National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Symantec CyberWolf v2.0

Report Number: CCEVS-VR-04-0061
Dated: June 4, 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

William L. Jones
National Security Agency
Ft. Meade, MD

Timothy J. Bergendahl
The MITRE Corporation
Bedford, MA 01730

Common Criteria Testing Laboratory

Computer Sciences Corporation
132 National Business Parkway
Annapolis Junction, MD 20701

Evaluation Team

Charles Nightingale
Bob Seavers
Gus Massey
Michelle Burchell

Table of Contents

Figures

Tables

I. Executive Summary

The purpose of this Validation Report (VR) is to document the results of the evaluation of Symantec CyberWolf v2.0, a product of Symantec Corporation., Cupertino, CA. CyberWolf v2.0 is automated incident reporting system designed for security operations centers and managed security service providers that need automated incident reports in near real-time.

Evaluation at EAL2 of Symantec CyberWolf v2.0 was performed by the Computer Sciences Corporation (CSC) Common Criteria Testing Laboratory (CCTL), Annapolis Junction, MD. Evaluation results identified in this VR were drawn from the Symantec CyberWolf v2.0 Evaluation Technical Report (ETR) prepared by the CSC CCTL.

This VR is not an endorsement of the product by any agency of the United States Government, and no warranty of the product is either expressed or implied.

Symantec CyberWolf v2.0 does not claim conformance to any protection profile.

The all-software Target of Evaluation (TOE) consists of the Symantec CyberWolf v2.0 system which is comprised of four sub-systems, specifically SecurSite, Tomcat, Monitor, and Manager; the ISS RealSecure Expert; and the Snort Expert. The CyberWolf v2.0 system runs on one host; the ISS RealSecure Expert runs on a RealSecure system; and the Snort Expert runs on a Snort system.

Evaluated software includes Symantec CyberWolf v2.0 and Tomcat v4.06. The operating systems and hardware upon which the TOE executes were not evaluated, but were assumed to operate correctly and securely. In addition, an Oracle 8/9 database was implemented on the same host as CyberWolf v2.0, and was used by CyberWolf v2.0 to store user names, passwords, alerts and security incident-related information. Although not a TOE component, the Oracle 8/9 database was assumed to operate correctly and securely.

The following security functions are controlled by the TOE:

- Identification and Authentication
- Security Management
- User Action Log
- Data Collection
- Key Management
- Communications Security
- Data Reporting

The overall Strength of Function (SOF) claim for the TOE is SOF-basic.

The TOE was evaluated using the *Common Criteria for Information Technology Security Evaluation*, Version 2.1, dated August 1999 [CCV2.1], including applicable Interpretations, and the *Common Methodology for Information Technology Security Evaluation*, Version 1.0, Part 2: Evaluation Methodology, dated August 1999 [CEMV1.0P2]. The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) best practices as described within CCEVS Publication #3 [CCEVS3] and Publication #4 [CCEVS4].

The Security Target (ST) for Symantec CyberWolf v2.0 is contained within the CSC document *Symantec CyberWolf v2.0 Security Target,* Version 1.0, Revision 1.22, dated April 26, 2004 [STV1.0R1.22]. The ST has been shown to be compliant with the *Specification of Security Targets* requirements found within Annex C of Part 1 of the *Common Criteria for Information Technology Security Evaluation* dated August 1999 [CCV2.1].

The CSC CCTL Evaluation Team concluded that the TOE was found to be Part 2 extended and Part 3 conformant, and recommended that an EAL2 certificate rating be issued for the TOE. The Validation Team agreed with the conclusion of the CSC CCTL, and recommended to CCEVS Management that an EAL2 certificate rating be issued for the Symantec CyberWolf v2.0.

A search for obvious vulnerabilities associated with Symantec CyberWolf v2.0 was completed on April 27, 2004, the date of TOE testing.

The project, which also involved evaluation of the associated Security Target, was completed on June 4, 2004.

