National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Lancope StealthWatch and StealthWatch + Therminator Appliances containing StealthWatch version 3.3.0 – Build 4140 Software

Report Number: CCEVS-VR-04-0064
Dated: 30 June 2004
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team
Margaret T. Webster-Butler
Rashida F. Doss
National Security Agency
Ft. Meade, MD 20755

Common Criteria Testing Laboratory

Evaluation Team
Science Applications International Corporation
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

Table of Contents

Executive Summary

The Target of Evaluation (TOE) is the Lancope StealthWatch and StealthWatch + Therminator appliances containing StealthWatch version 3.3.0 – Build 4140 intrusion detection software. The TOE was evaluated by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in the United States, beginning on September 29, 2003, and completed on June 30, 2004. The evaluation was for the Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.2. The evaluation was conducted in conformance with the Common Criteria (CC) for Information Technology Security Evaluation, parts 1, 2, 2a, and 3; and, the Common Evaluation Methodology for Information Technology Security (CEM), parts 1 and 2. The evaluation was conducted in accordance with the rules and regulations of the NIAP Common Criteria Evaluation and Validation Scheme, and the conclusions of SAIC in their Evaluation Technical Report (ETR) were consistent with the evidence adduced. SAIC concluded that the Common Criteria requirements of EAL2 augmented with ALC_FLR.2 had been met for the TOE.

The TOE is defined as the Lancope StealthWatch and StealthWatch + Therminator appliances containing StealthWatch version 3.3.0 – Build 4140 intrusion detection software. 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). From the available product models, these appliances were used in testing:

a) StealthWatch Appliance Model M250x
b) StealthWatch Appliance Model G1
c) StealthWatch + Therminator Appliance Model G1cx
d) StealthWatch + Therminator Appliance Model M45.

The TOE claims and meets conformance to the Intrusion Detection System System Protection Profile, Version 1.4, February 4, 2002 (IDSSPP).

The Lancope StealthWatch Security Target (ST) version 1.0 dated July 14, 2004, identifies the specific version and build of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the Lancope StealthWatch product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

1.1. Evaluation Highlights

Dates of Evaluation: September 29, 2003 through June 30, 2004
Evaluated Product: Lancope StealthWatch and StealthWatch + Therminator Appliances containing StealthWatch version 3.3.0 Build 4140 Software
Developer: Lancope Incorporated, 3650 Brookside Parkway, Suite 400, Alpharetta, Georgia, 30022
CCTL: SAIC, 7125 Columbia Gateway Drive, Suite 300, Columbia, Maryland 21046
Evaluation Class: EAL2 augmented with ALC_FLR.2
PPs Claimed: IDSSPP
Validation Team: Margaret T. Webster-Butler and Rashida F. Doss, National Security Agency

2. Product Identification

ST: Lancope StealthWatch version 1.0 dated July 14, 2004

TOE Identification: Lancope StealthWatch and StealthWatch + Therminator appliances containing StealthWatch version 3.3.0 – Build 4140 intrusion detection software

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

3. Security Policy

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. The TOE 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. It characterizes and analyzes the data that flows between Internet Protocol (IP) devices on the network to differentiate abnormal network behavior from normal network behavior without examining the contents of each packet that traverses the network

The TOE implements the following security policies:

Identification and Authentication Policy:
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. Administrative guidance defines the assignment of these user identities.

Security Audit Policy:
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.

Security Management Policy:
The TOE provides a secure web-based (utilizing SSL) management interface for all three classes of users performing administrative tasks.
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.

Protection of the TOE Security Functions Policy:
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.

System Data Collection Policy:
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 found under System Data Analysis and Reaction Policy.

System Data Analysis and Reaction Policy:
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.

System Data Review, Availability, and Loss Policy:
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.

4. Assumptions and Threats, Clarification of Scope and Interpretations

4.1 Usage Assumptions and Threats

With one exception, the assumptions, threats and organizational security policies are taken from the IDSSPP. The ST includes one additional physical assumption, A.ITNET and its corresponding objective, O.PLTFRM with the following rationale for each:

- 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.

- 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.

4.2 Clarification of Scope

In addition to the additional Assumption and its corresponding Objective stated above, other changes have been made in the ST, but compliance to the IDSSPP is still maintained. 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. They were dropped because the TOE has no communication with external IT products and the SFRs were deemed 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 that the O.EXPORT objective was erroneously replicated into the IDSSPP. Therefore, this ST deleted the O.EXPORT objective in order 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. FPT_ITT.1 was not included in the SFRs because this TOE is not a distributed one.

