National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

NFR® Sentivist™ v4.0.2 Updated to v4.06 and Sentivist Sensors 310C, 320C and 320 F

Report Number: CCEVS-VR-05-0100

Dated: 15 April 2005

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

Jandria Alexander

The Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

Arca Common Criteria Testing Laboratory

SAVVIS Communications

Sterling, Virginia

Table of Contents

1 EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the CCEVS evaluation of the NFR® Sentivist™ v4.0.2 (Sentivist™) and Sentivist Sensors 310C, 320C and 320F Models intrusion detection system. The evaluation was performed by the Arca Common Criteria Testing Laboratory. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by Arca and submitted to the validators. The evaluation determined that the product conforms to the Common Criteria Version 2.1, Part 2 extended and Part 3.

The TOE is a NFR Security, Inc. network-based Intrusion Detection System that monitors traffic in real-time. The Sentivist analyzes each packet. Raw packets are captured and compared against signatures of known attacks. These signatures can be edited by authorized administrators and operators of the Sentivist™. The Sentivist™ uses protocol analysis and anomaly detection techniques to determine previously undiscovered attacks and check for unexpected activity and deviations from coded standards in its knowledge base.

The Sentivist™ consists of three components. The Sentivist™ Sensor (vendor-supplied hardware and software); the Sentivist™ Server (vendor supplied software installed on customer-supplied hardware and operating system); and the Sentivist™ Administration Interface.

The following features have been excluded from the Common Criteria Evaluated Configuration of the Sentivist.

- Command Line Query tool is prepackaged with the Sentivist Server product distribution CD – Installing and Using Command Line Query, NFR Sentivist Getting Started Guide. This feature of the Sentivist is not a part of the evaluated configuration of the TOE and hence should not be used in the Common Criteria Evaluated Configuration of the Sentivist.

- The Alert Continuity Installation Option of the Sentivist by installing a Backup Sentivist Server as detailed on Page 3 – Sentivist Sensor Installation Options, in the NFR Sentivist Getting Started Guide should not be used under the Common Criteria Evaluated Configuration of the Sentivist.

- Sentivist Enterprise Console Version 4.0 provided along with NFR Sentivist Version 4.0.2 – Updated to v4.0.6.

- Sentivist DBExport feature

- SAM (Suspicious Activity Monitoring) Client Integration with Checkpoint VPN-1/Firewall-1 and firewall updates feature

- NFR Plus for Tivoli SecureWay Risk Manager Feature

- NFR Integration Module for HP OpenView Operations

- Ethereal – Network Protocol Analyzer V 0.9.13a which comes with the NFR Sentivist V4.0.2 – Updated to v4.0.6

- WinPcap 3.0 – Packet Capture Utility which comes with the NFR Sentivist V4.0.2 – Updated to v4.0.6

- The sha1sum program used to create an encrypted password for the Sentivist Sensor Administrator.

- Software only version of the Sentivist Sensor is not a part of the evaluated configuration of the TOE

The validation team observed the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team's observations support the conclusion that the product satisfies the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the validation team concludes that the findings of the evaluation team are accurate, and the conclusions justified.

2 IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant (if applicable);
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	NFR Sentivist™ v4.0.2 and Sentivist Sensor Models 310C, 320C and 320F
Protection Profile	Intrusion Detection System System Protection Profile, Version 1.4, February 4, 2002.
Security Target	NFR Sentivist Version 4.02-Updated to v4.06 and Sentivist Sensor Models 310C, 320C and 320F Security Target, April 18, 2005
Evaluation Technical Report	Evaluation Technical Report for NFR Sentivist Version 4.02-Updated to v4.06 and Sentivist Sensor Models 310C, 320C and 320F, March 10 2005
Conformance Result	Part 2 extended, Part 3 conformant, EAL2
Sponsor	NFR Security, Inc.
Developer	NFR Security, Inc.
Evaluators	Arca CCTL
Validators	The Aerospace Corporation

3 SECURITY POLICY

The NFR Sentivist does not implement a security policy in the traditional sense of enforcing a set of access control rules. The TOE collects, stores and manages all IDS System records.