II. Identification

2.1 TOE, CC, and CEM Identification

TOE: Symantec CyberWolf v2.0

Evaluated Software: Symantec CyberWolf v2.0
Tomcat v4.06

Developer: Symantec Corporation
20300 Stevens Creek Boulevard
Cupertino, California 95014

CCTL: Computer Sciences Corporation
132 National Business Parkway
Annapolis Junction, MD 20701

CC Identification: *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999 [CCV2.1].

Interpretations: All NIAP and CCIMB interpretations as of the date of the Kick-off meeting held on December 3, 2003, were considered during the evaluation. The interpretations listed in Table 1 had a direct impact on the work performed.

Table 1. Interpretations impacting the CyberWolf v2.0 evaluation.

Short Title	Subject
CCIMB-INTERP - 003	Unique identification of configuration items in the configuration list
CCIMB-INTERP - 016	Objective for ADO_DEL
CCIMB-INTERP - 025	Level of detail required for hardware descriptions
Revised CCIMB-INTERP - 031	Obvious vulnerabilities
CCIMB-INTERP - 032	Strength of Function Analysis in ASE_TSS
CCIMB-INTERP - 037	ACM on Product or TOE?
CCIMB-INTERP - 038	Use of 'as a minimum' in C&P elements
CCIMB-INTERP - 043	Meaning of "clearly stated" in APE/ASE_OBJ.1
CCIMB-INTERP - 049	Threats met by environment
CCIMB-INTERP - 051	Use of documentation without C & P elements
CCIMB-INTERP - 064	Apparent higher standard for explicitly stated requirements
CCIMB-INTERP - 065	No component to call out security function management
CCIMB-INTERP - 075	Duplicate informative text for different work units
CCIMB-INTERP - 084	Aspects of objectives in TOE and environment
CCIMB-INTERP - 085	SOF Claims additional to the overall claim
CCIMB-INTERP - 092	Release of the TOE
CCIMB-INTERP - 098	Limitation of refinement
CCIMB-INTERP - 111	Settable Failure Limits are Permitted
CCIMB-INTERP - 116	Indistinguishable work units for ADO_DEL
Revised CCIMB-INTERP – 127	Work unit not at the right place
Revised CCIMB-INTERP - 128	Coverage of the Delivery Procedures

Short Title	Subject
CCIMB-INTERP - 140	Guidance Includes AGD_ADM, AGD_USR, ADO, and ALC_FLR
CCIMB-INTERP - 150	A Completely Evaluated ST is not Required when TOE evaluation starts
CCIMB-INTERP - 151	Security Attributes Include Attributes of Information and Resources
CCIMB-INTERP - 202	Selecting One or More items in a selection operation and using "None" in an assignment

CEM Identification: *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999.

2.2 TOE Overview

Symantec CyberWolf v2.0 is automated incident reporting system designed for security operations centers and managed security service providers that need automated incident reports in near real-time.

A basic environment for the TOE is shown in Figure 1.

The all-software TOE consists of the Symantec CyberWolf v2.0 system which is comprised of four sub-systems, specifically SecurSite, Tomcat, Monitor, and Manager; the ISS RealSecure Expert; and the Snort Expert. The CyberWolf v2.0 system runs on one host; the ISS RealSecure Expert runs on a RealSecure system; and the Snort Expert runs on a Snort system.

Evaluated software includes Symantec CyberWolf v2.0 and Tomcat v4.06. The operating systems and hardware upon which the TOE executes were not evaluated, but were assumed to operate correctly and securely. In addition, an Oracle 8/9 database was implemented on the same host as CyberWolf v2.0, and was used by CyberWolf v2.0 to store user names, passwords, alerts and security incident-related information. Although not a TOE component, the Oracle 8/9 database was assumed to operate correctly and securely.

The overall Strength of Function claim for the TOE is SOF-basic.