4.3 Interpretations

Based on International Interpretations, changes were made within the ST. These interpretations had no impact on conformance to the IDSSPP since they only served to clarify assurance claims. The following sections provide the title and number of the applicable interpretations and the CEM class in which they were considered.

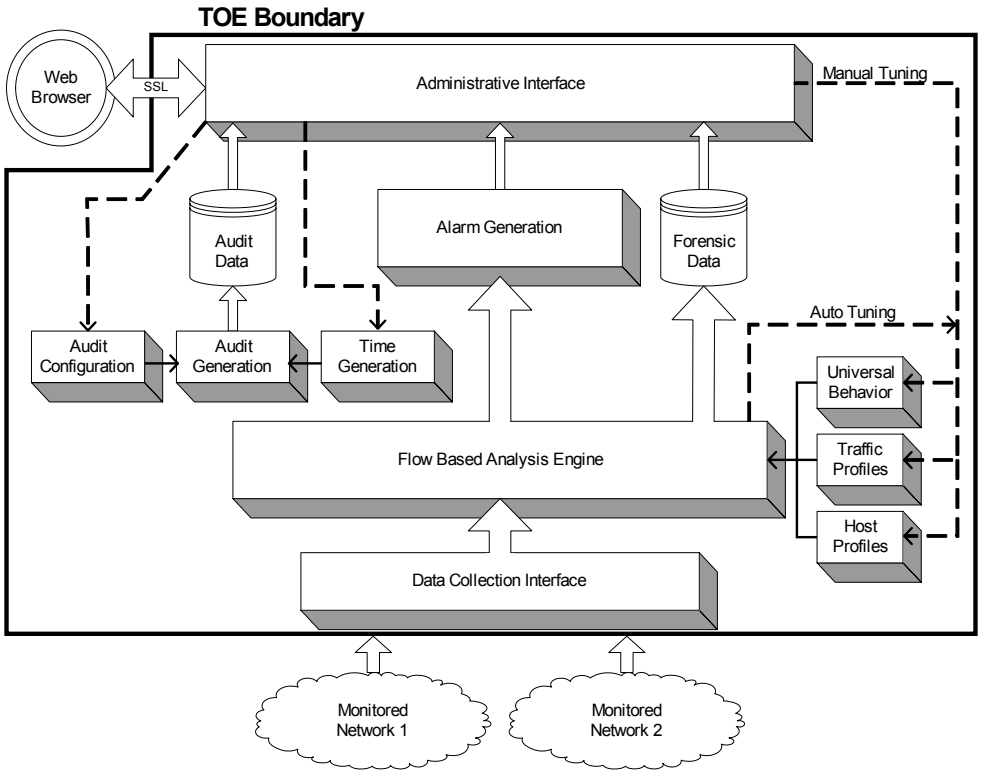
1. Separate objectives for TOE and environment (084) - ASE
2. Level of detail required for hardware descriptions (025) - ADV
3. Unique Configuration of CIs (003) – ACM
4. Underlying Hardware and Firmware (006) – ADV
5. Augmented and Conformant Overlap (008) – ASE
6. Deliver procedures may include confidentiality (016) - ADO
7. Evidence is required of entire TOE (024) – ADV
8. Events and actions (027) – AGD
9. Vulnerabilities not in TOE not applicable (031) – AVA
10. SOF analysis need not be in ST (032)
11. CM applicable to TOE (037) – ACM

12. CM requirement modified (038) – ASE
13. ADO_IGS and AVA_VLA requirements modified (051) – ASE
14. FMT_SMR (new requirement) as a dependency of FMT_MOF (065) – ASE, ADV
15. FAU_STG.2 modified (141) – ASE, ADV
16. FAU_GEN.1 permits the selection of only one options (202) – ASE, ADV

5. Architectural Information

There are six components that comprise the TOE: 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 TOE architecture.



5.1 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.

5.2 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).

6. Delivered Product

The evaluation team selected the G1 appliance to be delivered to the Lancope Facility for this evaluation, which consisted of the following:

1. The package was delivered to Lancope with the tamper seal of their name on the seams of the appliance.
2. The package contained a sealed envelope, a rack, the power cords, and Ethernet cord.
3. The sealed envelope contained the configured default user name and password; a CD labeled with the TOE version; and a hard copy of the Quick Start Configuration Checklist and the Release Notes both labeled with the TOE version.
4. The CD contents were the Owner's Manual, Configuration Guide, and Quick Start Configuration Checklist, all labeled with the TOE version.

