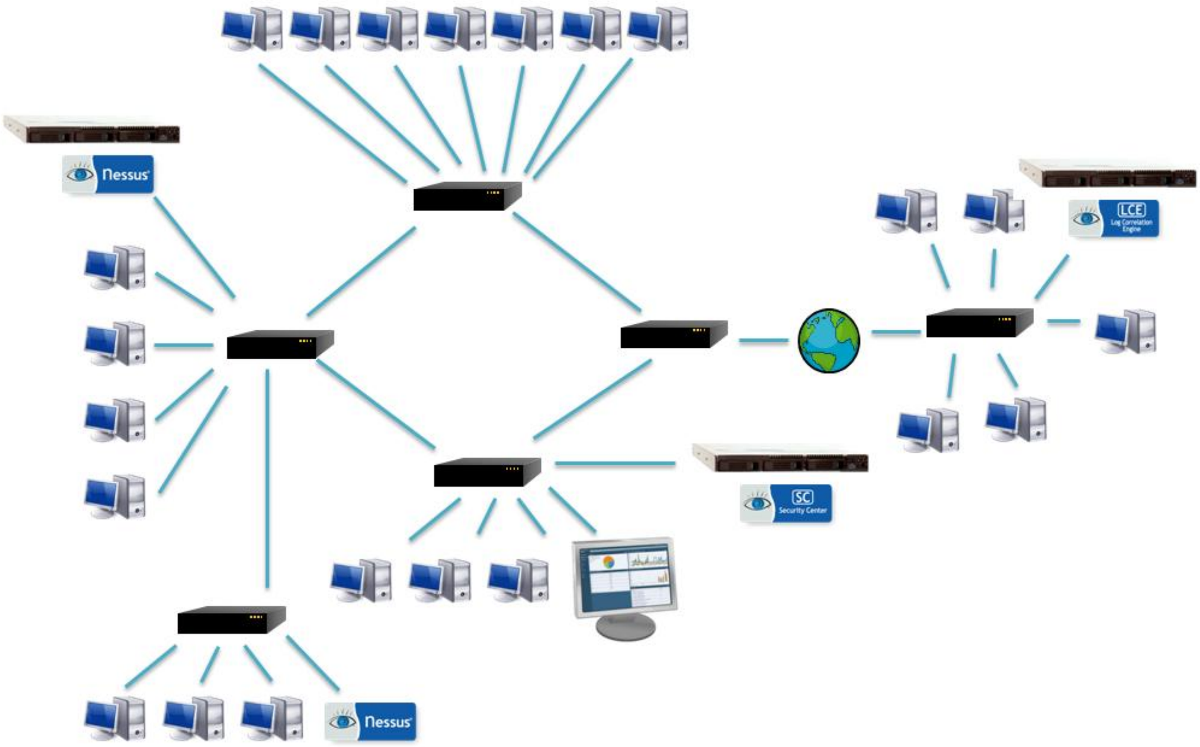
Since multiple scanners with different processors are used to conduct scans, the scans finish more rapidly than using a single scanner. Console users will not see a difference in the vulnerabilities reported, but they will see much less network impact and their scans will complete several times faster than previous scans.

Vulnerability data from PVS is handled differently. Since it is running 24x7, it is configured to record vulnerability data and send it to SecurityCenter once an hour by default. SecurityCenter will save any passive vulnerability data for 7 days by default. Vulnerability data from a PVS automatically shows up on SecurityCenter and populates its knowledge of network vulnerabilities.

With this distributed architecture, the Nessus scanners can also be used to target networks other than what they scan for by default. In the above network, each Nessus scanner would have been associated with their default target networks and this is called a “zone”. SecurityCenter scans can be configured to override default zones and ask, for example, the Nessus scanner in the upper portion of the network, to scan the network segment on the bottom. This type of “zone” scanning allows for testing of firewall policies and exercising network IDS sensors.

Single Log Correlation Engine Architecture

SecurityCenter capability can be extended with one or more LCEs. This engine can be deployed either on the same or a separate server and can receive logs from many different devices including IDS/IPS devices. All logs are sent to the LCE and very little data is sent back to SecurityCenter.



Example SecurityCenter and Log Correlation Engine

In the above network diagram, the SecurityCenter and the single LCE are placed on two different servers.

Although not shown, dozens of LCE agents can be placed on key servers and at network choke points to aggregate as many logs as possible. The agents would connect back over TCP port 31300 to the LCE. Devices that can generate SYSLOG messages can also be sent to the LCE. This SYSLOG data can also include IDS data from a wide variety of intrusion detection devices. Other supported protocols include SNMP, SDEE, RDEP, and OPSEC.

SecurityCenter communicates with the LCE through secure SSH and SCP connections. All reporting and data analysis is presented through the SecurityCenter UI, but performed remotely by the LCE. If the LCE discovers an anomaly or a specific type of event correlation, it can send a message to SecurityCenter that treats the alert as if it came from an intrusion detection device.