The TOE logical boundary consists of the following security functions that are controlled by the TOE:

- Identification and Authentication (TSF_INA)
- Security Management (TSF_FMT)
- User Action Log (TSF_UAL)
- Data Collection (TSF_EDC)

- Key Management (TSF_KMG)
- Communications Security (TSF_KMG)
- Data Reporting (TSF_DRE)

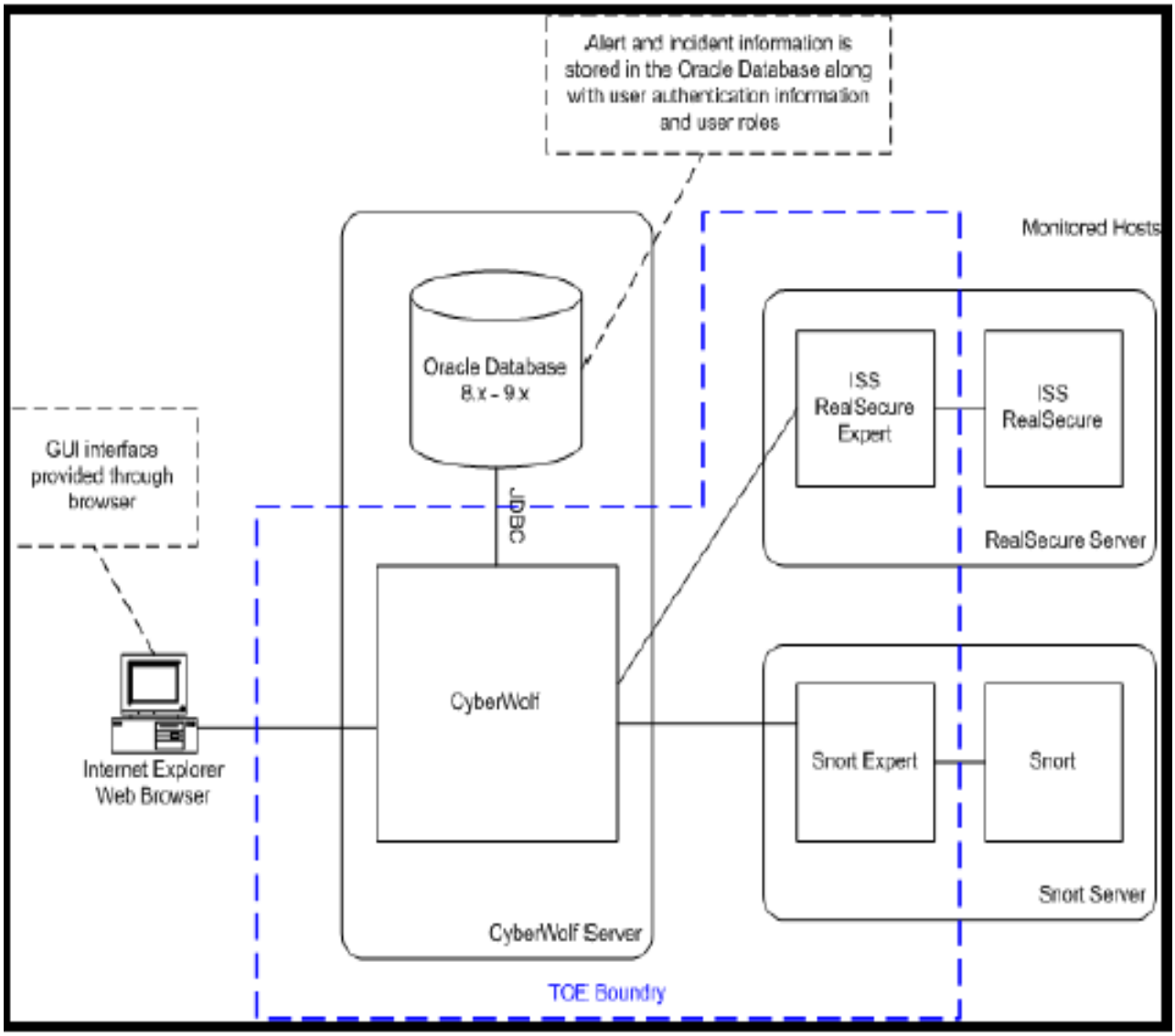

Figure 1. A basic environment for the TOE.

III. Security Policy

A high-level description of the Symantec CyberWolf v2.0 security policy is as follows.