The Security Objectives for the TOE as outlined in the IDS System PP require that:

- The TOE must protect itself from unauthorized modifications and access to its functions and data.
- The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
- The TOE must allow authorized users to access only appropriate TOE functions and data.
- The TOE must include a set of functions that allow effective management of its functions and data.
- The TOE must respond appropriately to analytical conclusions.
- 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.
- 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.
- The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
- The TOE must appropriately handle potential audit and System data storage overflows.
- The TOE must record audit records for data accesses and use of the System functions.
- The TOE must ensure the integrity of all audit and System data.
- When any IDS component or the TOE makes its data available to another IDS component, the TOE will ensure the confidentiality of the System data.

3.1 Roles

The product supports three roles: Authorized Administrator, Authorized System Administrator\nfr, and Authorized Operator.

- **Authorized Administrator** – Operating system administrator for the Sentivist™ Server, this person is responsible for the installation and configuration of the Sentivist™ Server and the underlying operating system.

- **Authorized System Administrator** – This default authorized system administrator role created during the installation of the Sentivist™ Server "nfr" has all privileges. The default user name for this role is "nfr". This role is created with all of the Access Control, Audit View, Audit Configure, Configure, Alert View, Restart Sensor, Query and Diagnostic privileges. This role is the primary role through which one can log into the Sentivist Administration Interface and create Authorized Operators, who are defined as having equal or lesser privileges than the "nfr" account. In addition to this, the "nfr" account also performs administrative functions on the Sentivist Sensor via the Sentivist Server CLI; this is accomplished during the Operations Mode of the Sentivist Sensor. It is important to note that Authorized Operators are not to log into the Command Line Interface.

- **Authorized Operator** – Authorized Operators are created by the Authorized System Administrator. Permissions control what an Authorized Operator can see and do within the Sentivist Administration Interface. The authorized operators created by the authorized system administrator can have some or all of these permissions depending on the level of access.

    - **Access Control**: Allows the user to add and delete user accounts, change user permissions, set authentication attempts for users, and unlock users.

    - **Configure**: The configure permissions controls access to the Administration, Packages, and Status shortcut bars within Sentivist Administration Interface, allowing the user to change the configuration of various components. This includes allowing the operator to configure alerts.

    - **Diagnostics:** Allows a user to retrieve diagnostic files from Sentivist Server.

    - **Audit Configure:** Allows the user to configure audit-related alerts and functions. Users with this permission have the ability to change the rules that process security- related events.

    - **Audit View:** Allows the user to see audit related alerts (records written to the auditlist) through the Alert Window or popup windows. The auditlist is designed to track events related to internal security.

    - **Query:** The query permission allows access to the Packages shortcut bar.

    - **Alert View:** The alert view permission allows viewing and receipt of alerts.

    - **Restart Sentivist Sensor:** This permission allows reboot of a Sentivist Sensor connected to a Sentivist Server

- **Sensor Box:** This allows the user to access to the Sensor in order issue the Run Mirror command to push data out to the Sensor.

Each authorized user of the TOE is assigned to one and only one role. A user account cannot be created without an associated role; if no role is specified when the user is created then the default role of viewer is assigned.

3.2 Security Management

The TOE provides security management functionality necessary to manage TOE and IDS data. This includes the ability to query TOE data, and modify the data analysis, reaction and collection parameters.

4 ASSUMPTIONS

4.1 Usage Assumptions

The evaluation made the following assumptions concerning product usage.

- The TOE has access to all the IT system data and resources it needs to perform its functions.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- The TOE is appropriately scalable to the IT System the TOE monitors.

4.2 Physical Assumptions

The evaluation made the following environmental assumptions:

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

4.3 Personnel Assumptions

The evaluation made the following personnel assumptions:

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

5 ARCHITECTURAL INFORMATION

The TOE consists of the following components:

- Sentivist™ Sensor;
- Sentivist™ Server; and
- Sentivist™ Administration Interface (SAI).

Together the subsystems provide security functionality for audit generation, selection, review and protection; identification and authentication; management of security functions; protection of TOE security functions; and, Intrusion Detection System data collection, analysis, review, reaction and protection.

Sentivist™ Sensor (Sensor):

Each Sentivist™ deployment will at least have one or more Sentivist™ Sensors, one Server and Administration Interface. The Sentivist™ Sensor is delivered as a pre-configured appliance consisting of the appropriate hardware and software combination for each Sensor model.