SecurityCenter users can analyze any normalized log and correlated events obtained by the LCE with the same rights the user has to look at vulnerabilities. Users with the appropriate role-based permissions automatically have this access.

Multiple Log Correlation Engine Architecture

SecurityCenter can make use of more than one LCE. A single SecurityCenter can have as many organizations as desired. Each organization can also have its own LCE.

From the SecurityCenter's point of view, it really does not matter how each remote LCE is configured. One LCE could be focused completely on long-term NetFlow monitoring, another on firewall logs and another on application logs from Exchange, the SQL farm and the Citrix server.

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 SecurityCenter account to access the data. Its only form of communication with SecurityCenter is via an SSL communication path. During 3DT configuration with a SecurityCenter, after clicking "Test Login" for the first time, a certificate warning is displayed for the remote SecurityCenter. If the remote host is known and trusted, the warning is acknowledged to perform the login. Users launch the 3DT tool, establish an SSL connection with SecurityCenter and then authenticate to the SecurityCenter through a valid SecurityCenter user account. It supports three reporting modes: node traits, connections and counts. 3DT users can make one or more queries to populate the 3DT data 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 SecurityCenter, allowing the centralization of log analysis and vulnerability management.

Each SecurityCenter 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. SecurityCenter users see only the LCE events they are authorized to see.

The LCE implements a SYSLOG interface that it uses 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 sent to SC4, the data is normalized and forwarded. The LCE enables the SecurityCenter to perform high-speed analysis and reporting for many types of events.

The LCE includes an event scripting language, based on Tenable's 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 SC4 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 SC4. SC4 can be extended with one or more LCEs. The LCE can run on a separate server from the SC4. 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 SC4. The SC4 monitors the status of each LCE server attached to it so that any system failure can be quickly investigated.

LCE includes client agents for Unix, Windows, NetFlow, OPSEC, RDEP/SDEE 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. The LCE's default behavior is to monitor each host with a client, including 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.

In the evaluated configuration, the LCE is configured such that it is used only via the SC4. In relation to the evaluated configuration, the LCE GUI may not be used for regular operational activities in the role of a TOE component.

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
-
- 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

SC4 fuses this information with the active or credentialed scan results from Tenable's Nessus vulnerability scanner. Note that the period of PVS logging is configured and SC4 gets the available data when it connects for that purpose. As such, PVS and SC4 should be coordinated appropriately. SC4 communication is facilitated via a proxy enabling the use of web-based SSL interactions. When a credentialed 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 or other traffic and sniffs out vulnerabilities from network session traffic. Most protocols carry internal version and identity information.

PVS includes a scripting language called PASL, which stands for the "Passive Analysis Scripting Language" and is a library based on TASL (the Tenable application scripting language) and NASL (the scripting language used for Nessus vulnerability scanner scripts), but independent from the Nessus backend. The format is similar to that used for writing NASLs for the Nessus vulnerability scanner, making it easier for those familiar with writing NASLs to write event correlation algorithms for events in the LCE. Specifically, PASL contains all functionality of TASL, along with all knowledgebase features of NASL.

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) and 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 SC4 and LCE. Similarly, while the PVS can be configured to forward vulnerability and alert data via SYSLOG to non-TOE components, this capability is disabled in the evaluated configuration. If the PVS is being used as a vulnerability source, it can be configured to send its data directly to the SC4. Once the vulnerability data is on the SC4, it is pushed down to the LCE for correlation. If PVS is being used as a pseudo IDS source, it can be configured to send its data directly to the LCE for correlation that can be accessed on demand from the SC4.

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.

In the evaluated configuration, the PVS is configured such that it is used only via SC4. In relation to the evaluated configuration, the PVS CLI is only used for initial installation and configuration of the product and for any technical support issues where use of the CLI is required for failure recovery. The PVS CLI may not be used for regular operational activities in the role of a TOE component.

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 SC4, 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), SSH netstat, WMI netstat, SNMP and 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 architecture has the flexibility to deploy the scanner 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):*** Providing target system credentials to Nessus will allow it to find local information from a remote host. 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 48,000 plugins, each of which checks for one or more unique vulnerabilities across dozens of operating systems and hundreds of different software packages and provides scan results based on these checks. Plugins are organized into families for convenience and optimizing scans. While this evaluation addresses whether specific Nessus plugins can be selected and exercised, the evaluation does not determine the efficacy of any one specific plugin or plugin family.

The administrator can opt to enable all security checks or to enable all security checks except the checks that are potentially harmful. 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. The severity ratings are derived from the associated CVSS score, where less than 5 is "Low", less than 7 is "Medium", 10 or less is "High" and a CVSS score of 10 can be flagged as "Critical" if so desired. Nessus security reports can be displayed as a new web browser instance. All reports are archived and available for later viewing, printing or comparing with other reports.