- The TOE supports four roles: Administrator; Senior Incident Handler; Junior Incident Handler; and Read-only user

- Users of the TOE are required to be identified and authenticated before being allowed access to the system
- The TOE utilizes encryption for all message traffic between components
- The TOE collects a log of certain user actions that result in changes to the CyberWolf v2.0 database

Additional details about the TOE security policy are contained within *Annex D* of this Validation Report, and within the ST [STV1.0R1.22].

IV. Assumptions and Clarification of Scope

This section provides an overview of the threats and assumptions not countered by the TOE.

4.1 Threats

- Threats to the TOE are considered to be users with public knowledge of how the TOE operates.

4.2 Environmental assumptions

- The TOE has been delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.
- There will be one or more competent system administrator(s) assigned to manage the TOE and the security of the information it contains.
- The system administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the system administration documentation.
- Procedures exist for granting system administrator(s) access to the TSF.
- Users and administrators change their passwords every 60 days.
- The TOE will be located within facilities providing controlled access to prevent unauthorized physical access.
- The host machines running the TOE software will provide the TOE with a reliable time and date.
- The operating systems upon which the TOE software runs will be configured to restrict modification to TOE executables, configuration files, and cryptographic keys to only the CyberWolf authorized administrators.

Additional details are contained within *Annex E* of this Validation Report, and within the ST [STV1.0R1.22].

V. Evaluated Configuration

Details about the evaluated configuration are contained within the Installation and Generation documents identified in Table 2. Entries in the right-most column are abbreviations used within this VR.

Table 2. Installation and generation documents.

Installation and Generation	
Installation Guide, Mountain Wave, Inc., Version 2	SCW_IG
Symantec CyberWolf 2.0 Install Guide Errata, January 8, 2004	SCW_IGE
Symantec CyberWolf 2.0 Device Expert Guide, January 8, 2004	SCW_DEG

- SCW_IG is the master installation document for the TOE.
- SCW_DEG provides installation guidance for CyberWolf device experts.
- SCW_IGE is an errata sheet that clarifies issues or changes within SCW_IG.

Documents relating to Administrator Guidance, and User Guidance are identified in *Annex H* of this VR.

VI. Evaluation Process and Conclusions

The Computer Sciences Corporation CCTL Evaluation Team followed the procedures outlined in CCEVS Scheme Publication #4, *Guidance to Common Criteria Testing Laboratories* [CCEVS4].

The Evaluation Team concluded that the TOE was found to be CC Part 2 extended and CC Part 3 conformant, and recommended that an EAL2 certificate rating be issued for the TOE.

VII. Validation Process and Conclusions

The Validation Team followed the procedures outlined in CCEVS Scheme Publication #3, *Guidance to Validators of IT Security Evaluations* [CCEVS3].

The Validation Team agreed with the conclusion of Computer Sciences Corporation CCTL Evaluation Team, and recommended to CCEVS Management that an EAL2 certificate rating be issued for Symantec CyberWolf v2.0.

VIII. Validator Comments/Recommendations

The Validation Team offers the following:

- Computer Sciences Corporation CCTL personnel were very cooperative with all aspects of this project.

- Testing of the Symantec CyberWolf v2.0 TOE was well thought out, thorough, and very professionally done.

- The Validation Team recommended to CCEVS Management that Symantec CyberWolf v2.0 receive an EAL2 certificate.

IX. Annexes

Annex A: Architectural Description of the TOE

Refer to Section 2.2, TOE Overview, and to the Security Target [STV1.0R1.22] for the architectural description.

Annex B: Assurance Requirements Results

Symantec CyberWolf v2.0 satisfies the EAL2 security assurance requirements identified in Part 3 of the *Common Criteria* [CCV2.1]. These requirements are displayed in Table 3.

Table 3. TOE security assurance requirements.

Assurance Component ID	Assurance Component Name
ACM_CAP.2	Configuration items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

The security assurance requirements were neither iterated nor refined. In addition, no additional security assurance requirements were involved.

Identification of the EAL2 security assurance requirements that Symantec CyberWolf v2.0 satisfies, as well as the details of how the product meets each of them, are contained in the ST [STV1.0R1.22].

Annex C: Security Functional Requirements Results

Symantec CyberWolf v2.0 satisfies the TOE security functional requirements and the explicitly-stated requirements for the TOE. The former are listed in Table 4, and the later are listed in Table 5.

