# Lancope StealthWatch Security Target

Version 1.0

July 14, 2004

Prepared for:
**Lancope, Inc.**
**3650 Brookside Parkway, Suite 400**
**Alpharetta, GA 30022**

Prepared By:
**Science Applications International Corporation**
**Common Criteria Testing Laboratory**
**7125 Columbia Gateway Drive, Suite 300**
**Columbia, MD 21046**

**Restricted Rights Legend**

## LIST OF TABLES

# 1. Security Target Introduction

This section provides a Security Target Overview and Organization, identifies the Security Target and Target of Evaluation (TOE), ST conventions terminology & acronyms, and ST conformance claims. The TOE is provided by Lancope, Inc. embedded in the following products: the StealthWatch Appliance and StealthWatch + Therminator.

## 1.1 Security Target Overview and Organization

The Lancope StealthWatch TOE is a network based intrusion detection system that monitors a computer communications network for activity that may inappropriately affect the network's assets. The TOE consists of a sensor that collects information regarding network activity and forwards that information to an analysis engine. The analysis engine performs flow based analysis and reporting of the collected information. The Lancope StealthWatch TOE provides the following security services: audit, identification and authentication, security management, protection of the TOE Security Functions (TSF), and intrusion detection.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8)

## 1.2 Security Target, TOE and CC Identification

**ST Title –** Lancope StealthWatch Security Target

**ST Version** – Version 1.0

**ST Date** – July 14, 2004

**TOE Identification** – Lancope StealthWatch Appliance and StealthWatch + Therminator Appliance containing StealthWatch version 3.3.0 – Build 4140 software.

**CC Identification** – Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408.

## 1.3 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999, ISO/IEC 15408-2.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, ISO/IEC 15408-3.
  - Part 3 Conformant

  - EAL 2 augmented with ALC_FLR.2
- This TOE is conformant to the following Protection Profile (PP):
  - Intrusion Detection System System Protection Profile, Version 1.4, February 4, 2002 (IDSSPP)
- Strength of Function Claim
  - The minimum strength of function level for the security functional requirements is SOF-basic

## 1.4 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

### 1.4.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1(a) and FDP_ACC.1(b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
  - Note that operations already performed in the corresponding Protection Profile are not identified in this Security Target.
- Explicitly stated Security Functional Requirements (i.e., those not found in Part 2 of the CC) are identified with "(**EXP**)".
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

### 1.4.2 Acronyms

The acronyms used within this Security Target are expanded below:

| | |
|---|---|
| AGD | Administrator Guidance Document |
| CC | Common Criteria |
| CI | Concern Index |
| DOS | Denial Of Service |
| EAL | Evaluation Assurance Level |
| HTTP | Hyper Text Transmission Protocol |
| HTTPS | Hyper Text Transmission Protocol, Secure |
| ICMP | Internet Control Message Protocol |
| ID | Identifier |

| | |
|---|---|
| IDS | Intrusion Detection System |
| IDSSPP | IDS System Protection Profile |
| I/O | Input/Output |
| NIST | National Institute of Standards and Technology |
| NTP | Network Time Protocol (RFC 1305) |
| PGP | Pretty Good Privacy |
| PP | Protection Profile |
| RPC | Remote Procedure Call |
| SF | Security Functions |
| SFR | Security Functional Requirement |
| ST | Security Target |
| SWA | StealthWatch Appliance |
| SW+T | StealthWatch + Therminator |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TOE | Target of Evaluation |
| TOS | Type of Service |
| TSF | TOE Security Functions |
| TSP | TOE Security Policy |
| TSC | TSF Scope of Control |
| UDP | User Datagram Protocol |
| UI | User Interface |
| URI | Uniform Resource Identifier |

# 2. TOE Description

The TOE is defined as the Lancope StealthWatch appliance and the StealthWatch + Therminator appliance containing StealthWatch version 3.3.0 – Build 4140 intrusion detection software.

These products are designed and manufactured by Lancope Incorporated, located at 3650 Brookside Parkway, Suite 400, Alpharetta, Georgia, 30022.

The difference between the StealthWatch Appliance and the StealthWatch + Therminator products is that Therminator provides additional GUI interfaces that allow an administrator to view system network traffic from different statistical viewpoints.

The TOE consists of applications and data files that provide the intrusion detection related functions and associated security management functions, an Intel CPU-based Dell 1750 hardware platform, and a Linux operating system (Red Hat distribution v9.0).

StealthWatch characterizes and analyzes the data that flows between Internet Protocol (IP) devices on the network to differentiate abnormal network behavior from normal network behavior. Unlike signature based IDS systems, StealthWatch detects out-of-profile behavior without examining the contents of each packet that traverses the network.

## 2.1 Product Type

The TOE is a network-based intrusion detection system that monitors, records, analyzes, displays, detects and alerts to security breaches and internal misuse on IP based networks. A behavior-based IDS operating on a proprietary flow-based architecture, the TOE enables configurable alarming, provides network surveillance, is capable of operating at near gigabit speeds, recognizes unknown threats and creates forensic data of network activity.

## 2.2 Product Description

StealthWatch approaches intrusion detection and network management through a behavior-based architecture that provides protection from unknown threats, network policy management, activity tracking, and forensics tools for a proactive approach to managing threats. StealthWatch characterizes, and analyzes the data flow between Internet Protocol (IP) devices to differentiate abnormal network behavior from normal behavior. StealthWatch should not be confused with signature, or protocol anomaly products.

## 2.3 Product Features

Lancope's StealthWatch expands intrusion detection beyond monitoring, detecting and responding to network misuse in real-time. Unlike traditional IDS, StealthWatch detects out-of-profile behaviors without looking inside each packet that transits the network. Because it can passively monitor high utilization networks without interfering with the flow of traffic, StealthWatch handles network traffic without the latency induced by IDS solutions that examine the contents of each packet.

### 2.3.1 Detection and Protection

StealthWatch is capable of recognizing attacks that typically evade intrusion detection systems such as undocumented attacks, encrypted attacks, mutated signatures, internal hacking attempts, DoS attacks and Trojan Horses. Unlike traditional IDS's, StealthWatch does not rely on signature updates for attack recognition. Its behavior-based recognition is available from the time it is introduced to the network architecture. In addition, StealthWatch can trace the source of attacks, a useful tool when responding to attacks.

### 2.3.2 Intelligent Alarming

StealthWatch differentiates between legitimate and suspicious connections (probes). Instead of alarming system administration on every ping, probe or scan, StealthWatch builds a profile of each suspicious host. By using an algorithm to determine the level of suspicion, StealthWatch can filter out background noise associated with traditional IDS tools. When the Concern Index of any particular host surpasses an administrator-defined threshold, StealthWatch responds with customizable alerts.

### 2.3.3 High-Speed Network Scalability

By not having to search through strings of signature data, StealthWatch's flow-based engine can analyze network traffic at bandwidth rates approaching 1 Gbps. Furthermore, StealthWatch is a passive monitoring device that introduces zero latency in the enterprise network.

### 2.3.4 Security Policy Management and Enforcement

An important component in a secure network environment is the ability to monitor services that are run on a daily basis within the network. Maintaining a timely and complete picture of network services on each host is time consuming and difficult using manual techniques, and traditional network management tools are also labor intensive. StealthWatch provides a unique component in this arena, allowing security teams to set policies and enforce them. With its service profiler, administrators can view the services running on the network, by host, to determine which are appropriate and in profile. The appropriate system administrator will be notified whenever an out-of-profile service is run.