Sentivist™ Server (Server):

The Sentivist™ Server processes, and manages event and alert data provided from the Sentivist™ Sensors. It provides a management interface to this data for applications such as the Sentivist™ Administration Interface. The Sentivist™ Server provides services for storing and managing event, alert, and status data from the Sensor appliances. Sentivist™ Server functionality include:

- **Data Reception and Management:** Receives data from multiple Sensors. Data includes events, alerts, and status. The data is processed, stored to a local data store, and made available to external management applications.
- **Configuration Management:** Provides an agent and command line interfaces for configuration. The management agent listens for requests from management clients (SAI) and attempts to carry out their requested management commands. The Management Agent is a web-server like component on the Sentivist Server. It listens for and services the Management Client's requests via the Management interface. The management agent is the executable guisrv and a set of CGI commands. This includes configuration of Sensor appliances and NFR Administration users communicating with the Server.
- **Fault Management:** Provides alert notification to a standard communications channel or an agent for queries on the stored alert data.

Sentivist™ Administration Interface (SAI): Sentivist™ Administration Interface (SAI) provides a Microsoft Windows-based interface to Sentivist™ Server for Sentivist™ Sensor configuration, viewing and managing Sensor alerts, and performing administration tasks. A single SAI may manage multiple Sensors; multiple SAIs may manage one or more Sensors. The Sentivist Server is the central repository for all the identification and authentication mechanisms of the Sentivist Administration Interface.

6 DOCUMENTATION

Following is a table of the evaluation evidence used to support this evaluation:

Evidence

Category	Title(s)
Security Target	NFR Security, Inc. NFR® Sentivist™ v4.0.2 – Updated to v4.0.6 and Sentivist Sensors 310C, 320C and 320F Models Security Target Version 2.6 March 8, 2005
Configuration Management	NFR Security, Inc., Sentivist Version 4.0.2, Configuration Management, Version 1.7, March 8, 2005
Delivery and Operation:	NFR Security, Inc., Sentivist Version 4.0.2 – Updated to v.4.0.6, Secure Delivery Guidance, Version 1.6 March 8, 2005
	NFR Sentivist v4.0.2 – Updated to v.4.0.6, Common Criteria Wrapper Guide, Version 1.7, March 8, 2005
Design Documentation:	NFR Sentivist V4.0.2 – Updated to v4.0.6, Functional Specification, Version: 1.8, March 8, 2005
	NFR Sentivist v4.0.2 – Updated to v.4.0.6, High Level Design, Version: 1.6, March 8, 2005
	NFR Sentivist V4.0.2 – Updated to v4.0.6, Functional Specification, Version: 1.8, March 8, 2005 NFR Sentivist v4.0.2 – Updated to v.4.0.6, High Level Design, Version: 1.6, March 8, 2005
Guidance Documentation:	NFR Sentivist Getting Started Guide, v4.0.0-04.30.04
	NFR Sentivist Users Guide, v4.0.0-10.30.03
	NFR Sentivist Server v4.0.2 Release Notes
	NFR Sentivist Server v4.0.6 Release Notes
	NFR Sentivist Sensor v4.0.2 Release Notes
	NFR Sentivist Administration Interface v4.0.2 Release Notes
Test Documentation:	NFR® Security, Inc., Sentivist Version 4.0.2 - Updated to v4.0.6, Common Criteria Test Plan, Version 1.0, March 8, 2005
	NFR Sentivist v4.0.2 - Updated to v4.0.6 Consolidated Test Plan v1.0, March 8, 2005
	NFR Sentivist TM Version 4.0.2 EAL 2 Team Test Plan Version 1.4, March 7, 2005
Vulnerability and Assessment Documentation:	NFR Security, Inc., Sentivist™ Version 4.0.2 Strength of TOE Security Function Analysis, Version 0.6, March 8, 2004

Category	Title(s)
	NFR Security, Inc., Sentivist Version 4.0.2 –Updated to v.4.0.6, Vulnerability Assessment (Vulnerability Analysis), Version 1.0, March 8, 2005

7 IT PRODUCT TESTING

7.1 Vendor Testing

At EAL2 testing must demonstrate correspondence between the tests and the functional specification. However complete testing is not required; "coverage analysis need not demonstrate that all security functions have been tested, or that all external interfaces to the TSF have been tested."[1]

