

National Information Assurance Partnership



Common Criteria Evaluation and Validation Scheme Validation Report

netForensics V3.1.1 With Point Update 45149

Report Number: CCEVS-VR-05-0097
Dated: 27 April 2005
Version: 1.1

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

VALIDATION REPORT
netForensics netForensics V3.1.1

ACKNOWLEDGEMENTS

Validation Team

**Franklin Haskell
The MITRE Corporation
Bedford, Massachusetts**

Common Criteria Testing Laboratory

**COACT, Inc.
Columbia, Maryland**

Table of Contents

1	Executive Summary	1
1.1	Evaluation Details	1
1.2	Interpretations	2
1.3	Threats to Security	3
2	Identification	4
3	Security Policy	4
4	Assumptions.....	4
4.1	Personnel Assumptions	4
4.2	Physical Assumptions	4
5	Architectural Information	4
6	Documentation.....	6
7	IT Product Testing	6
7.1	Developer Testing.....	6
7.2	Evaluation Team Independent Testing	6
7.3	Evaluation Team Penetration Testing.....	6
8	Evaluated Configuration	6
9	Results of the Evaluation	8
10	Validator Comments/Recommendations	8
11	Annexes.....	9
12	Security Target.....	9
13	Glossary	10
14	Bibliography	10

List of Tables

Table 1 - Threats 3
Table 2 - TOE Subsystems 5
Table 3 - Software Requirements 7
Table 4 - Hardware Requirements 7

1 Executive Summary

The evaluation of **netForensics V3.1.1 With Point Update 45149** was performed by COACT, Inc., in the United States and was completed on 7 April 2005. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.1 and the Common Methodology for IT Security Evaluation (CEM), Version 1.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the netForensics product by any agency of the US Government and no warranty of the product is either expressed or implied.

The COACT evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 2) have been met.

The validation team monitored the activities of the evaluation team, examined evaluation testing procedures, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The validation team notes that the claims made and successfully evaluated for the product represent a more limited set of requirements than what might be used for a "normal" product deployment. Specifically, no claims are made for protection of data transmission between parts of the TOE in spite of the fact that it will mostly likely be configured and setup in a distributed fashion over a network whose traffic could well be less than benign. It then becomes quite necessary for the administrators to fulfill the requirements levied on the environment.

The technical information included in this report was obtained from the Evaluation Technical Report for netForensics 3.1.1 With Point Update 45149 (ETR) produced by COACT.

1.1 Evaluation Details

Evaluated Product: netForensics V3.1.1 With Point Update 45149

Sponsor & Developer: netForensics, Inc.
200 Metroplex Drive
Edison, NJ 08817

CCTL: COACT, Inc.,
Rivers Ninety Five
9140 Guilford Road, Suite G

VALIDATION REPORT
netForensics netForensics V3.1.1

Columbia, MD 21046-2587

Completion Date:	7 April 2005
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.1
Interpretations:	The interpretations used for this evaluation are listed in the section following.
CEM:	Common Evaluation Methodology for Information Technology Security, Part 1: Introduction and General Model, Version 0.6, January 1997; Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 1.0, August 1999.
Evaluation Class:	EAL 2
Description	<p>The netForensics is a Security Information Management (SIM) tool. It collects and analyzes information from security devices deployed in a network and provides users with tools for viewing and evaluating the collective security state of the protected systems. It may be deployed in a distributed fashion.</p> <p>The threats to itself that it addresses are those from illegal access and unauthorized activity. It assumes that it will operate in a benign environment, is properly installed and configured, and that the devices sending information to it are well-behaved.</p>
Disclaimer	The information contained in this Validation Report is not an endorsement of the netForensics product by any agency of the U.S. Government and no warranty of the netForensics product is either expressed or implied.
PP:	none
Evaluation Personnel	Robert West, Ching Lee, Tom Benkart
Validation Team:	Franklin Haskell The MITRE Corporation 202 Burlington Road Bedford, MA 01730-1420