### 2.3.5 Forensics

StealthWatch's patent-pending technology, called data flow analysis, provides a unique forensics tool - the network flow log. By characterizing each flow that occurs on the network, StealthWatch can maintain a detailed and easy-to-digest trail of information. This log is maintained for up to 30 days and can be archived for later use. In addition, StealthWatch provides on-demand, daily and weekly reports of network activity.

### 2.3.6 Auto Tuning

The intent of StealthWatch is to reduce resource requirements and provide ease-of-use. StealthWatch requires minimal configuration during implementation and its user interface allows administrators to quickly determine the likelihood of possible malicious activity. The concern index and service profile capabilities are meaningful metrics that combine to reduce false positives, and reduce the time required of administrators or security teams.

## 2.4 Security Environment TOE Boundary

The TOE includes both physical and logical boundaries as defined in the following sections.

### 2.4.1 Physical Boundaries

The TOE is physically comprised of an Intel based hardware platform. The TOE utilizes process, disk, and memory management services provided by the hardware to manage itself. The TOE also uses network communication services to monitor network traffic and to communicate between the StealthWatch appliance and the web-based administrative interface. The only security relevant aspect of the operating system and underlying hardware is that they work together to provide reliable time information for use by the StealthWatch application software.

The components that comprise StealthWatch are the data collection interface, the flow based analysis engine (including universal behavior, traffic patterns, and host profile data files), a forensic data repository, the alarm generation component, the audit component (comprised of audit configuration, time generation, audit generation, and an audit repository), and the administrative interface. The following figure provides a depiction of the StealthWatch architecture.

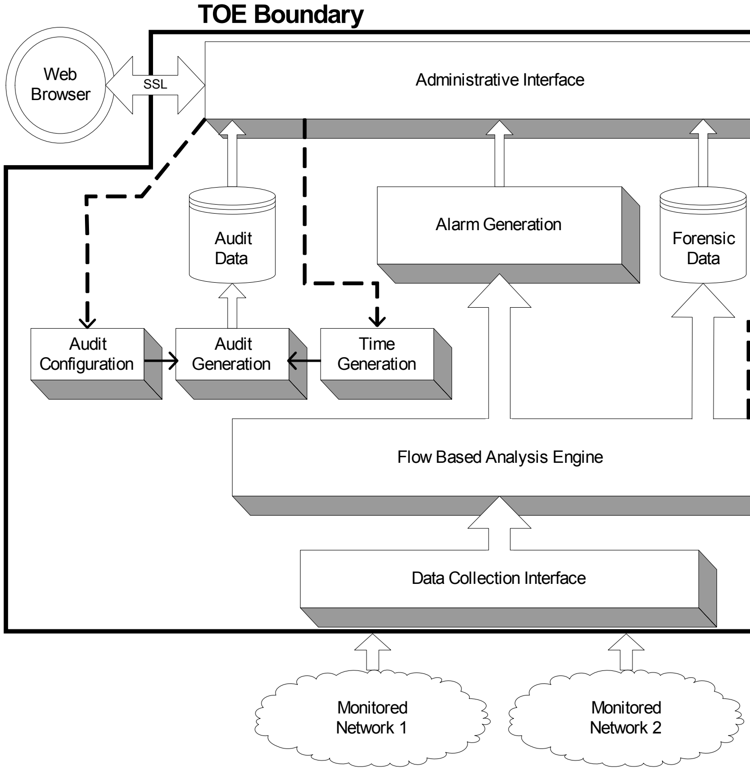

Figure 1 StealthWatch Component Architecture

## 2.4.2 Logical Boundaries

The logical boundaries of the TOE fall into two categories. The first deals with security and administration of the system as a whole (Security Audit, Identification and Authentication, Security Management, and Protection of Security Functions). The second deals with collection and analysis of data regarding the network traffic on the monitored networks (System Data Collection; System Data Analysis and Reaction; and System Data Review, Availability, and Loss).

### 2.4.2.1 Security Audit

The TOE generates audit data for administrative and management actions taken on the system. This audit is unrelated to the system data that is collected about the monitored networks. The actions audited by the TOE include start-up and shutdown of the system, system access, access to collected system and audit data, modification to the auditing configuration, modifications to configuration data, and adding or removing users. Access to the security audit log is provided through the administrative interface via a secure connection from a web browser.

### 2.4.2.2 Identification and Authentication

All users of the TOE must enter a valid user identity and password before the user can access any TOE functionality. There are 3 types of accounts, Administrator, Web Administrator, and Technician. The Administrator and Web Administrator accounts have predefined identities (usernames), but configurable authentication data. Administrative guidance defines the assignment of these user identities. The users holding the authorised System Administrator role (see definition in section 2.4.2.3) can create the third type of account: Technician. Technician accounts have a definable identity (username) and authentication data, but are limited in the access allowed to configuration and audit data.

### 2.4.2.3 Security Management

The TOE provides a secure web-based (utilizing SSL) management interface for all administrative tasks.

There are three classes of user accounts supported by the TOE. Those account classes have the following access rights defined:

- Administrator: Read/write access to the Administration/Appliance (hardware configuration) GUI as well as all areas of the StealthWatch GUI, including the StealthWatch configuration screens.
- Web Administrator: Read/write access to all areas of the StealthWatch GUI, including the StealthWatch configuration screens. The Web Administrator account does not have access to the Administration/Appliance (hardware configuration) GUI.
- Technician: Read/write access to all areas of the StealthWatch GUI except for read-only access to the StealthWatch configuration screens. Technicians do not have access to the Administration/Appliance (hardware configuration) GUI.

The Administrator and Web Administrator accounts are provided with the ability to modify the behavior of the analysis and reporting functions by allowing them to modify the policies and thresholds of a host that is being monitored by the TOE. The Administrator and Web Administrator classes comprise the authorised System administrator role, while the Technician class comprises the authorised administrator role.

### 2.4.2.4 Protection of the TOE Security Functions

The TOE protects its own security functions through a variety of mechanisms. One of the primary protections is that users must authenticate before any administrative operation can be performed. The data transferred between the TOE and the administrative user is protected by using SSL to encrypt and verify the communication.

The data collection interface of the TOE is protected from the monitored network by operating in a completely passive mode. The TOE does not respond to any traffic received from the monitored networks. The TOE cannot receive any management requests or input from the monitored network interfaces. Management requests can only be received via a physically separate network management port.

The TOE protects its ability to continue recording audit data by periodically purging data, starting with the oldest data first. In a situation where there is adequate storage space, audit data is preserved for 30 days. If storage space is exhausted prior to 30 days, the oldest records are overwritten with new data on a first-in / first-out basis. This ensures that there is always storage available for recording current audit events.

### 2.4.2.5 System Data Collection

The TOE collects communications flow information about all monitored network activity. The system can either auto-tune itself by monitoring normal activity on the network for a pre-defined period of time, or it can be manually tuned utilizing the zone and host policies (see section 2.4.2.6).

### 2.4.2.6 System Data Analysis and Reaction

The TOE monitors all network traffic against predefined thresholds (called Concern Indices (or CIs)) and policies (set at the granularity of a specific host or a collection of hosts, known as a zone), to detect potential intrusions, and to generate alarms when either are detected.

Extensive analysis tools are provided via the Administrative interface to view system data. The main menu of the Administrative interface provides the following options:

- Status Screen: The system "dashboard." It displays a variety of graphs and data that assist the authorised administrator to monitor the network.
- Alarm Manager: Displays all non-cleared alarms, with an option to display cleared alarms.