Nessus can save all of its vulnerability data in various file formats (notably XML and HTML). 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 on 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 NESSUS, HTML and TXT formats.

In the evaluated configuration, Nessus is configured such that it is used only via SC4. As such, SC4 utilizes the Nessus CLI and references to the administrator, as stated above, apply to the SC4 administrator and not a Nessus-specific role. In relation to the evaluated configuration, the Nessus CLI is only used for initial installation and configuration of the product and for any technical support issues where use of the CLI is required for failure recovery. The Nessus CLI and the Nessus Server Manager GUI (an additional server management interface) may not be used for regular operational activities in the role of a TOE component. 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 SC4 for the purpose of interacting with the Nessus component(s).

2.1.6 xTool

Tenable designed the xTool to work with the official XCCDF Tier IV content used in the FDCC program. Beta quality XCCDF-compliant content (Tier 3 and below) is also available from NIST. SecurityCenter users can obtain the various SCAP bundles at http://nvd.nist.gov/fdcc/download_fdcc.cfm . Bundles can be downloaded collectively as a single .zip archive, or separately based on SCAP bundle types (IE 7, Vista, Windows XP, Vista Firewall, XP Firewall, Windows 7, Windows 7 Firewall, IE8). The xTool is capable of generating .audit files from XCCDF and OVAL content, and can also convert .nessus report files to XCCDF and OVAL output.

In the evaluated configuration, xTool is configured on a Windows operating system and can authenticate to SecurityCenter for queries over SSL on TCP port 443. Its only form of communication with SecurityCenter is via an SSL communication path. During xTool configuration with a SecurityCenter, after clicking "Test Login" for the first time, a certificate warning is displayed for the remote SecurityCenter. If the remote host is known and trusted, the warning is acknowledged to perform the login. Audit files or output files are generated by xTool, but the underlying operating system is solely responsible for the upload of all files to SecurityCenter for use in configuration auditing.

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:

- SC4 – Tenable SecurityCenter 4.4
- 3DT – 3D Tool 2.0.1
- LCE – Log Correlation Engine 3.6.1
- PVS – Passive Vulnerability Scanner 3.6 for Linux/Unix and Windows
- Nessus – Nessus Scanner 5.0.1
- xTool – xTool 2.1

Each bulleted item is licensed separately, except for the 3DT and xTool, which do not require a license. 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 (SecurityCenter, 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 SC4

SC4 consists of the Tenable SecurityCenter 4.4 software component.

SecurityCenter 4 is available for Red Hat Enterprise Server 4 (32-bit only), 5 and 6 (32/64-bit). CentOS 5.3 (32/64-bit) is also officially supported. It must be configured with a Fully Qualified Domain Name (FQDN).

SC4 installation requirements:

Scenario	Recommended Hardware
SC4 and Nessus Scanner 5.0.1 managing 500 to 2,500 active IPs	**CPU:** 1 dual-core 2 GHz or greater CPU **Memory:** 2 GB RAM (4GB RAM recommended) **Hard drive:** 80 GB at 7,200 rpm (160 GB at 10,000 rpm recommended)
SC4 managing 2,500 to 10,000 active IPs	**CPU:** 1 dual-core 3 GHz CPU (2 dual-core recommended) **Memory:** 4 GB RAM (6 GB RAM recommended) **Hard drive:** 80 GB at 10,000 rpm (160 GB at 10,000 rpm recommended)
SC4 managing 10,000-25,000 IPs	**CPU:** 2 dual-core 3 GHz CPU (1 quad-core recommended) **Memory:** 6 GB RAM (8 GB RAM recommended) **Hard drive:** 160 GB at 10,000 rpm (250 GB at 15,000 rpm with striped RAID recommended)
SC4 managing more than 25,000 active IPs	**CPU:** 2 dual-core 3 GHz CPU (4 dual-core recommended or 2 quad-core 3GHz CPU) **Memory:** 8 GB RAM (12 GB RAM recommended) **Hard drive:** 250 GB at 15,000 rpm (500 GB at 15,000 rpm with striped RAID recommended)

2.2.1.2 3DT

3DT consists of the Tenable 3D Tool 2.0.1 software component.

3DT is supported for installation on the following platforms: Windows 2000, Windows Server 2003, Windows 2008, Windows XP Professional, Windows Vista, and Windows 7.