The vendor partially tested each security function as listed:

- Security Audit (FAU)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Protection of the TOE Security Functions (FPT)
- IDS Component Requirements (IDS)

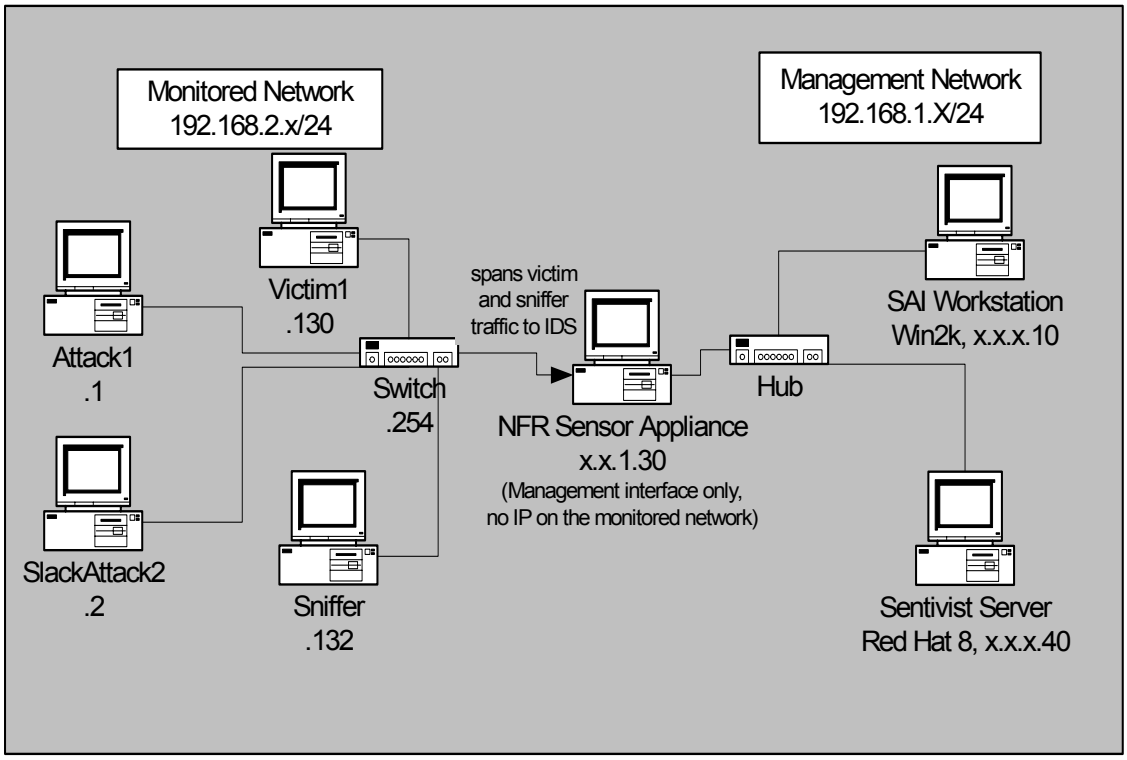
The vendor tests covered 65 of 72 TOE Security Functional Interfaces.

7.2 Evaluator Testing

The evaluation team performed the TOE installation, as specified in the Installation, Generation and Startup documentation, functional, independent and vulnerability testing. The test configuration used by the CCTL is illustrated below:

[1] CEM, V1.0, paragraph 6.8.2.2 (application note for EAL2:ATE_COV.1)

Figure 1: NFR Sentivist CCTL testing environment



Evaluator testing covered the following areas:

- Collection and detection of intrusion attacks and audit events
- TSF Self protection of data in transmission;
- Audit storage and review;
- Management roles enforcement;
- Identification and Authentication.

8 EVALUATED CONFIGURATION

The evaluation configuration consists of Sentivist™ 4.0.2 . The specific models in the include:

Sentivist™ Administration Interface: The Sentivist™ Administration Interface is required to operate under a subset of Windows operating environments. These environments are as follows:

Intel platform running the following operating systems:

- Windows 2000 Professional with Service Pack 2
- Windows XP with Service Pack 1

Minimum Hardware: The Sentivist™ Administration Interface will run on the following minimum set of hardware:

- Intel 800 MHz Pentium
- 512 MB of RAM
- 100 Mbps network connection
- 1+ GB usable disk drive

Sentivist™ Server: The Sentivist™ Server is required to operate under a subset of UNIX operating environment. These operating environments are defined as follows.