- Security Menu: Security-related screens associated with concern index, probes[1], and touched hosts[2].
- Hosts Menu: Displays several host-specific screens such as service profiles, traffic profiles, and snapshot reports.
- Policy Menu: Displays, and allows authorised System administrators to configure, various settings and exceptions on both a per host and per zone basis, that affect how the system processes incoming and outgoing flows
- Traffic Menu: Displays several screens of traffic flow data.

#### 2.4.2.7 System Data Review, Availability, and Loss

The TOE protects the data it collects by limiting access. It limits access in two ways:

1) Only authorised administrators are permitted to read system data
2) The only interface provided to the data store is read only

The TOE ensures availability and limits loss of system data by periodically purging data, starting with the oldest data first. In a situation where there is adequate storage space, system data is preserved for 30 days. If storage space is exhausted prior to 30 days, the oldest records are overwritten with new data on a first-in / first-out basis, and an alarm is sent to the authorised administrator. This ensures that there is always storage available for recording current system data.

[1] Any effort, such as a communications request or transaction which is used to gather information about a computer or the network state.

[2] A touched host is a host computer hat has been contacted by another computer that is outside its zone.

# 3. Security Environment

This section defines the assumptions, threats, and organizational security policies that the TOE, in conjunction with its environment, is subject to. With one exception, the assumptions, threats and organizational security policies are taken from the IDS System PP. This ST includes one additional physical assumption, A.ITNET.

## 3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

### 3.1.1 Intended Usage Assumptions

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

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

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

### 3.1.2 Physical Assumptions

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

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

A.ITNET Any network resources used for network-based TOE management will be adequately protected from unauthorised access and will provide necessary services without impacting the ability of the TOE to implement its security functions.

### 3.1.3 Personnel Assumptions

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

A.NOEVIL The authorised 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 authorised users.

## 3.2 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.

### 3.2.1 TOE Threats

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

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

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

T.NOHALT An unauthorised user may attempt to compromise the continuity of the Systems collection and analysis functions by halting execution of the TOE.

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

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

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

T.FACCNT Unauthorised attempts to access TOE data or security functions may go undetected.

### 3.2.2 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 Unauthorised 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.

## 3.3 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 TOE and the intended environment of the TOE.

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 authorised users.

P.ACCESS All data collected and produced by the TOE shall only be used for authorised 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 unauthorised accesses and disruptions of TOE data and functions.

# 4. Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. With one exception, the security objectives, categorized as either IT security objectives for the TOE or its environment are taken from the IDS System PP. This ST includes one additional security objective for the environment, O.PLTFRM. All of the identified organization policies are addressed by the security objectives described below.

## 4.1 IT Security Objectives for the TOE

O.PROTCT The TOE must protect itself from unauthorised 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 authorised users to access only appropriate TOE functions and data.

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

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

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

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

## 4.2 Security Objectives for the Environment

O.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.

O.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

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

O.PERSON Personnel working as authorised administrators shall be carefully selected and trained for proper operation of the System.

O.INTROP The TOE is interoperable with the IT System it monitors.

O.PLTFRM The IT Environment that hosts the TOE will be free from code or other features that might impact the security functions implemented by the TOE, will provide the functional services required for the TOE to operate properly, and will be protected from any unauthorised access (such as physical attacks).

# 5. IT Security Requirements

This section provides a list of all security functional requirements for the TOE. Security functional requirements in this ST are drawn from the IDSSPP.

## 5.1 TOE Security Functional Requirements

Table 1 describes the SFRs that are satisfied by the TOE.

| 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_ATD.1: User Attribute Definition |
| | FIA_UAU.1: Timing of Authentication |
| | FIA_UID.1: Timing of Identification |
| **FMT: Security Management** | FMT_MOF.1: Management of Security Functions Behaviour |
| | FMT_MTD.1: Management of TSF Data |
| | FMT_SMR.1: Security Roles |
| **FPT: Protection of the TOE Security Functions** | FPT_RVM.1: Non-bypassability of the TSP |
| | FPT_SEP.1: TSF domain separation |
| | FPT_STM.1: Reliable time stamps |
| **IDS: Intrusion Detection System** | IDS_ANL.1: Analyser analysis (EXP) |
| | IDS_RCT.1: Analyser react (EXP) |
| | IDS_RDR.1: Restricted Data Review (EXP) |
| | IDS_SDC.1: System Data Collection (EXP) |
| | IDS_STG.1: Guarantee of System Data Availability (EXP) |
| | IDS_STG.2: Prevention of System data loss (EXP) |

Table 1 Security Functional Components

### 5.1.1 Security Audit (FAU)

#### 5.1.1.1 Audit Data Generation (FAU_GEN.1)

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

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

b) All auditable events for the basic level of audit **(as included by Table 2)**; and

c) Access to the System and access to the TOE and System data.

| 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 | |

| Component | Event | Details |
|---|---|---|
| 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. 1 | All use of the authentication mechanism | User identity, location |
| FIA_UID.1 | 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

Note: The IDS_SDC and IDS_ANL requirements in this ST address the recording of results from IDS scanning, sensing, and analysing tasks (i.e., 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.

### 5.1.1.2 Audit Review (FAU_SAR.1)

**FAU_SAR.1.1** The TSF shall provide **[the authorised administrators and the authorised System administrators]** 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.

### 5.1.1.3 Restricted Audit Review (FAU_SAR.2)

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

### 5.1.1.4 Selectable Audit Review (FAU_SAR.3)

**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.

### 5.1.1.5 Selective Audit (FAU_SEL.1)

**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**].

### 5.1.1.6 Guarantees of Audit Data Availability (FAU_STG.2)

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

**FAU_STG.2.2** The TSF shall be able to detect **unauthorised** modifications to the audit records in the audit trail. *(per International Interpretation #141)*

**FAU_STG.2.3** The TSF shall ensure that **[the most recent, limited by available storage space]** audit records will be maintained when the following conditions occur: **[*audit storage exhaustion*]**.

#### 5.1.1.7 Prevention of Audit Data Loss (FAU_STG.4)

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

### 5.1.2 Identification and Authentication (FIA)

#### 5.1.2.1 Timing of Authentication (FIA_UAU.1)

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

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

#### 5.1.2.2 User Attribute Definition (FIA_ATD.1)

**FIA_ATD.1.1** The TSF shall maintain the following list of security attributes belonging to individual users:

a) User identity;

b) Authentication data;

c) Authorisations; and

d) **[no other security attributes]**.

#### 5.1.2.3 Timing of Identification (FIA_UID.1)

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

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

### 5.1.3 Security Management (FMT)

#### 5.1.3.1 Management of Security Functions Behaviour (FMT_MOF.1)

**FMT_MOF.1.1** The TSF shall restrict the ability to modify the behaviour of the functions of System data collection, analysis and reaction to authorised System administrators.

#### 5.1.3.2 Management of TSF Data (FMT_MTD.1)

**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 **[the authorised administrators and the authorised System administrators]**.

#### 5.1.3.3 Security Roles (FMT_SMR.1)

**FMT_SMR.1.1** The TSF shall maintain the following roles: authorised administrator, authorised System administrators, and **[no other authorised identified roles]**.