2.2.1.3 PVS

PVS is the Tenable Passive Vulnerability Scanner 3.6 software component, which can be installed on Red Hat Linux ES4, ES5, and ES6 (32-bit and 64-bit), and CentOS 5 and 6 (32-bit and 64-bit), Windows XP Professional, Windows Server 2003, Windows Server 2008, Windows Vista and Windows 7. 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:

Scenario	Recommended Hardware
Passive Vulnerability Scanner managing 20,000-50,000 hosts	CPU: 1 single-core 2 GHz CPU Memory: 2 GB RAM (4 GB RAM recommended) HDD: 72 GB at 7,200 rpm (72 GB at 10,000 rpm recommended)
Passive Vulnerability Scanner managing in excess of 50,000 hosts	CPU: 1 dual-core 3 GHz CPU (2 dual-core recommended) Memory: 2 GB RAM (4 GB RAM recommended) HDD: 72 GB at 10,000 rpm (72 GB at 15,000 rpm recommended)

2.2.1.4 LCE

LCE consists of the Tenable Log Correlation Engine 3.6.1 software component. The server component is supported for installation on the following platforms: Red Hat Linux ES3, ES4, ES5 for 32-bit platforms (4.x and 5.x for 64-bit platforms).

Number of Events	Recommended Memory Size
<2 million	1 GB
2-10 million	2 GB
10-50 million	4 GB
50-80 million	8 GB
90+ million	16 GB

Number of Events	Recommended CPU
<1 million	1 single-core 3 GHz CPU
1-2 million	1 single-core 3 GHz CPU (10,000 rpm disk recommended)
2-10 million	1 dual-core 3 GHz CPU (15,000 rpm disk recommended)
10-50 million	2 single-core 3 GHz CPU (striped RAID disk is recommended)
50-80 million	2 dual-core 3 GHz CPU (striped RAID disk is recommended)
90+ million	4 dual-core 3 GHz CPU (striped RAID disk is recommended)

2.2.1.5 Nessus

Nessus server includes the Nessus Scanner 5.0.1 software component. It is supported for installation on the following Windows, Unix and Unix-like systems:

- Windows: Windows XP, Server 2003, Server 2008, Server 2008 R2, Vista and Windows 7 (i386 and x86-64).
- Unix:FreeBSD 9 (i386 and x86-64)
- Unix-like:
  - Debian 6 (i386 and x86-64)
  - Fedora Core 16 (i386 and x86-64)
  - Mac 10.6 and 10.7 (i386, x86-64, ppc)
  - Oracle Linux 5 (i386 and x86-64)
  - Red Hat ES 4 / CentOS 4 (i386)
  - Red Hat ES 5 / CentOS 5 (i386 and x86-64)
  - Red Hat ES 6 / CentOS 6 (i386 and x86-64) [Server, Desktop, Workstation]
  - SuSE 10(x86-64) and 11 (i386 and x86-64)
  - Ubuntu 8.04 , 9.10, 10.04, 10.10, and 11.10 (i386 and x86-64)

2.2.1.6 xTool

xTool consists of the xTool 2.1 software component.

xTool is supported for installation on the following platforms: Windows Server 2003, Windows 2008, Windows XP Professional, Windows Vista, and Windows 7.

2.2.2 TOE Logical Boundaries

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

The following features are exclusions, assumptions, or configuration restrictions in the TOE evaluated configuration:

- Assumption: The evaluated configuration requires at least one instance of each identified TOE component. Rationale: *This is necessary in order to evaluate the interaction between the TOE and all associated components*.
- Exclusion: Use of Nessus, PVS or LCE components directly rather than via the SC4 interfaces is excluded from the evaluated configuration. Rationale: *This is necessary in order to evaluate the communications between the TOE and all associated components.*
- Exclusion: Use of third party authentication servers, such as LDAP, is not allowed in the evaluated configuration. Rationale: *The TOE provides its own means of authentication and the PP requires the TOE to perform authentication.*
- Exclusion: Custom roles are unique to each individual Organization and thus are excluded from the evaluated configuration. Rationale: *Custom roles are not pre-defined within the TOE and thus are outside of the scope of the PP.*
- Configuration restriction: Exporting data (from any TOE component) via SYSLOG outside the TOE is not allowed in the evaluated configuration. Rationale: *Monitoring data and functions outside of the TOE is outside the scope of the PP.*
- Exclusion: The LCE clients that operate within non-TOE components have not been subject to the evaluation. *Rationale: 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.*

- Exclusion: The PVS's inability to interfere with network traffic has not been subject to the evaluation. Rationale: *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 does not 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 (EXT) and IDS_ANL.1 (EXT) 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 SC4 GUI that is used by authorized system administrators to read the audit trail and to sort audit data. Authorized system administrators are also able to sort through audit data using operating system command such as 'grep', 'awk', and 'sed'. The TOE restricts access to the audit trail to authorized system administrators. When SC4 audit logs are sent to the LCE, specific audit events can be selected for viewing by the SC4 Analysis Tool's "Raw Syslog Data" option through the configuration of a built-in PRM file.