Intel platform running the following operating systems:

- Red Hat Linux 7.3.
- Red Hat Linux 8.0.

Sun SPARC platform running the following operating systems:

- Solaris 8
- Solaris 9

Minimum Hardware: The Sentivist™ Server must perform to an acceptable level on the following minimum sets of hardware:

- Red Hat Linux 7.3 or 8.0 running on the following hardware:
  - 1.4 GHz Pentium class machine
  - 1GB of RAM

- Hard Disk Drive: Multiple SCSI drives in RAID 0+1, 1, or 5 configuration (10GB usable)
- 100 Mbps network connection

- Solaris 8 or 9 running on the following hardware:
  - 400 MHz UltraSparc CPU
  - 2 GB of RAM
  - Multiple SCSI drives in RAID 1, 0+1, or 5 configuration (10GB usable)
  - 100 Mbps network connection

Sentivist™ Sensor: The Sentivist™ Sensor appliance is required to operate under the Free BSD 4.8 operating system with the hardware configuration referenced below. The Sensor CD has the Free BSD 4.8 operating system and custom NFR code resident on it.

The hardware specifications for the various Sentivist™ Sensor models that are part of this evaluation are:

- Sentivist™ Sensor 310C
- Sentivist™ Sensor 320C
- Sentivist™ Sensor 320F

Sentivist™ Sensor 310C Hardware:

- 1U Rack mountable Chassis for Intel WV533 board - 350W Power Supply, 2 x 1" ATA Cold-swap OR 3 x
- 1" U320 Hot-Swap HDD
- WV533 SCSI board for Dual Xeon processors w/512k cache, 400 or 533MHz bus
- WV533 SCSI 1U Backplane
- Intel® Xeon™ processor 2.8GHz, with 533MHz FSB & 512k cache, 1U Heat-sink variant
- Black locking front 1U Bezel 1

- Slimline CD/Floppy combo kit.
- 36 GB Ultra 320 15K RPM Cheetah LP 1" with SCA Connector
- 1GB DDR266 Low Profile Reg ECC RAM (requires 2 matching pieces) - 2GBs total
- RJ-45 to DB9 Serial Console adapter Cable
- US Power Cord, PS/2 "Y-cable" (included with original Intel packaging - enclosed in "Accessory box")
- front & mid-mount rack kit (included from original Intel kit, with Intel documentation removed)
- CD**:** Sentivist™ Sensor v4.0.2

Sentivist™ Sensor 320C Hardware:

- 1U Rack mountable Chassis for Intel WV533 board - 350W Power Supply, 2 x 1" ATA Cold-swap OR 3 x 1" U320 Hot-Swap HDD
- WV533 SCSI board for Dual Xeon processors w/512k cache, 400 or 533MHz bus
- WV533 SCSI 1U Backplane
- Intel® Xeon™ processor 2.8GHz, with 533MHz FSB & 512k cache, 1U Heat sink variant
- Black locking front 1U Bezel 1
- Slimline CD/Floppy combo kit.
- 36 GB Ultra 320 15K RPM Cheetah LP 1" with SCA Connector
- 1GB DDR266 Low Profile Reg ECC RAM (requires 2 matching pieces) - 4GBs total

- Single Port Copper (10/100/1000) Ethernet
- RJ-45 to DB9 Serial Console adapter Cable
- US Power Cord, PS/2 "Y-cable" (included with original Intel packaging - enclosed in "Accessory box")
- CD: Sentivist™ Sensor v4.0.2

Sentivist™ Sensor 320F Hardware

- 1U Rack mountable Chassis for Intel WV533 board - 350W Power Supply, 2 x 1" ATA Cold-swap OR 3 x 1" U320 Hot-Swap HDD
- WV533 SCSI board for Dual Xeon processors w/512k cache, 400 or 533MHz bus
- WV533 SCSI 1U Backplane
- Intel® Xeon™ processor 2.8GHz, with 533MHz FSB & 512k cache, 1U Heat sink variant
- Black locking front 1U Bezel
- Slimline CD/Floppy combo kit.
- 36 GB Ultra 320 15K RPM Cheetah LP 1" with SCA Connector
- 1GB DDR266 Low Profile Reg ECC RAM (requires 2 matching pieces) - 4GBs total
- SysKonnect SK-9844 SK-NET GE-SX dual link Optical Gb Ethernet
- RJ-45 to DB9 Serial Console adapter Cable
- US Power Cord, PS/2 "Y-cable" (included with original Intel packaging - enclosed in "Accessory box")

In addition, the Sentivist products must be installed and operated as described in the Evaluation Installation and Guides and Release Notes.