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

## 5.1.4 Protection of the TOE Security Functions (FPT)

### 5.1.4.1 Non-bypassability of the TSP (FPT_RVM.1)

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

### 5.1.4.2 TSF domain separation (FPT_SEP.1)

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

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

### 5.1.4.3 Reliable time stamps (FPT_STM.1)

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

## 5.1.5 Intrusion Detection System (IDS)

### 5.1.5.1 System Data Collection (EXP) (IDS_SDC.1)

**IDS_SDC.1.1** The System shall be able to collect the following information from the targeted IT System resource(s):

a) **[*service requests, network traffic*]**; and

b) **[no other specifically defined events]**. **(EXP)**

**IDS_SDC.1.2** At a minimum, the System shall collect and record the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) The additional information specified in the Details column of Table 3 System Events. **(EXP)**

| Component | Event | Details |
|---|---|---|
| IDS_SDC.1 | Service Requests | Specific service, source address, destination address |
| IDS_SDC.1 | Network traffic | Protocol, source address, destination address |

Table 3 System Events

### 5.1.5.2 Analyser analysis (EXP) (IDS_ANL.1)

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

a) **[*statistical*]**; and

b) **[no other analytical functions]**. **(EXP)**

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

a. Date and time of the result, type of result, identification of data source; and

b. **[data flow statistics]**. **(EXP)**

### 5.1.5.3 Analyser react (EXP) (IDS_RCT.1)

**IDS_RCT.1.1** The System shall send an alarm to **[the Alarm Manager]** and take **[no other actions]** when an intrusion is detected. **(EXP)**

#### 5.1.5.4 Restricted Data Review (EXP) (IDS_RDR.1)

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

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

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

#### 5.1.5.5 Guarantee of System Data Availability (EXP) (IDS_STG.1)

**IDS_STG.1.1** The System shall protect the stored System data from unauthorised deletion. **(EXP)**

**IDS_STG.1.2** The System shall protect the stored System data from modification. **(EXP)**

**IDS_STG.1.3** The System shall ensure that **[the most recent, limited by available storage space]** System data will be maintained when the following conditions occur: **[*System data storage exhaustion*]**. **(EXP)**

#### 5.1.5.6 Prevention of System data loss (EXP) (IDS_STG.2)

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

## 5.2 TOE Security Assurance Requirements

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

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

Table 4 EAL 2 augmented with ALC_FLR.2 Assurance Components

### 5.2.1 Configuration management (ACM)

#### 5.2.1.1 Configuration items (ACM_CAP.2)

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

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

**ACM_CAP.2.3d** The developer shall provide CM documentation.

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

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

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

The configuration list shall uniquely identify all configuration items that comprise the TOE.*(per International Interpretation #003)*

**ACM_CAP.2.4c** The configuration list shall describe the configuration items that comprise the TOE.

**ACM_CAP.2.5c** The CM documentation shall describe the method used to uniquely identify the configuration items.

**ACM_CAP.2.6c** The CM system shall uniquely identify all configuration items.

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

## 5.2.2 Delivery and operation (ADO)

### 5.2.2.1 Delivery procedures (ADO_DEL.1)

**ADO_DEL.1.1d** The developer shall document procedures for delivery of the TOE or parts of it to the user.

**ADO_DEL.1.2d** The developer shall use the delivery procedures.

**ADO_DEL.1.1c** The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

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

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

**ADO_IGS.1.1d** The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

**ADO_IGS.1.1c** The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE. *(per International Interpretation #51 (rev 1))*

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

**ADO_IGS.1.2e** The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

## 5.2.3 Development (ADV)

### 5.2.3.1 Informal functional specification (ADV_FSP.1)

**ADV_FSP.1.1d** The developer shall provide a functional specification.

**ADV_FSP.1.1c** The functional specification shall describe the TSF and its external interfaces using an informal style.

**ADV_FSP.1.2c** The functional specification shall be internally consistent.

**ADV_FSP.1.3c** The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

**ADV_FSP.1.4c** The functional specification shall completely represent the TSF.

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

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

#### 5.2.3.2 Descriptive high-level design (ADV_HLD.1)

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

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

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

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

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

**ADV_HLD.1.5c** The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

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

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

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

**ADV_HLD.1.2e** The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

#### 5.2.3.3 Informal correspondence demonstration (ADV_RCR.1)

**ADV_RCR.1.1d** The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

**ADV_RCR.1.1c** For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

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

### 5.2.4 Guidance documents (AGD)

#### 5.2.4.1 Administrator guidance (AGD_ADM.1)

**AGD_ADM.1.1d**The developer shall provide administrator guidance addressed to system administrative personnel.

**AGD_ADM.1.1c**The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

**AGD_ADM.1.2c**The administrator guidance shall describe how to administer the TOE in a secure manner.

**AGD_ADM.1.3c**The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

**AGD_ADM.1.4c** The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

**AGD_ADM.1.5c** The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

**AGD_ADM.1.6c** The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

**AGD_ADM.1.7c** The administrator guidance shall be consistent with all other documentation supplied for evaluation.

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

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

#### 5.2.4.2 User guidance (AGD_USR.1)

**AGD_USR.1.1d** The developer shall provide user guidance.

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

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

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

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

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

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

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

### 5.2.5 Life cycle support (ALC)

#### 5.2.5.1 Flaw reporting procedures (ALC_FLR.2)

**ALC_FLR.2.1d** The developer shall ~~document the flaw remediation procedures~~ provide flaw remediation procedures addressed to TOE developers. *(modified per International Interpretation #94)*

**ALC_FLR.2.2d** The developer shall establish a procedure for accepting and acting upon user 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. *(added per International Interpretation #94)*

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

**ALC_FLR.2.6c** 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.2.1e** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

## 5.2.6 Tests (ATE)

### 5.2.6.1 Evidence of coverage (ATE_COV.1)

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

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

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

### 5.2.6.2 Functional testing (ATE_FUN.1)

**ATE_FUN.1.1d** The developer shall test the TSF and document the results.

**ATE_FUN.1.2d** The developer shall provide test documentation.

**ATE_FUN.1.1c** The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

**ATE_FUN.1.2c** The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

**ATE_FUN.1.3c** The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

**ATE_FUN.1.4c** The expected test results shall show the anticipated outputs from a successful execution of the tests.

**ATE_FUN.1.5c** The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

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

### 5.2.6.3 Independent testing - sample (ATE_IND.2)

**ATE_IND.2.1d** The developer shall provide the TOE for testing.

**ATE_IND.2.1c** The TOE shall be suitable for testing.

**ATE_IND.2.2c** The developer shall provide an equivalent set of resources to those that were used in the developer’s functional testing of the TSF.

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

**ATE_IND.2.2e** The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

**ATE_IND.2.3e** The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

## 5.2.7 Vulnerability assessment (AVA)

### 5.2.7.1 Strength of TOE security function evaluation (AVA_SOF.1)

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

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

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

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

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

### 5.2.7.2 Developer vulnerability analysis (AVA_VLA.1)

**AVA_VLA.1.1d** The developer shall perform a vulnerability analysis. *(per International Interpretation #51 (rev 1))*

**AVA_VLA.1.2d** The developer shall provide vulnerability analysis documentation. *(per International Interpretation #51 (rev 1))*

**AVA_VLA.1.1c** The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP. *(per International Interpretation #51 (rev 1))*

**AVA_VLA.1.2c** The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities. *(per International Interpretation #51 (rev 1))*

**AVA_VLA.1.3c** The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. *(per International Interpretation #51 (rev 1))*

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

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

# 6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

## 6.1 TOE Security Functions

### 6.1.1 Security Audit

**FAU_GEN.1 Audit Data Generation**

Auditing is the recording of events within the system, exclusive of the recording of sensing and analysis tasks performed by the flow based analysis engine. StealthWatch utilizes a protected disk file to record audit log information in a data store.

The following information relevant to each auditable event is stored in the audit data store:

a) Date and time that the event occurred,

b) The type of event,

c) The user causing the event,

d) The outcome of the event – success or failure.