The TOE installation guides advise the systems administrator how to configure and manage the TOE security audit storage so that storage exhaustion is prevented. Depending on settings, if audit trail storage becomes exhausted, the TOE will prevent auditable events, except those taken by a system administrator with administrative privileges on the TOE system.

All systems running TOE components must have the LCE client installed and configured to send event data to the LCE server with the system_monitor.tasl script installed. This script will generate an alert if system resources (memory, disk, CPU) reach a specified threshold that could negatively impact TOE performance. Should these alerts be ignored and systems resources become exhausted, individual TOE component functionality may be adversely affected.

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 SC4 provides a web-based logon and users must be successfully identified and authenticated prior to accessing this information.

2.2.2.3 Security Management

SC4 restricts the ability to manage functions based on the user role. The predefined roles supported by the SC4 are SecurityCenter Administrator (SCA), Organization Head (OH), Manager 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 multiple 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 SecurityCenter 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 SC4 administration tasks to the Information Security group. If the business unit is an Organization Head or Organization, an Information Security Officer in the business unit may be responsible for all security functions within that unit and would serve as the Manager for that business unit. A large organization might have multiple Managers or Organization Heads depending on Organizational units.

Within the business units, End Users may be designated. These End Users are managed by the unit's 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 SC4 component provides the tools necessary to define users and configure access.

SC4integrates repositories of vulnerability data that are shared as needed among users and organizations based on manager-defined assets. The use of repositories allows for scalable and configurable data storage for organizations. Repositories can also be shared between multiple SecurityCenters. Repositories are configured by the administrative user and made available to the Organization Head to assign to users as needed.

There are three types of repositories: “Local”, “Remote” and “Offline”. Local repositories are active repositories of SC4 data collected via scanners attached to the local SC4. Remote repositories contain IP address and vulnerability information obtained via network synchronization with a second (remote) SC4. Offline repositories enable SC4 to obtain repository data via manual export/import from a remote SecurityCenter that is not network-accessible. If separation of data is required between two different organizations, separate repositories assigned to each organization is used for access control. The underlying operating system limits access to the “tns” user but the SC4 product actually performs access control on its users.

A description of the roles supported by the SecurityCenter follows:

Security Center Administrator (SCA)

The SecurityCenter Administrator role is able to configure and manage the SC4 application. No access to the underlying operating system platform is required. All functions can be performed through the SC4 GUI. The SCA defines and manages organizations, specifying which network ranges within which network traffic may be monitored for each Organization. Each Organization has a unique name and serial number. There are three Organization roles: the Organization Head, Manager and End User.

The SecurityCenter Administrator’s role includes performing the following functions:

- Manage the SecurityCenter
- Managing SecurityCenter Organization Accounts
- Managing SecurityCenter Components
- Monitoring SecurityCenter Audit Logs

The SecurityCenter Administrator (SCA) cannot access Organization data nor initiate IDS scans.

Organization Head (OH)

The Organization Head (OH) has full rights for the entire network space of an organization and cannot be deleted without removing the entire organization entry. The Organization Head may define additional users for the address space as either Managers, End Users or custom roles. The Organization Head is typically the security representative for the Organization and is responsible for its overall security posture.

An Organization Head can access only one organization’s data and can initiate IDS scans on only one Organization’s network.

Manager

The Manager has the same rights as the Organization Head. There can be many Managers for an Organization, but only one Organization Head.

A Manager can access only one Organization’s data and can initiate IDS scans for only one Organization.

End User (EU)

The End User is typically a system or network engineer who has responsibility for running a network. The 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.
- Managers can add, edit and delete new users that 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.
- Managers can open tickets for which vulnerabilities need to be mitigated and end users can close tickets assigned to them 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 Organization's network and can access only the data relevant to that part of the one Organization'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 SecurityCenter runs. The Systems Administrator has administrative ("root") access to the underlying operating system, but does not have access to any SecurityCenter 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 SecurityCenter Software
- Installation of the SecurityCenter Components (Nessus, PVS, LCE)
- 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.

			Organization Accounts	
Security Function	**Authorized Administrator**[4]	**Authorized System Administrator**[5]	**Organization Head / Manager**	**End User**
Install and configure SC4[1]	X			
Manage Organization accounts[2]		X		
Manage user accounts[2]			X	
Manage SC4 components[2]		X		
Monitor SC4 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 SC4 "SecurityCenter 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 SC4. 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 SC 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 a system 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 0.9.8u. For most communication paths, the TOE must 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 SC4 and the LCE is performed using SSH and SCP (over SSH). The SSH encryption is also supported using the OpenSSL module.

2.3.2 Non-bypassability of the TSP

The TOE must 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 must 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 through the host systems included in the TOE, which the TOE uses in its audit function. The system administrator needs to be aware that use of a network time protocol (NTP) ensures consistent time across the different components and associated events and configure each TOE component host system to ensure time synchronization across the TOE components.