7. IT Product Testing

7.1 Examination of Vendor Tests

Testing of the TOE security functions is provided by a series of manual tests provided by the vendor, Lancope. These tests demonstrate the security-relevant behavior of the TOE for the external interfaces defined in the Functional Specification and High-Level Design. The goal of these tests is to demonstrate that the TOE meets the security functional requirements that are specified in the Security Target. The security functions tested were Security Audit, User Data Protection; Identification and Authentication; Security Management; Protection of TOE Security Functions; and Intrusion Detection System.

Based upon the vendor test documentation, there are a total of 28 tests related to the security functions claimed in the security target. The total amount of vendor tests run by the evaluation team was 12. This number of tests makes the coverage of tests run by the evaluation team over 20% of the total amount of tests stated to be an acceptable percentage per CEM guidance for ATE_IND.2-9 (para 1656). The tests listed in this section are categorized according to the security function that is being tested. For each test case run, the evaluation team completed the Actual Results column in the table with a "P" (Pass) or an "F" (Fail). The model that each test case was run on and the results are summarized in the table below.

No.	Security Function	Test Section	Test Procedures	Actual Results P/F			
				M45	G1cx	G1	M250x
1	Security Audit	3.1.1	Audit Generation [FAU_GEN.1]	P	P	P	P
2		3.1.2	Audit Fields [FAU_GEN.1]	P	P	P	P
3	Identification and Authentication	3.2.3	Attribute Definition [FIA_ATD.1]	P	P	P	P
4	Security Management	3.3.1	Administrative Accounts [FMT_MOF.1]	P	P	P	P

5		3.3.3	Security Roles [FMT_SMR.1]	P	P	P	P
6	Protection of Security Functions	3.4.4	Non-bypassibility [FPT_RVM.1]]	P	P	P	P
7		3.4.5	Safe Domain [FPT_SEP.1]	P	P	P	P
8	Intrusion Detection System	4.1.1	System Data Collection [IDS_SDC.1]	P	P	P	P
9		4.1.2	System Data Format [IDS_SDC.1]	P	P	P	P
10		4.2.1	Analyzer Analysis [IDS_ANL.1]	P	P	P	P
11		4.3.1	Restricted Data Review [IDS_RDR.1]	P	P	P	P
12		4.3.3	Prevention of Data Loss [IDS_STG.2]]	P	P	P	P

The expected results had already been examined by the evaluation team to be sufficient as justified in the ATE ETR. A "P" in the Actual Results column of the above table indicates that the actual results for the associated test case were found to be equivalent to the expected results in the Test Plan document.

7.2 Evaluation Team Independent Tests

The evaluation team performed a subset of twelve of Lancope's functional tests that were provided. In addition, the evaluation team used the provided tests to create additional and enhanced independent tests. The evaluation team tests listed in this section are also categorized according to the security function that was tested. The evaluation team used the same test configuration used to perform the vendor's test subset to perform their team independent test. For each test, the evaluation team completed the Actual Results column with a "P" (Pass) or an "F" (Fail). The model that each test case was run on and the results are summarized in the table

below. A "P" in the Actual Results column of the table indicates that the actual results for the associated test case were found to be equivalent to the evaluation team's expectation of what the results should be.

No.	Security Function	Test Procedures	Actual Results P/F			
			M45	G1cx	G1	M250x
1	Security Audit	Audit Generation - FAU_GEN.1	P	P	P	P
2		Audit Selection - FAU_SEL.1 (with vendor update)	P	See Note 1		P
3		Audit Storage – FAU_STG.2, FAU_STG.4	P	P	See Note 2	P
4	Identification and Authentication	FIA_UAU.1, FIA_ATD.1	P	P		P
5	Protection of Security Functions	Reliable Time Stamp – FPT_STM.1	P	P		P
6	Intrusion Detection System	Restricted Data Review - IDS_RDR.1	P	P		P

Note1: The initial run of the FAU_SEL.1 team test exposed a bug in the TOE software where the audit records were generated for events that were deselected, thus FAU_SEL.1 failed the initial performance of the team test. The vendor resolved the bug, re-built the TOE, created an addendum to their Test Plan to verify that the bug as been resolved and installed the new TOE software on the M45 and M250x. The team was able to successfully run the team test case for FAU_SEL.1.