Table 4. TOE security functional requirements.

Class FIA: Identification and Authentication	
FIA_UAU.2	User authentication before any action
FIA_UAU.7	Protected authentication feedback
FIA_UID.2	User identification before any action
Class FMT: Security Management	
FMT_MOF.1	Management of security functions behavior
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
Class FPT: Protection of the TSF	
FPT_ITT.1	Basic internal TSF data transfer protection
Class FCS: Cryptographic Support	
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation

Table 5. Explicitly-stated requirements for the TOE.

Requirement	**Title**	**Reason for inclusion**
SCW_UAL.1	User action log	To ensure that a security-relevant subset of user actions is logged.
SCW_EDC.1	System data collection	To ensure that event data is collected from the various systems the TOE's device experts are installed on.
SCW_DRE.1	Data reporting	To ensure that data collected by the TOE is reported in a collection of specified reports.

Details about each of the security functional requirements, including the explicitly stated requirements, that Symantec CyberWolf v2.0 satisfies, are contained in the ST [STV1.0R1.22].

Annex D: Security Policy Details

- The TOE supports four roles, as follows: Administrator; Senior Incident Handler; Junior Incident Handler; and Read-only user.

    - Administrator: An authorized user who manages the CyberWolf v2.0 product, and who has the ability to enable, disable, or modify the behavior of all security functions.
    - Senior Incident Handler: An authorized user who responds to CyberWolf v2.0 incidents, and who has the ability to assign, modify, and close incidents.
    - Junior Incident Handler: An authorized user who responds to CyberWolf v2.0 incidents, and who has the ability to assign, modify, and close already-assigned incidents.
    - Read-only user: An authorized user who can read, but not alter, CyberWolf v2.0 incidents and reports.

- Symantec CyberWolf v2.0 users are required to be identified and authenticated before being allowed access to the system. The Identification and Authentication (I&A) mechanism is built on top of Tomcat's Java Database Connectivity (JDBC) Realms. During authentication, the security roles defined for the user are accumulated, and the user is permitted access using those roles.

- Symantec CyberWolf v2.0 utilizes encryption for all message traffic between components. The encryption algorithm to be used is selected at install time. The available encryption algorithms include DES, TripleDES, and Blowfish.

- Symantec CyberWolf v2.0 collects a log of certain user actions that result in changes to the CyberWolf database. The logs include the name of the person associated with the action, the type of event, the date and time of the event, and the outcome of the event.

Additional details about the Symantec CyberWolf v2.0 security policy are contained in the ST [STV1.0R1.22].

Annex E: Assumptions and Clarification of Scope

E.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL2 assurance requirements:

ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance

E.2 Environmental Assumptions

The environmental assumptions listed in Table 6 are required to ensure the security of the TOE.

Table 6. Environmental assumptions.

Assumption	Description
A.INSTALL	The TOE has been delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.
A.MANAGE	There will be one or more competent system administrator(s) assigned to manage the TOE and the security of the information it contains.
A.NO_EVIL_ADM	The system administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the system administration documentation.
A.PROCEDURE	Procedures exist for granting system administrator(s) access to the TSF.
A.CHANGE_PWD	Users and administrators change their passwords every 60 days.
A.PHYSICAL_PROTECT	The TOE will be located within facilities providing controlled access to prevent unauthorized physical access.
A.RELIABLE_TIME	The host machines running the TOE software will provide the TOE with a reliable time and date.
A.ACCESS_CONTROL	The operating systems upon which the TOE software runs will be configured to

Assumption	Description
	restrict modification to TOE executables, configuration files, and cryptographic keys to only the CyberWolf authorized administrators.

E.3 Clarification of Scope

Threats to the TOE are considered to be users with public knowledge of how the TOE operates. Details are shown in Table 7.

Table 7. Threats to the TOE.

Assumption	Description
T_ALTER_CONFIG	An unauthorized user may attempt to access the TOE through an external interface in order to alter the TOE configuration to circumvent the configured policy so they can obscure intrusion attempts on the network from the TOE's users.