2.3.5 Trusted Path

The TOE environment uses HTTPS sessions by default 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.

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.2) 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.

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 careless, willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.

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.

O.EXPORT When any IDS component makes its data available to another IDS component, the TOE will ensure the confidentiality of the 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.INTROP The TOE is interoperable with the IT System it monitors.

OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.

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

OE.AUDIT_SORT The IT Environment will provide the capability to sort the audit information

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.2: 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_STM.1 Reliable time stamps
IDS: Intrusion Detection System	IDS_ANL.1 (EXT): Analyzer analysis
	IDS_RCT.1 (EXT): Analyzer react
	IDS_RDR.1 (EXT): Restricted data review
	IDS_SDC.1 (EXT): System data collection
	IDS_STG.1 (EXT): Guarantee of system data availability
	IDS_STG.2 (EXT): 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

Table 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.2 - Guarantees of Audit Data Availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to [*detect*] modifications to the audit records.

FAU_STG.2.3 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 [***prevent auditable events, except those taken by the authorised user with special rights***] 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: SecurityCenter Administrator, Organization Head, Manager, and End User. More information is provided in Section 6.1.3.*

5.1.4 FPT – Protection of the TSF

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

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.

5.1.5 IDS – Intrusion Detection System

IDS_ANL.1 (EXT) - 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**]. (EXT)

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**]. (EXT)

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 (EXT) - 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. (EXT)

IDS_RDR.1 (EXT) - 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. (EXT)

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

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. (EXT)

IDS_SDC.1 (EXT) - 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) [**Start-up and shutdown, *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**]. (EXT)

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. (EXT).

Event	Details
Start-up and shutdown	None
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 3: System Events

IDS_STG.1 (EXT) - Guarantee of System Data Availability

IDS_STG.1.1 The System shall protect the stored System data from unauthorized deletion. (EXT)
IDS_STG.1.2 The System shall protect the stored System data from modification. (EXT)
IDS_STG.1.3 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***]. (EXT)

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

IDS_STG.2.1 The System shall [***prevent System data, except those taken by the authorised user with special rights***] and send an alarm if the storage capacity has been reached. (EXT)

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL2 augmented with ALC_FLR.2 as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_ARC.1	Architectural Design with domain separation and non-bypassibility
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic design

Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life Cycle Support	ALC_CMS.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - conformance
Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 4: EAL 2 augmented with ALC_FLR.2 Assurance Components

5.2.1 ADV -Development

5.2.1.1 ADV_ARC.1 Security architecture description

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing development functionality.

Evaluator action elements:

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

5.2.1.2 ADV_FSP.2 Security-enforcing functional specification

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

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

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.1.3 ADV_TDS.1 Basic design

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all behavior described in the TOE design is mapped to the TSFIs that invoke it.

Evaluator action elements:

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

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.2.2 AGD –Guidance Documents

5.2.2.1 AGD_OPE.1 Operational user guidance

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance 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.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

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

5.2.2.2 AGD_PRE.1 Preparative procedures

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

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

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 ALC –Life Cycle Support

5.2.3.1 ALC_CMC.2 Use of a CM system

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

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

5.2.3.2 ALC_CMS.2 Parts of the TOE CM coverage

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

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

5.2.3.3 ALC_DEL.1 Delivery procedures

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

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

5.2.3.4 ALC_FLR.2 Flaw reporting procedures

ALC_FLR.2.1D The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D 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.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C 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.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C 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.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C 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.2.8C 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.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 ATE –Tests

5.2.4.1 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 in the test documentation and the TSFIs 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.

5.2.4.2 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, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

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

5.2.4.3 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 execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 AVA –Vulnerability Assessment

5.2.5.1 AVA_VAN.2 Vulnerability analysis

AVA_VAN.2.1D The developer shall provide the TOE for testing.

AVA_VAN.2.1C The TOE shall be suitable for testing.

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

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing basic attack potential.

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 SC4 component. If the SC4 component is enabled, then auditing is turned on 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.

The SC4 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 SC4 and also send an e-mail to a configured user (Organization Head 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.2: Audit data availability
- FAU_STG.4: Prevention of audit data loss

6.1.2 Identification and Authentication

The SC4 TOE component provides an HTTPS-based GUI login interface. TOE users are required to login to the SC4 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 SecurityCenter 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 SecurityCenter Administrator to request that a locked account be unlocked.

When using the 3DT and xTool clients, users must still authenticate successfully to the SC4. The 3DT client is simply an application that makes visualization more pleasant for the administrator. The 3DT application will pass authentication credentials to the SC4 to perform authentication before any TOE information can be displayed to the end user. The xTool application will pass authentication credentials to the SC4 to perform authentication before any scan result or repository query 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: Timing of authentication
- FIA_UID.2: Timing of identification

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: SecurityCenter Administrator, Organization Head, 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. Otherwise, each role will be identified specifically. The TOE restricts the ability to manage functions related to audit and system data to SecurityCenter 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 Organization Heads, 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.