The following auditable events can be included in the set of audited events:

a) Startup and shutdown of the audit function,

b) Access to the system,

c) All access to the TOE and System data – including the requested access,[3]

d) All modification to the audit configuration that occur during collection

e) All authentication attempts – including the identification data (e.g. username) and location where authentication was attempted

f) All modification to the behavior of the TSF

g) All modifications to TSF data values

h) All modifications to user accounts – including the user identity that was created, deleted, or modified, and the user identity that performed the modification.

**FAU_SAR.1 Audit Review**

StealthWatch provides the ability for users in the authorised administrator or authorised System administrator role to view security audit data for the system. The audit logs are viewable through the standard web-based administrative interface.

**FAU_SAR.2 Restricted Audit Review**

No security related actions can be taken without successful user authentication, therefore only authorised users who have the authorised administrator or authorised System administrator role can view the audit records.

**FAU_SAR.3 Selectable Audit Review**

While viewing the security audit records, it is possible to sort and filter the data based upon the following properties:

[3] Note: The object IDS required to be audited by the FAU_GEN.1 requirement is inherent in the location of the audit log. The audit record itself does not contain this information, but each StealthWatch appliance (e.g. IDS System) contains only one audit log which is for that particular appliance. Therefore the appliance being accessed to view the audit log is the object IDS of the audit record.

- Date and time
- User
- Type of event
- Success or Failure of the event

**FAU_SEL.1 Selectable Audit**

The StealthWatch administrative interface provides a GUI screen that allows a user with the authorised System administrator role to select auditable events from the set of audited events based on the event type. The selection is via a series of check boxes in the administrative interface that identify which events will be audited.

**FAU_STG.2 Guarantees of Data Availability**

The only way to access the audit records is through the administrative interface. The TOE provides protection for the security audit records primarily by preventing access to the system without successful authentication. Secondly, no interface is provided for the authorised administrator or authorised System administrator roles to modify the audit records. Further, since the audit function starts automatically with the TOE, and cannot be disabled, all actions taken against the audit records are recorded. The most recent audit records will always be available as the oldest audit records are overwritten in the event of audit storage exhaustion.

**FAU_STG.4 Prevention of Audit Data Loss**

When the TOE exhausts the available storage space for audit records, an alert is entered in the Alarm Manager. If the audit process runs out of storage space, then the oldest records will be automatically overwritten to prevent new audited events from occurring without being audited.

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

- FAU_GEN.1
- FAU_SAR.1
- FAU_SAR.2
- FAU_SAR.3
- FAU_SEL.1
- FAU_STG.2
- FAU_STG.4

### 6.1.2 Identification and Authentication

**FIA_UAU.1 Timing of Authentication**

When a potential user attempts to access the TOE, the user is presented with a username and password dialog. No access to the TOE will be provided until the potential user has successfully authenticated themselves to the TOE. The TOE requires users to provide unique identification (username) and authentication data (passwords) before any access to the system is granted. In order for access to be granted the password provided must match the password that the TSF recognizes as being assigned to the provided username. No actions are allowed, other than entry of identification and authentication data, until successful authentication occurs.

**FIA_ATD.1 User Attribute Definition**

User accounts in the TOE have the following attributes: user name, authentication data (password), and their assigned role (authorizations). All user accounts are in either the authorised administrator or authorised System administrator role. The requirements for password complexity and password assignment are provided in the administrative guidance.

**FIA_UID.1 Timing of Identification**

StealthWatch requires users to provide unique identification and authentication data (passwords) before any access to the system is granted. No actions are allowed, other than entry of identification and authentication data, until successful identification occurs.

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

- FIA_UAU.1
- FIA_ATD.1
- FIA_UID.1

### 6.1.3 Security Management

**FMT_MOF.1 Management of Security Functions Behavior**

StealthWatch requires user authentication before any actions can be performed (other than entry of identification and authentication data) on the TOE, security-related or otherwise. Due to this, only authorised administrators or authorised System administrators can access any functions on the system. Users with the authorised System administrator role have the ability to modify traffic and host profiles that influence how System Data is analyzed, displayed, and reacted to. Users with the authorised administrator role only have the ability to view the settings that influence how System Data is analyzed, displayed, and reacted to. The authorised System administrator role is the only role that can manage the security settings on the system, such as user accounts and audit settings. No user can modify the behavior of the TOE relevant to System data collection, as all communication flow data collected by the system is always collected. Users can only affect the way the collected data is analyzed, displayed, and reacted to.

**FMT_MTD.1 Management of TSF Data**

See FMT_SMR.1.

**FMT_SMR.1 Security Roles**

The TOE has three classes of users that form two roles, each with its own set of privileges. When a user is assigned to a class, the class mandates the role.

- “Administrator” class: this class of user can perform all management functions on the TOE. The user in this class can manage user accounts (create, delete, modify), view the security audit log, view, query, modify, and delete the System Data log and manually tune the profiles that govern the IDS.
- “Web Administrator” class: The user in this class can view the security audit log, view, query, and modify the System Data log and manually tune the profiles that govern the IDS.
- “Technician” class: A user of this class can view the security audit logs, view and query the System Data log, and clear alarms.

Note that the Administrator and Web Administrator classes of users form the “authorised System administrator” role and the Technician class of users forms the “authorised administrator” role. The Administrator and Web Administrator classes each have a single predefined user identity each of which is assigned to a single user as stipulated in the StealthWatch administrative guidance.

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

- FMT_MOF.1
- FMT_MTD.1
- FMT_SMR.1

### 6.1.4 Protection of the TOE Security Functions

**FPT_RVM.1 Non-bypassability of the TSP**

The TSF requires that all users successfully authenticate before any actions can view or modify the TSP. No actions are allowed on the TOE until after successful authentication, and the allowed actions are determined by the assigned user role. The TOE implements a receive only, passive, monitoring interface on the monitored network. The TOE does not provide any interface for an entity to interact with it via the monitored network. TOE management is accomplished via a protected network as discussed in A.ITNET.

**FPT_SEP.1 TSF Domain Separation**

The TOE is housed by an enclosed appliance in which all operations are self-contained. The TOE does not respond to any network traffic on the network it monitors and its management interface is on a physically protected network. No operations are performed outside the physical boundary of the TOE.

**FPT_STM.1 Reliable Time Stamps**

The TOE provides time stamps to system data and audit data log entries. It requests and receives time from its hardware clock via an operating system call and then applies that time directly to the corresponding log entry. The TOE provides a limited interface to the time mechanism that allow authorized System administrators to set the correct time utilizing the administrative interface. The time keeping mechanism is the only security relevant aspect of the operating system and hardware that underlies the StealthWatch application software.

The Protection of the TOE Security Functions function is designed to satisfy the following security functional requirements:

- FPT_RVM.1
- FPT_SEP.1
- FPT_STM.1

### 6.1.5 Intrusion Detection System

**IDS_SDC.1 System Data Collection**

StealthWatch has the ability to manually and automatically tune profiles that define when alerts are generated, indicating potential intrusions. While StealthWatch contains default universal behaviors to detect known vulnerabilities and exploits, new profiles can be defined to alert on abnormal behaviors as well as specific network traffic, allowing the authorised System administrator role complete control over the types of traffic that will be alerted. Note that these profiles do not affect the flows that are monitored, as all communication flows are monitored for potential later analysis. As Ethernet frames are received through one of the promiscuous interfaces on the StealthWatch appliance, these packets are fed into a flow analysis engine that separates and categorizes the active data flows.