The vendor included an addendum to the Test Plan, which tests the TOE to ensure the bug is resolved:

- *Addendum-1 to Executed Test Plan for StealthWatch Appliance and StealthWatch + Therminator Release Version 3.3.0, 05/20/2004*

To ensure that the new build of the TOE software still included the same functionalities, the team test cases for FIA_UAU.1, FIA_ATD.1, and IDS_RDR.1 were re-run. The tests were successfully executed gaining the same results as were received previously.

Note2: With the exception of FAU_GEN.1, the remaining team test cases could not be run on the G1 product. During the running of the vendor test subset by the evaluation team, one of the test preparation steps for IDS_STG.2 was incorrectly performed which caused the TOE to later fail during team test, exposing a vulnerability of the TOE's environment. This vulnerability was due to the inclusion of the secure shell program, which was only used for testing purposes. The secure shell software is not included in the delivered appliances.

7.3 Strength of Function

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behavior can be made using the results of a quantitative or statistical analysis of the security behavior of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim. The overall SOF claim for the TOE made in this ST was expressed as a basic SOF rating.

According to the Common Evaluation Methodology Part2, Annex B.8, Para. 1849 "A minimum claim of SOF-basic is required wherever components for AVA_SOF are claimed." This fact, and the Common Evaluation Methodology Part2, Annex B.8, Table B-2, "a SOF rating of SOF-basic is adequate protection against an attacker with an attack potential of low", led the evaluator to concur with the developer's SOF claim. The calculations were performed independently by the evaluation team and found to equal the results in the developer analysis. The validation team concurred with these findings.

7.4 Vulnerability Analysis

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate any TOE Security Policies.

The evaluation team conducted the following independent vulnerability tests:

1. A test to determine if a logged in user can continue to have access when the user is deleted
2. Verify that the shell access is not present in the customer's delivered version of the product.
3. Verification that the TOE will still function properly when the disk space is exhausted.
4. Simulate a denial of service attack, where high volume of network traffic bombards the TOE.

In all cases, the evaluators' expected results were in line with the actual results.

8. Evaluated Configuration

Of the available models, the evaluated configurations that were used to test models of the TOE were:

- StealthWatch Appliance Model M250x
- StealthWatch Appliance Model G1
- StealthWatch + Therminator Appliance Model G1cx
- StealthWatch + Therminator Appliance Model M45
- PC computer running Windows XP
- PC computer running Linux
- PC computer running Linux used to generate network packets
- 2 Hubs
- Monitor and keyboard used for direct connection to appliances
- Network cables

The evaluation team provided rationale to justify that the models used sufficiently represented a subset of the StealthWatch Appliance suite.

9. Results of the Evaluation

The validator followed the procedures outlined in the Common Criteria Evaluation Scheme [CCEVS] publication number 3 for Technical Oversight and Validation Procedures (CCEVS_PUB 3). The validator observed that the evaluation and all of its activities were in accordance with the CC, the CEM and CCEVS. The validator therefore, concludes that the evaluation and its results of **Pass** are complete.

9.1 Assurance Content

The evaluation provides for Assurance at the EAL 2 level with ALC_FLR.2 augmentation. The assurance components are shown in the table below:

EAL2 Augmented with ALC_FLR.2 Assurance Requirements

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_CAP.2 Configuration items
Delivery and Operation (ADO)	ADO_DEL.1 Delivery Procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life Cycle Support (ALC)	ALC_FLR.2 Flaw reporting procedures
Tests (ATE)	ATE_COV.1 Evidence of Coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample

Vulnerability assessment (AVA)	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

10.Validator Comments/Recommendations

Comments:

The TOE is largely comprised of software. However, the security relevant aspect of the operating system and underlying hardware was included in the evaluation (i.e., they are part of the TOE) in order to provide reliable time stamp information for conformance to the Intrusion Detection System System Protection Profile, Version 1.4, February 4, 2002 (IDSSPP).

Recommendation:

This evaluation shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The product has been evaluated at the assurance level of EAL 2 augmented with ALC_FLR.2 and it has been determined that it meets its functional claims.

The validators observed that the evaluation and all of its activities were in accordance with the CC the CEM, and CCEVS practices; and that the CCTL presented appropriate CEM work units and rationale. The validators therefore conclude that the evaluation and its results of **Pass** are complete and correct.

11. Security Target

The Security Target is provided separately.

ST: Lancope StealthWatch Security Target v1.0, dated 14 July 2004.