1.2 Interpretations

The Evaluation Team determined that the following NIAP Interpretations were applicable to this evaluation:

I-0405 – American English Is An Acceptable Refinement

VALIDATION REPORT
netForensics netForensics V3.1.1

I-0407 – Empty Selections Or Assignments

I-0416 – Association Of Access Control Attributes With Subjects And Objects

I-0422 – Clarification Of "Audit Records"

I-0423 – Some Modifications To The Audit Trail Are Authorized

I-0442 – Restrictive Is Not Fully Defined Without Specification Of Attributes

The Evaluation Team determined that the following CCIMB interpretations were applicable to this evaluation:

RI#003 – Unique identification of configuration items in the configuration list (11 February 2002)

RI#008 – Augmented and Conformant overlap (31 July 2001)

RI#016 – Objective for ADO_DEL (11 February 2002)

RI#019 – Assurance Iterations (11 February 2002)

RI#031 – Obvious vulnerabilities (25 October 2002)

RI#049 – Threats met by environment (16 February 2001)

RI#064 – Apparent higher standard for explicitly stated requirements (16 February 2001)

RI#065 – No component to call out security function management (31 July 2001)

RI#075 – Duplicate Informative Text for ATE_FUN.1-4 and ATE_IND.2-1 (15 October 2000)

RI#084 – Aspects of objectives in TOE and environment (31 July 2001)

RI#085 – SOF Claims additional to the overall claim (11 February 2002)

RI#116 – Indistinguishable work units for ADO_DEL (31 July 2001)

RI#127 – Work unit not at the right place (25 October 2002)

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.

1.3 Threats to Security

The following are the threats that the evaluated product addresses:

Table 1 - Threats

T.UNAUTH	Unauthorized user	Illegal access through the administrator interface
T.USER_ACC	Authorized System Analyst	Illegal access
T.ATTACK	Attacker	Directs malicious activities against the network
T.INADVERT	User	Careless Operation
T.NOACCNT	Authorized System Analyst	Malicious Activity

2 Identification

The product being evaluated is netForensics Version 3.1.1 With Point Update 45149. Note that the actual target of evaluation defined is only certain parts of the whole product.

3 Security Policy

There are no Security Policies for the evaluated product.

4 Assumptions

4.1 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

- A.NOEVILADMIN The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- A.PLATFORM The platforms used to host the TOE components will be installed and configured by an administrator and will conform to the specifications listed in Table 3 - Software Requirements.
- A.INSTALL The hardware, operating systems, and software required to support the TOE will be installed and configured by an administrator in conformance with the installation guides.
- A.PROTECTED Administrators will ensure that proper firewall and network controls are in place to prevent un-trusted and unknown source network hosts from sending events to the nF Agents.
- A.COMPATIBLE Administrators will ensure that Security Devices sending events to the TOE are compatible with the TOE.

4.2 Physical Assumptions

The following physical assumptions are identified in the Security Target:

- A.ENVIRON The TOE will be located in an environment that provides physical security, uninterruptible power, air conditioning, and all other conditions required for reliable operation of the hardware.

5 Architectural Information

The TOE is only software. There is no hardware included in the evaluation. It is a Security Information Management (SIM) tool in that it collects and analyzes information from Security Devices deployed in a network and provides users with tools for viewing and evaluating the collective state of security.

netForensics collects, normalizes, and aggregates data from a number of third-party Security Devices. Users are able to monitor the collected data in real-time at differing levels of granularity

VALIDATION REPORT
netForensics netForensics V3.1.1

and aggregation through pre-defined views. A wide-range of canned reports, queries, and drilldowns are provided to support forensics, analysis, and risk assessment.

The following table contains descriptions of the major sub-systems of the TOE.