The system data that is collected includes the following information:

a) Date and time that the event occurred,

b) The type of event,

c) The outcome of the event,

d) The protocol of the particular event,

e) The service identifier of the event,

f) The source IP address,

g) The source MAC address,

h) The destination IP address,

i) The destination MAC address.

**IDS_ANL.1 Analyzer Analysis**

To analyze the data collected by the data collection interface, StealthWatch uses a collection of universal behaviors, traffic profiles, and host profiles.

Universal behaviors and profiles are patterns of traffic that define normal activity for the network and for each host, and can be used to detect attacks, exploits, and misuse of the network.

StealthWatch operates by establishing a behavioral profile of normal network activity and usage. During initial installation, an autotuning period will take place, allowing StealthWatch to "autotune" host specific thresholds and settings. Once the profile is complete and final manual tuning has taken place, the behavioral profile is "locked down."

In normal operation, once the collected data flows have been properly categorized, StealthWatch performs periodic analysis of the collected data, checking host profiles, traffic profiles, and system-wide Universal Behavior threshold settings to verify the flows satisfy the parameters of the established behavioral profile.

Nefarious traffic is then identified and reported. As patterns emerge and suspect flows are identified, StealthWatch begins to accumulate Concern Index points for the suspect host. As a host's Concern Index increases, StealthWatch raises alarms to notify an administrator of the host's activity.

Each network host has an individual Concern Index threshold. During the autotuning process, or manually through the StealthWatch host profiler, a host's Concern Index threshold will be set to its optimum value.

All communication flows are logged and contain, at least, the information specified below:

a) Flow start date & time

b) Flow end date & time

c) Source IP

d) Source MAC

e) Destination IP

f) Destination MAC

g) Total bytes transferred during the flow

h) Average Kb per second

i) Total packets transferred during the flow

j) Length in seconds of the flow

k) TCP, UDP or other IP protocol type

l) Data bytes sent by source IP

m) Data bytes sent by destination IP

n) Number of packets sent by source IP

o) Number of packets sent by destination IP

**IDS_RCT.1 Analyzer React**

When any communication flow occurs, the details of that flow are logged in the system data log for future forensic analysis and event reconstruction. In addition, when the characteristics of a communication flow violate the defined acceptable behavior of a host, an alarm is triggered. When an alarm is triggered, it is recorded in the Alarm Manager to notify the authorised System administrator and authorised administrator roles.

**IDS_RDR.1 Restricted Data Review**

In StealthWatch, only successfully authenticated users can access the TOE. Since all users that successfully authenticate are members of either the authorised System administrator role or authorised administrator role, no further restrictions on the ability to review the system data log are necessary.

All system data is only available through the administrative interface provided by StealthWatch. The alarm generation component identifies events of particular interest and the administrative interface interprets the data in a readable format for the user. The information is then displayed via the administrative interface. All members of the authorised System administrator and authorised administrator roles are granted explicit read access to all system data.

**IDS_STG.1 Guarantee of System Data Availability**

StealthWatch protects the gathered system data log from unauthorised modification or deletion by presenting only the administrative interface to all users. No users are allowed to edit the log; it is marked for read-only access, preventing user modification. Only users with the authorised System administrator role can delete the log.

To guarantee that the most recent system data is always able to be recorded, when the system data storage space is exhausted, the oldest events stored in the system data store will be overwritten.

**IDS_STG.2 Prevention of System Data Loss**

To prevent the loss in new/current event data, the oldest events stored in the log will be overwritten when the system data storage capacity is exhausted. When this occurs the authorised System administrator and the authorised administrator roles will be alerted via a system alert.

The Intrusion Detection System function is designed to satisfy the following security functional requirements:

- IDS_SDC.1
- IDS_ANL.1
- IDS_RCT.1
- IDS_RDR.1
- IDS_STG.1
- IDS_STG.2

## 6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL2 assurance requirements:

- Configuration Management,
- Delivery and Operation,
- Development,
- Guidance Documentation,
- Tests,
- Vulnerability Assessment.

In addition, Lancope implements the following assurance measure, exceeding the assurance requirements of EAL2:

- Life Cycle Support.

### 6.2.1 Configuration Management

The configuration management measures applied by Lancope ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Lancope performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, the CM documentation, and the Vulnerability Assessment documentation. These activities are documented in:

- StealthWatch Configuration Management Procedure
- Configuration Item List, StealthWatch Appliance V3.3.0
- Configuration Item List, StealthWatch + Therminator V3.3.0

The Configuration management assurance measure satisfies the following EAL 2 assurance requirements:

- ACM_CAP.2

### 6.2.2 Delivery and Operation

Lancope provides delivery documentation that explains how the TOE is delivered, procedures to identify the TOE, and procedures to allow detection of unauthorised modifications of the TOE. These procedures are documented in:

- StealthWatch Build, Test and Delivery Procedures

Lancope provides installation and initialization procedures in the administrator guidance. The installation and generation procedures describe the steps necessary to install StealthWatch products in accordance with the evaluated configuration and the procedures to be used for the generation, and start-up of the TOE.

The installation, generation, and start-up procedures are documented in:

- StealthWatch Installation Process
- StealthWatch Quick Start Configuration Checklist
- StealthWatch Configuration Guide

The Delivery and Guidance assurance measure satisfies the following Assurance requirements:

- ADO_DEL.1,
- ADO_IGS.1,

### 6.2.3 Development

The Design Documentation provided for StealthWatch is provided in the following documents:

- Functional Specification for StealthWatch Appliance (SWA) and StealthWatch+Therminator (SW+T), Release Version 3.3.0
- High Level Design Document for StealthWatch Appliance (SWA) and StealthWatch+Therminator (SW+T), Release Version 3.3.0
- Correspondence Document for StealthWatch Appliance (SWA) and StealthWatch + Therminator (SW+T), Release V3.3.0

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

The Development assurance measure satisfies the following EAL 2 requirements:

- ADV_FSP.1
- ADV_HLD.1

- ADV_RCR.1

### 6.2.4 Guidance documents

Lancope provides administrator guidance documents that describe the administrative functions and the administrative interface available to authorised System administrators and authorised administrators of the StealthWatch appliance. These documents are consistent with other supplied documentation and describe how to administer StealthWatch in a secure manner. The guidance documents describe the assumptions regarding user behavior that is relevant to the secure operation of the appliance, and describes the parameters that are under the control of the authorised System administrators and the authorised administrators.

These activities are documented in:

- StealthWatch On-Line Help (version 3.3.0)
- StealthWatch Owner's Manual (version 3.3.0)
- Lancope Customer Release Notes for StealthWatch Appliance (SWA) and StealthWatch + Therminator (SW+T) v3.3.0
- StealthWatch Configuration Guide (version 3.3.0)

The Guidance documents assurance measure satisfies the following EAL 2 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

### 6.2.5 Life cycle support

Lancope has a series of procedures that define the process for accepting and acting upon user reports of security flaws. These procedures describe the acceptance criteria for security flaws, how all security flaws are tracked and the status of the fix for each security flaw.

In addition, the flaw remediation procedures describe how fixes are reviewed to ensure that they do not introduce new security flaws and how the fixes for security flaws are issued to Lancope customers.