9 RESULTS OF THE EVALUATION

The evaluation was conducted based upon the Common Criteria (CC), Version 2.1, dated August 1999 [1,2,3]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [5];

and all applicable National and International Interpretations in effect on 26 September 2002. The evaluation confirmed the product as being Part 2 extended and Part 3 EAL 2 compliant. The details of the evaluation are recorded in the Evaluation Technical Report, which is controlled by the Arca CCTL. The evaluation determined the product to be **Part 2 extended conformant, Part 3 conformant,** and to meet the requirements of **EAL 2**. The product was evaluated and tested against the claims presented in the NFR Sentivist Version 4.02-Updated to v4.06 and Sentivist Sensor Models 310C, 320C and 320F Security Target, April 18, 2005.

The validation team followed the procedures outlined in the Common Criteria Evaluation Scheme [CCEVS] publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

Evaluation of the NFR Sentivist Target (ST) (ASE)

The evaluation team applied each EAL 2 ASE CEM work unit. Evaluation team action during the course of the ST evaluation ensured that the ST contained a description of the environment in terms of threats, assumptions and policies; a statement of security requirements claimed to be met by the NFR Sentivist product that are consistent with the Common Criteria; and product security function descriptions that support the requirements.

Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensures that the integrity of the TOE is adequately preserved; in particular, that configuration management provides confidence to the consumer that the TOE and documentation used for evaluation are the ones prepared for distribution. It also ensures that the TOE is accurately and uniquely identified such that the consumer is able to identify the evaluated TOE and discern one version from another. Configuration Management (CM) systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking changes and by ensuring that all changes are authorized. The Evaluation Team identified and analyzed the CM process to ensure that its documented procedures were followed and the procedures were employed during the course of this evaluation. The evaluation team ensured that the following items were considered configuration items: TOE implementation, design documentation, test documentation, and user guidance.

Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to securely deliver, install, configure, and operationally use the TOE; and ensured that the security protection offered by the TOE was not compromised during these events.

Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF implements/employs the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team verified the adequacy of the administrator guidance in describing how to securely administer the TOE.

Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team tests and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain obvious vulnerabilities that can be exploited in the evaluated configuration, based upon the developer strength of function analysis and the developer vulnerability analysis as well as the evaluation team's performance of penetration tests.

Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor test suite, the independent tests, and the penetration test further demonstrated the claims in the ST.

10 VALIDATOR COMMENTS AND RECOMMENDATIONS

The validator observations support the evaluation teams conclusion that the NRF Sentivist 4.02 Updated to v4.06 meets the claims stated in the Security Target. In particular, the product provides the functionality cited in the IDS System Protection Profile to which it claims conformance.

11 SECURITY TARGET

The ST, NFR Sentivist™ v4.0.2 – Updated to v4.0.6, Sentivist Sensors 310C, 320C and 320F Models Security Target version 2.7 April 18, 2005is included here by reference.

12 GLOSSARY

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CD	Compact Disk
CEM	Common Evaluation Methodology
CGI	Common Gateway Interface
CLI	Command Line Interface
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IDS	Intrusion Detection System
IP	Internet Protocol
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

13 BIBLIOGRAPHY

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

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

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

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

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

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

[7] NFR Sentivist™ v4.0.2 – Updated to v4.0.6, Sentivist Sensors 310C, 320C and 320F Models Security Target version 2.7 April 18, 2005

[8] NFR Sentivist™ v4.0.2 EAL 2 Team Test Plan Version 1.4, March 8, 2005, Arca CCTL, SAVVIS Communications

[9] Evaluation Technical Report, for NFR Sentivist™ v4.0.2 – Updated to v4.0.6 and Sentivist Sensors Models 310C, 320C and 320F 2.7 March 10, 2005