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

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

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

The TOE offers access by Organization Heads, Managers and End Users via these directories, according to the scope of their authority. Organization Heads and Managers can access Organization directories. End Users can access only specific subdirectories within an Organization directory. This access is determined by the TOE. When an Organization Head account is deleted, the corresponding Organization 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 SC4 functions are controlled by asset lists. Individual SecurityCenter 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

6.1.4 FMT_SMR.1: Security roles

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 and SCP (over SSH) is used between the SC4 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. However, 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 no 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.

The TOE uses capabilities of its environment to provide a source of reliable time stamps, which the TOE uses in its audit function. The system administrator needs to be aware that use of Network Time Protocol (NTP) ensures consistent time across the different TOE components and associated events and such functionality must be enabled in order to ensure the reliability of this function.

- FPT_ITT.1: Basic internal TSF data transfer protection
- FPT_STM.1: Reliable time stamps

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 SC4. 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 SecurityCenter Administrator can specify the types of events that will be audited by configuring the various PVS 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 SC4 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 SecurityCenter 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 SecurityCenter 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 SC4 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 system.

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

Section 2.1 (TOE Description) and 2.2 (TOE Architecture) of the ST contain more detailed information about the specific IDS capabilities of the TOE.

7. Protection Profile Claims

The TOE conforms to the US Government Intrusion Detection System System Protection Profile (IDSSYPP), Version 1.7, July 25, 2007.

This Security Target includes all of the Security Functional and Security Assurance Requirements from the PP.

This Security Target includes all of the assumptions and threats statements described in the PP, verbatim. None were added.

This Security Target includes all of the Security Objectives from the PP, verbatim. 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. Additionally, 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.

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. Operational environment objectives are included in this Security Target to cover any objectives not directly addressable by the TOE.

8. Rationale

This section provides the rationale for the selection of the IT security requirements, objectives, assumptions, and threats. In particular, it shows that the IT security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment. The rationale addresses the following areas:

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

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the Intrusion Detection System System Protection Profile. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

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.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP
Intended usage assumptions	**A.ACCESS**					X
	A.ASCOPE					X
	A.DYNMIC				X	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 has the needed access.

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

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 hardware and software.

8.1.1.6 A.MANAGE

There will be one or more competent individuals assigned to manage the TOE 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.

8.1.1.7 A.NOEVIL

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

This Assumption is satisfied by ensuring that:

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

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.

8.1.2 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.EADMIN**	**O.ACCESS**	**O.IDAUTH**	**O.OFLOWS**	**O.AUDITS**	**O.INTEGR**	**OE.INSTAL**	**OE.PHYCAL**	**OE.CREDEN**	**OE.PERSON**	**OE.TIME**	**OE.AUDIT_SORT**	**OE.AUDIT_PROTECTION**
P.DETECT		X	X						X						X		
P.ANALYZ				X													
P.MANAGE	X				X	X	X				X		X	X			
P.ACCESS	X					X	X										X
P.ACCACT							X		X						X	X	
P.INTGTY										X							
P.PROTCT								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 is collected.
- O.IDSCAN: the required scanner data is collected.
- OE.TIME: The IT Environment will provide reliable time stamp to the TOE. Time stamps associated with an audit record must be reliable.

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

8.1.2.3 P.MANAGE

The TOE shall only be managed by authorized users.

This Policy is satisfied by ensuring that:

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

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

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: The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions.
- O.IDAUTH: The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.
- OE.TIME: The IT Environment will provide reliable time stamp to the TOE. Time stamps associated with an audit record must be reliable .
- OE.AUDIT_SORT: The IT environment must provide the ability to review and manage the audit trail of the System to include sorting the audit data.

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

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: The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions.
- OE.PHYCAL: The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

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	O.EXPORT	OE.INSTAL
T.COMINT	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											
T.SCNMLC		X											
T.SCNVUL		X											
T.FALACT					X								
T.FALREC				X									
T.FALASC				X									
T.MISUSE			X										
T.INADVE			X										
T.MISACT			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: The O.IDAUTH objective provides for authentication of users prior to any TOE data access.
- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data.
- O.INTEGR: The O.INTEGR objective ensures no TOE data will be modified.

- O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection.

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: The O.IDAUTH objective provides for authentication of users prior to any TOE data access.
- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data.
- O.EXPORT: The O.EXPORT objective ensures that confidentiality of TOE data will be maintained.
- O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection.

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

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: The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses.
- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
- O.IDSCAN, O.IDSENS, and O.IDANLZ: The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to 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: The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses.
- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
- O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection.

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 O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product.
- O.IDAUTH: The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses.
- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
- OE.INSTAL: The OE.INSTAL objective states the authorized administrators will 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: The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.