These activities are documented in:

- Flaw Remediation Procedure for StealthWatch Products

The Life cycle support assurance measure satisfies the following assurance requirement, exceeding EAL2:

- ALC_FLR.2

### 6.2.6 Tests

The Test Documentation is found in the following documents:

- Test Plan for StealthWatch Appliance and StealthWatch + Therminator, V3.3.0
- Executed Test Plan for StealthWatch Appliance (SWA) and StealthWatch + Therminator (SW+T), Release V3.3.0
- Addendum-1 to Executed Test Plan for StealthWatch Appliance (SWA) and StealthWatch + Therminator (SW+T), Release V3.3.0
- Test Coverage Analysis for StealthWatch Appliance (SWA) and StealthWatch + Therminator (SW+T), Release V3.3.0

These documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

The Tests assurance measure satisfies the following EAL 2 assurance requirements:

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

### 6.2.7 Vulnerability assessment

Lancope performs vulnerability analyses of the TOE to identify weaknesses that can be exploited in the TOE. All of the SOF claims are based on password space calculations and based on the SOF rationale provided in the Vulnerability Assessment. The vulnerability analysis is documented in:

- Vulnerability Assessment for StealthWatch Appliance and StealthWatch + Therminator, Release Version 3.3.0

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

- AVA_SOF.1; and,
- AVA_VLA.1.

# 7. Protection Profile Claims

The TOE conforms to the US Government Intrusion Detection System System Protection Profile, Version 1.4, February 4, 2002.

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. However, the following assumption has been added:

- A.ITNET – this assumption has been added to address threats that might be associated with communication among management interfaces. The TOE is designed to be managed using a web browser. These network capabilities are supported on a TOE network connection distinct from network connections monitored by the TOE. This assumption does not diminish conformance with the PP since this network can readily be isolated and protected (e.g., physically) to provide the necessary TOE protections while not imposing any restrictions or conditions on the primary objective of the TOE - to monitor other networks.

This Security Target includes all of the Security Objectives from the PP, verbatim. However, the following security objective for the IT environment has been added:

- O.PLTFRM – this objective was added to support A.ITNET and also ensure that the portion of the IT environment providing operational support is adequate and adequately protected.

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

### Interpretations

The following changes have been made to requirements based on International Interpretations. These interpretations have no impact on conformance with the PP since they only serve to clarify one of the assurance claims.

- FAU_STG.2 – an element was modified per International Interpretation RI #141
- ACM_CAP.2 – a new element was added to this component per International Interpretation RI #003.
- ADO_IGS.1 – an element was replaced per International Interpretation RI #051 (rev 1).
- ALC_FLR.2 – one element was modified and another element was added per International Interpretation RI #094.
- AVA_VLA.1 – three elements were replaced per International Interpretation RI #051 (rev 1).

# 8. Rationale

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

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- TOE Summary Specification;
- Security Functional Requirement Dependencies; and
- Internal Consistency.

## 8.1 Security Objectives Rationale

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

### 8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

| | O.PROTCT | O.IDSCAN | O.IDSENS | O.IDANLZ | O.RESPON | O.EADMIN | O.ACCESS | O.IDAUTH | O.OFLOWS | O.AUDITS | O.INTEGR | O.INSTAL | O.PHYCAL | O.CREDEN | O.PERSON | O.INTROP | O.PLTFRM |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A.ACCESS** | | | | | | | | | | | | | | | | X | X |
| **A.DYNMIC** | | | | | | | | | | | | | | | X | X | |
| **A.ASCOPE** | | | | | | | | | | | | | | | | X | |
| **A.PROTCT** | | | | | | | | | | | | | X | | | | X |
| **A.LOCATE** | | | | | | | | | | | | | X | | | | X |
| **A.ITNET** | | | | | | | | | | | | | | | | | X |
| **A.MANAGE** | | | | | | | | | | | | | | | X | | |
| **A.NOEVIL** | | | | | | | | | | | | X | X | X | | | |
| **A.NOTRST** | | | | | | | | | | | | | X | X | | | |
| **T.COMINT** | X | | | | | | X | X | | | X | | | | | | |
| **T.COMDIS** | 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 | | | | | | | | | | | | |

| | O.PROTCT | O.IDSCAN | O.IDSENS | O.IDANLZ | O.RESPO | O.EADM | O.ACCESS | O.IDAUTH | O.OFLO | O.AUDITS | O.INTEGR | O.INSTAL | O.PHYCAL | O.CREDE | O.PERSO | O.INTRO | O.PLTFRM |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **T.FALREC** | | | | X | | | | | | | | | | | | | |
| **T.FALASC** | | | | X | | | | | | | | | | | | | |
| **T.MISUSE** | | | X | | | | | | | | | | | | | | |
| **T.INADVE** | | | X | | | | | | | | | | | | | | |
| **T.MISACT** | | | X | | | | | | | | | | | | | | |
| **P.DETECT** | | X | X | | | | | | | X | | | | | | | |
| **P.ANALYZ** | | | | X | | | | | | | | | | | | | |
| **P.MANAGE** | X | | | | | X | X | X | | | | X | | X | X | | |
| **P.ACCESS** | X | | | | | | X | X | | | | | | | | | |
| **P.ACCACT** | | | | | | | | X | | X | | | | | | | |
| **P.INTGTY** | | | | | | | | | | | X | | | | | | |
| **P.PROTCT** | | | | | | | | | X | | | | X | | | | |

Table 5 Environment to Objective Correspondence

#### 8.1.1.1 A.ACCESS

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

The O.INTROP objective ensures the TOE has the needed access. The O.PLTFRM objective additionally ensures that the IT environment, where the TOE is embedded, provides the necessary operational services to perform properly.

#### 8.1.1.2 A.DYNMIC

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

The O.INTROP objective ensures the TOE has the proper access to the IT System. The O.PERSON objective ensures that the TOE will managed appropriately.

#### 8.1.1.3 A.ASCOPE

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

The O.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

#### 8.1.1.4 A.PROTCT

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

The O.PHYCAL provides for the physical protection of the TOE hardware and software. The O.PLTFRM objective additionally ensures that the IT environment, where the TOE is embedded, is similarly protected.

#### 8.1.1.5 A.LOCATE

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

The O.PHYCAL provides for the physical protection of the TOE. The O.PLTFRM objective additionally ensures that the IT environment, where the TOE is embedded, is similarly protected.

#### 8.1.1.6 A.ITNET

*Any network resources used for communication between TOE components or for network-based TOE management will be adequately protected from unauthorised access and will provide necessary services without impacting the ability of the TOE to implement its security functions.*

The O.PLTFRM objective ensures that the IT environment relied upon to provide connection among TOE components and TOE management interfaces is protected and will not negatively impact the ability of the TOE to function properly.

#### 8.1.1.7 A.MANAGE

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

The O.PERSON objective ensures all authorised administrators are qualified and trained to manage the TOE.

#### 8.1.1.8 A.NOEVIL

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

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

#### 8.1.1.9 A.NOTRST

*The TOE can only be accessed by authorised users.*

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

#### 8.1.1.10 T.COMINT

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

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

#### 8.1.1.11 T.COMDIS

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

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

#### 8.1.1.12 T.LOSSOF

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

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

#### 8.1.1.13 T.NOHALT

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

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorised users to access TOE functions. 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.

#### 8.1.1.14 T.PRIVIL

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

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

#### 8.1.1.15 T.IMPCON

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

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

#### 8.1.1.16 T.INFLUX

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

The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.

#### 8.1.1.17 T.FACCNT

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

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

#### 8.1.1.18 T.SCNCFG

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

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.

#### 8.1.1.19 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.*

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.

#### 8.1.1.20 T.SCNVUL

*Vulnerabilities may exist in the IT System the TOE monitors.*

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.