Annex F: IT Product Testing

The Computer Sciences Corporation CCTL provided tests and test results applicable to Symantec CyberWolf v2.0.

The Evaluation Team tested all seven TOE security functions and the majority of associated security functional requirements. The Evaluation Team used information provided in the developmental evidence to determine which interfaces to stimulate to produce the desired effects.

The following issues were considered in devising specific test cases:

- Known public domain weaknesses commonly associated with this type of TOE were considered and, where applicable, test cases were designed to probe for those weaknesses.

- The significance of each security function was factored into test case development to ensure that all associated security objectives were being met.

- The SOF claim for the TOE, SOF-basic, was tested to ensure that the minimum password length (eight characters) is enforced.

- No TOE security function was, in and of itself, so complex as to necessitate a correspondingly complex testing approach. However, the evaluators did create a fairly complex testing environment to ensure that all configuration variations that fall within the physical/logical scope and boundaries of the TOE are tested.

- Tests for all types of interfaces to the TOE (e.g., remote user web access, direct administrator console access, component-to-component internal interfaces) were included in the test cases.

- The internal, intra-component encryption offered by the TOE was characterized unusual by the evaluators. To support testing of that function, the evaluators created an unencrypted installation of the TOE. The encrypted and unencrypted intra-component communications of the TOE in response to the same stimulus or request was compared and analyzed to verify that encryption is actually being applied to all internal TOE communications.

Annex G: Security Target

The Security Target (ST) for Symantec CyberWolf v2.0 is contained within the document *Symantec CyberWolf v2.0 Security Target,* Version 1.0, Revision 1.22, dated April 26, 2004, authored by Computer Sciences Corporation [STV1.0R1.22]. The ST is compliant with the *Specification of Security Targets* requirements found within Annex C of Part 1 of the CC [CCV2.1].

Annex H: Documentation

Documentation applicable to Symantec CyberWolf v2.0 Installation and Generation, Administrator Guidance, and User Guidance is identified in Table 8. Entries in the right-most column are abbreviations used within this VR.

Table 8. Selected documentation.

Installation and Generation	
Installation Guide, Mountain Wave, Inc., Version 2, March 22, 2004.	SCW_IG
Symantec CyberWolf 2.0 Install Guide Errata, January 8, 2004	SCW_IGE
Symantec CyberWolf 2.0 Device Expert Guide, January 8, 2004	SCW_DEG
Administrator and User Guidance	
SecurSite Features and User Manual, Mountain Wave, Inc., December 29, 2003	SCW_FUM
Symantec CyberWolf 2.0 User Guide Errata, January 8, 2004	SCW_UGE
Symantec – Understanding CyberWolf Rules, Version 2, January 8, 2004	SCW_UCR

Additional documentation, most of which is proprietary, was available to the Evaluation Team during the evaluation of Symantec CyberWolf v2.0.

Annex I: Glossary

Table 9 is a glossary of terms used within this VR.

Table 9. Glossary.

Acronym	Expansion
CC	*Common Criteria for Information Technology Security Evaluation*. [Note: Within this Validation Report, CC always means Version 2.1, dated August 1999.]
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CCIMB	Common Criteria Interpretations Management Board
CSC	Computer Sciences Corporation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
I&A	Identification and Authentication
JDBC	Java Database Connectivity
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

Annex J: Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap.nist.gov/cc-scheme).
- Computer Sciences Corporation (http://www.csc.com).
- Symantec Corporation (http://www.symantec.com).

CCEVS Documents

[CCV2.1] *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999.

[CEMV1.0P2] *Common Methodology for Information Technology Security Evaluation*, Version 1.0, Part 2: Evaluation Methodology, August 1999.

[CCEVS3] *Guidance to Validators of IT Security Evaluations*, Version 1.0, February 2000.

[CCEVS4] *Guidance to Common Criteria Testing Laboratories*, Draft, Version 1.0, March 2000.

Other Documents

[STV1.0R1.22] *Symantec CyberWolf v2.0 Security Target,* Version 1.0, Revision 1.22, dated April 26, 2004, authored by Computer Sciences Corporation.