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: The 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 O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change. The ST will state whether this threat must be addressed by a Scanner.

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 O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of malicious code. The ST will state whether this threat must be addressed by a Scanner.

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 O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a vulnerability. The ST will state whether this threat must be addressed by a Scanner.

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 O.RESPON objective ensures 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 O.IDANLZ objective provides the function that 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 O. IDANLZ objective provides the function that 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.IDSENS: the TOE, that contains a Sensor, collects sensor data.
- O.AUDIT: the TOE, that contains a Sensor, collects audit 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.IDSENS: the TOE, that contains a Sensor, collects sensor data.
- O.AUDIT: the TOE, that contains a Sensor, collects audit 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.IDSENS: the TOE, that contains a Sensor, collects sensor data.
- O.AUDIT: the TOE, that contains a Sensor, collects audit 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 5** 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	O.EXPORT	OE.TIME	OE.AUDIT_SORT	OE.AUDIT_PROTECTION
FAU_GEN.1										X					
FAU_SAR.1						X									
FAU_SAR.2							X	X							
FAU_SAR.3						X								X	
FAU_SEL.1						X				X					
FAU_STG.2	X						X	X	X		X				X
FAU_STG.4									X	X					
FIA_UAU.2							X	X							
FIA_ATD.1								X							
FIA_UID.2							X	X							
FMT_MOF.1	X						X	X							
FMT_MTD.1	X						X	X			X				
FMT_SMR.1								X							
FMT_SMF.1							X	X		X	X				
FPT_ITT.1	X										X	X			
ADV_ARC.1	X					X		X		X	X				
FPT_STM.1										X			X		
IDS_ANL.1 (EXT)				X											
IDS_RCT.1 (EXT)					X										
IDS_RDR.1 (EXT)						X	X	X							
IDS_SDC.1 (EXT)		X	X												
IDS_STG.1 (EXT)	X						X	X	X		X				
IDS_STG.2 (EXT)									X						

Table 5: 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.2].
- 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.1].
- The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1].
- Only authorized administrators of the 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 must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1].
- The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

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].

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].

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].

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].

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_SEL.1].
- The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1].
- The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1].
- The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

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].
- 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.2].
- The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.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].

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].
- The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2].
- 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.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].
- The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1].
- The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.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.2].
- 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.1].
- The System must prevent the loss of audit data in the event the audit trail is full [IDS_STG.2].

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 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].
- The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1].
- The TSF must be protected form interference that would prevent it from performing its functions [ADV_ARC.1].
- Time stamps associated with an audit record must be reliable [FPT_STM.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.2].
- The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1].
- 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].
- The TOE must ensure that all functions to protect the data are not bypassed [ADV_ARC.1].
- The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

8.2.1.12 O.EXPORT

When any IDS component makes its data available to another IDS component, the TOE will ensure the confidentiality of the System data.

This TOE Security Objective is satisfied by ensuring that:

- Data is protected when transmitted between separate parts of the TOE. [FPT_ITT.1].

8.2.1.13 OE.TIME

The IT Environment will provide reliable timestamps to the TOE.

This Environment Security Objective is satisfied by ensuring that:

- Time stamps associated with an audit record must be reliable [FPT_STM.1].

8.2.1.14 OE.AUDIT_SORT

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

This Environment Security Objective is satisfied by ensuring that:

- The IT environment must provide the ability to review and manage the audit trail of the System to include sorting the audit data [FAU_SAR.3].

8.2.1.15 OE.AUDIT_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 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.2].

8.3 Security Assurance Requirements Rationale

The selected security assurance level is EAL2 augmented with ALC_FLR.2.

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. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The base assurance level was augmented with ALC_FLR.2. 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 Requirement Dependency Rationale

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.2) are met as follows: ALC_FLR.2 has no dependencies per the active PP.

The SFRs included in the ST have all been adopted from the PP, with the following exceptions:

FPT_ITT.1 has been added and has no dependencies.

FMT_SMF.1 has been added and has no dependencies.

FPT_ITC.1 has been removed but does not serve to fulfill any dependencies of any other SFRs.

FPT_ITA.1 has been removed but does not serve to fulfill any dependencies of any other SFRs.

FPT_ITI.1 has been removed but does not serve to fulfill any dependencies of any other SFRs.

Other than the exceptions listed above, the rationale listed in the PP is applicable to this ST.

8.5 Extended Requirements Rationale

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

8.6 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.2	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_STM.1				X	
IDS_ANL.1 (EXT)					X
IDS_RCT.1 (EXT)					X
IDS_RDR.1 (EXT)					X
IDS_SDC.1 (EXT)					X
IDS_STG.1 (EXT)					X
IDS_STG.2 (EXT)					X

Table 6: Security Functions vs. Requirements Mapping