#### 8.1.1.21 T.FALACT

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

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

#### 8.1.1.22 T.FALREC

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

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

#### 8.1.1.23 T.FALASC

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

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

#### 8.1.1.24 T.MISUSE

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

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

#### 8.1.1.25 T.INADVE

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

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

#### 8.1.1.26 T.MISACT

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

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

#### 8.1.1.27 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.*

The O.AUDITS, O.IDSENS, and O.IDSCAN objectives address this policy by requiring collection of audit, Sensor, and Scanner data.

#### 8.1.1.28 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.*

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

#### 8.1.1.29 P.MANAGE

*The TOE shall only be managed by authorised users.*

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

#### 8.1.1.30 P.ACCESS

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

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

#### 8.1.1.31 P.ACCACT

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

The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.

#### 8.1.1.32 P.INTGTY

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

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

#### 8.1.1.33 P. PROTCT

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

The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The O.PHYCAL objective protects the TOE from unauthorised physical modifications.

## 8.2 Security Requirements Rationale

This section provides evidence supporting the completeness of the components (requirements) in the Security Target. Note that Table 6 indicates the requirements that effectively satisfy the individual objectives.

The purpose of the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of the TOE in meeting security needs.

All of the SFRs have been derived from the IDSSPP. All operations completed in this Security Target have been completed in accordance with the IDSSPP.

### 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 for which 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FAU_GEN.1 | | | | | | | | | | X | |
| FAU_SAR.1 | | | | | | X | | | | | |
| FAU_SAR.2 | | | | | | | X | X | | | |
| FAU_SAR.3 | | | | | | X | | | | | |
| FAU_SEL.1 | | | | | | X | | | | X | |
| FAU_STG.2 | X | | | | | | X | X | X | | X |
| FAU_STG.4 | | | | | | | | | X | X | |
| FIA_UAU.1 | | | | | | | X | X | | | |
| FIA_ATD.1 | | | | | | | | X | | | |
| FIA_UID.1 | | | | | | | X | X | | | |
| FMT_MOF.1 | X | | | | | | X | X | | | |
| FMT_MTD.1 | X | | | | | | X | X | | | X |
| FMT_SMR.1 | | | | | | | | X | | | |
| FPT_RVM.1 | X | | | | | X | | X | | X | X |
| FPT_SEP.1 | X | | | | | X | | X | | X | X |
| FPT_STM.1 | | | | | | | | | | X | |
| IDS_SDC.1 | | X | X | | | | | | | | |
| IDS_ANL.1 | | | | X | | | | | | | |
| IDS_RCT.1 | | | | | X | | | | | | |
| IDS_RDR.1 | | | | | | X | X | X | | | |
| IDS_STG.1 | X | | | | | | X | X | X | | X |
| IDS_STG.2 | | | | | | | | | X | | |

Table 6 Objective to Requirement Correspondence

#### 8.2.1.1 O.PROTCT

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

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 unauthorised 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 authorised users of the TOE [FMT_MOF.1]. Only authorised administrators of the System may query and add System and audit data, and authorised administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.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.*

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.*

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).*

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.*

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.*

The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1, FAU_SAR.3, FAU_SEL.1]. The System must provide the ability for authorised 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 [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1]

#### 8.2.1.7 O.ACCESS

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

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The 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 unauthorised deletion [IDS_STG.1]. Users authorised to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorised users of the TOE [FMT_MOF.1]. Only authorised administrators of the System may query and add System and audit data, and authorised administrators of the TOE may query and modify all other TOE data [FMT_MTD.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.*

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 unauthorised deletion [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorised 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 authorised to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorised users of the TOE [FMT_MOF.1]. Only authorised administrators of the System may query and add System and audit data, and authorised administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

#### 8.2.1.9 O.OFLOWS

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

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 the audit trail is full [FAU_STG.4]. The System is required to protect the System data from any modification and unauthorised 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.*

Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. The TOE must prevent the loss of collected data in the event the audit trail is full [FAU_STG.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.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.*

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 unauthorised deletion [IDS_STG.1]. Only authorised administrators of the System may query or add audit and System data [FMT_MTD.1]. The System must protect the collected data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1]. The TOE must ensure that all functions to protect the data are not bypassed [FPT_RVM.1]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1].

## 8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL2 assurance package augmented with ALC_FLR.2. The CC permits assurance packages to be augmented, which allows the addition of assurance components from the CC not already included in the EAL. Augmentation was chosen to provide the added assurance acquired by defining flaw remediation procedures and correcting security flaws. This ST is based on good commercial development practices to provide a low to moderate level of assurance. 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. Note that the security environment assumes physical protection. The TOE itself offers a very limited interface that can only be configured during initialization, offering essentially no opportunity for an attacker to subvert the security policies without physical access. As such, it is believed that EAL 2, augmented with ALC_FLR.2, provides an appropriate level of assurance in the security functions offered by the TOE.

## 8.4 Requirement Dependency Rationale

The ST satisfies all the requirement dependencies of the Common Criteria. Table 7 Requirement Dependencies Rationale lists each requirement from Section 5.1 with a dependency and indicates which requirement was included to satisfy the dependency. For each dependency not included, a justification is proved.

| Functional Component | Dependency | Included |
|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | YES |
| FAU_SAR.1 | FAU_GEN.1 | YES |
| FAU_SAR.2 | FAU_SAR.1 | YES |
| FAU_SAR.3 | FAU_SAR.1 | YES |
| FAU_SEL.1 | FAU_GEN.1 and FMT_MTD.1 | YES |
| FAU_STG.2 | FAU_GEN.1 | YES |
| FAU_STG.4 | FAU_STG.1 | NO |
| FIA_UAU.1 | FIA_UID.1 | YES |
| FMT_MOF.1 | FMT_SMR.1 | YES |
| FMT_MTD.1 | FMT_SMR.1 | YES |
| FMT_SMR.1 | FIA_UID.1 | YES |

Table 7 Requirement Dependencies Rationale

FAU_STG.4 includes a dependency on FAU_STG.1. FAU_STG.1 is not included in this ST, however FAU_STG.2 (which is hierarchical to FAU_STG.1) is included and satisfies the dependency.

International Interpretation, RI #65 adds a new dependency of FMT_SMF.1 to FMT_MOF.1 and FMT_MTD.1. FMT_SMF.1 has not been added to this ST because the IDSSPP was evaluated and it was concluded that the IDSSPP contained all the management requirements it needed to satisfy the PP objectives. Therefore, the FMT_SMF.1 requirement is not necessary to meet any PP objectives and has not been included in this ST.

## 8.5 Explicitly Stated Requirements Rationale

A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

## 8.6 Strength of Function Rationale

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

## 8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. 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.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. Table 8 Security Functions vs. Requirements Mapping demonstrates the relationship between security requirements and security functions.

| | Security Audit | Identification & Authentication | Security Management | Protection of TOE Security Functions | 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_UAU.1** | | X | | | |
| **FIA_ATD.1** | | X | | | |
| **FIA_UID.1** | | X | | | |
| **FMT_MOF.1** | | | X | | |
| **FMT_MTD.1** | | | X | | |
| **FMT_SMR.1** | | | X | | |
| **FPT_RVM.1** | | | | X | |
| **FPT_SEP.1** | | | | X | |
| **FPT_STM.1** | | | | X | |
| **IDS_SDC.1** | | | | | X |
| **IDS_ANL.1** | | | | | X |
| **IDS_RCT.1** | | | | | X |
| **IDS_RDR.1** | | | | | X |
| **IDS_STG.1** | | | | | X |
| **IDS_STG.2** | | | | | X |

Table 8 Security Functions vs. Requirements Mapping

## 8.8 PP Claims Rationale

- See section 7, Protection Profile Claims.