12. List Of Acronyms And Glossary Of Terms

The following acronyms are provided for reference:

ACM	Assurance Configuration Management
ADO	Assurance Delivery and Operation
AGD	Assurance Guidance Documents
ADV	Assurance Development
ATE	Assurance Tests
AVA	Assurance Vulnerability Assessment
CC	Evaluation Criteria for Information Technology Security (Common Criteria)
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CI	Concern Index
DOS	Denial Of Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
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)
PP	Protection Profile
RPC	Remote Procedure Call
SAIC	Science Applications International Corporation
SF	Security Functions
SFR	Security Functional Requirements
SFP	Security Function Policy
ST	Security Target
SWA	StealthWatch Appliance
SW+T	StealthWatch + Therminator
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	Target of Evaluation Security Functions
TSP	TOE Security Policy
UDP	User Datagram Protocol

UI	User Interface
URI	Uniform Resource Identifier

The following terms are provided for reference:

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions (TSF) - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP) - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

13. Documentation

The evidence used in this evaluation is based upon the product and the following documentation:

Lancope StealthWatch Security Target v 1.0 dated 14 July 2004;

SAIC ETRs for ACM_CAP.2, ADO_DEL.1, ADO_IGS.1, ADV_FSP.1, ADV_HLD.1, ADV_RCR.1, ADG_ADM.1, AGD_USR.1, ALC_FLR.2, ATE_COV.1, ATE_FUN.1, ATE_IND.2, AVA_SOF.1, AVA_VLA.1 assurance requirements and ASE_ENV.1, ASE_OBJ.1, ASE_REQ.1, ASE_SRE.1, ASE_PPC.1, ASE_TSS.1, ASE_INT.1, ASE_DES.1 for ST evaluation;

Intrusion Detection System System Protection Profile v1.4, dated 4 February 2002;

CCEVS-OR-0231;

StealthWatch Configuration Management Procedure, version 1.2, 11/21/03;

StealthWatch Configuration Item List, StealthWatch Appliance version 1.5, 05/27/04;

StealthWatch Configuration Item List, StealthWatch + Therminator version 1.5, 05/27/04;

StealthWatch Owner's Manual version 3.3.0, April 28, 2004;

Lancope Customer Release Notes for StealthWatch™ Appliance (SWA) and StealthWatch + Therminator™ (SW+T) v3.3.0, May 27, 2004;

StealthWatch Configuration Guide version 3.3.0;

StealthWatch v3.3 Online Help;

SWA Build, Test, & Delivery Process, v1.4, 4/28/04;

SWA Install Process, v1.4, 4/28/04;

StealthWatch Quick Start Configuration Checklist, SWA v3.3.0;

Functional Specification for StealthWatch Appliance (SWA) and StealthWatch + Therminator (SW+T), Release V3.3.0, v1.7, 05/27/2004;

High Level Design Document for StealthWatch Appliance (SWA) and StealthWatch +

Therminator (SW+T), Release V3.3.0, v1.5, 5/27/04;

Correspondence Document for StealthWatch Appliance (SWA) and StealthWatch + Therminator (SW+T), Release V3.3.0, v1.3, 4/30/04;

Flaw Remediation Procedure for StealthWatch Products, v1.6, 2/06/04;

Test Plan for StealthWatch Appliance and StealthWatch + Therminator (SW+T) Release v3.3.0 v1.9, 05/20/2004;

Executed Test Plan for StealthWatch Appliance and StealthWatch + Therminator Release Version 3.3.0, v1.7, 05/06/2004;

Test Plan Coverage Analysis for StealthWatch Appliance and StealthWatch + Therminator Release v3.3.0, v1.0, 05/05/2004;

Addedum-1 to Executed Test Plan for StealthWatch Appliance and StealthWatch + Therminator Release Version 3.3.0, v1.7, 05/20/2004;

Vulnerability Assessment for StealthWatch Appliance (SWA) and StealthWatch + Therminator (SW+T), Release V3.3.0, v1.4, 05/20/04;

SAIC Evaluation Team Test Plan;

SAIC Final ETR Part I (Non-Proprietary);

SAIC Final ETR Part I (Proprietary);

SAIC Final ETR Part II (Proprietary).

.

The evaluation and validation methodology was drawn from the following:

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, version 2.1.

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1.

[CC_PART2A] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, version 2.1.

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_PART1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[CCEVS_PUB 1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0, May 1999.

[CCEVS_PUB 2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000

[CCEVS_PUB 3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 1.0, January 2002.

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, 31 August 2000.