Table 2 - TOE Subsystems

Security Audit	<i>nF Provider</i> provides notifications for all database updates from admin screens. <i>SIM Desktop</i> provides the ability to review the security audits.
System Analysts' Access Control	<i>nF Master</i> distributes real-time and event information to <i>SIM Desktops</i> based upon the access rights of the users to specific device information. <i>nF Provider</i> restricts access to stored information based upon the access rights of the users to specific device information.
Identification and Authentication	<i>SIM Desktop</i> presents the login screen to the user and validates the Userid/Password entries. Security Portal also performs this function for access to generated reports.
Administration	<i>SIM Desktop</i> presents the user interface for administration of configuration parameters and settings. Queries and updates are sent to <i>nF Provider</i> . <i>nF Provider</i> provides methods for accessing and updating the configuration parameters and settings. <i>Report Scheduler</i> provides the functionality to configure reports to be generated.
Security Information Management	<i>nF Agents</i> collect information from non-TOE devices and normalize that information for processing by <i>nF Engines</i> . Pre-normalization and post-normalization filters may be applied to the information streams. <i>nF Engines</i> collect the normalized events from <i>nF Agents</i> , aggregates the events, filters and forwards events based upon configurable parameters, sends notifications, formats the application event timestamp, and forwards events to <i>nF Masters</i> . <i>nF Engine</i> sends events to <i>nF Provider</i> for entry into the database. <i>nF Masters</i> receive events from <i>nF Engines</i> and use this information to update the real-time user display, update the scoreboard, and forward events to users. <i>SIM Desktops</i> receive updates and events from <i>nF Master</i> and present that information to the user. <i>SIM Desktops</i> also provide the user front-end for retrieving information from the database. <i>nF Provider</i> receives event batches from <i>nF Engines</i> and executes them for insertion of event data into the database. <i>nF Provider</i> receives queries from the <i>SIM Desktops</i> to retrieve <i>SIM</i> data from the database. <i>Report Scheduler</i> provides a mechanism to generate and review reports based on <i>SIM</i> data stored in the database. <i>DBMS Utilities</i> provide a means to archive or purge <i>SIM</i> data stored in

	the database. <i>Security Portal</i> provides access to generated reports.
--	---

These services are configurable to run on separate machines.

6 Documentation

The following documents are delivered to customers and are pertinent to the installation, configuration, and operation of the TOE.

netForensics Administration Guide, Revision 1.3, November 2004;

netForensics User's Guide; Version 3.1.2, July 2004;

netForensics Security Portal Server Installation Guide, Version 3.1.1 December 2003;

netForensics Quick Start Guide, Version 3.0 October 2002;

netForensics Security Portal Server User's Guide, Version 3.1.1 December 2003;

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The vendor provided a complete set of test results for analysis. The evaluation team analyzed the vendor test procedures to determine if there was adequate coverage of the SFR's and to determine if the interfaces between subsystems behaved as expected. The Evaluation Team determined that the developer's actual test results matched the expected results.

7.2 Evaluation Team Independent Testing

The Evaluation Team chose to run a subset of the tests that the developer performed. The subset was chosen to ensure adequate coverage for all security functional requirements. This ensured that the Evaluation Team adequately addressed the security functions.

7.3 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team used a combination of vulnerability test tools, open-source vulnerability documentation, and a set of test procedures proposed by the penetration test team to identify penetration test cases based on the developer's vulnerability assessment documentation. The Evaluation Team used the developer's test configuration to successfully perform its penetration tests.

The Evaluation Team's ETR, Part 2, provides a detailed description of the tests, the results, and the effects, if any, on the information presented in the ST or other evaluation evidence.

8 Evaluated Configuration

netForensics can be deployed in several different modes. A full deployment has all netForensics components installed on the same server. Alternatively the various components can be installed on

VALIDATION REPORT
netForensics netForensics V3.1.1

different servers. The table below summarizes the operating system and application requirements for each TOE component.

Table 3 - Software Requirements

Component	Description
nF Engine	Red Hat Linux 7.1 (Kernel 2.4.9), Solaris 8
nF Master	Red Hat Linux 7.1 (Kernel 2.4.9), Solaris 8
nF Web Server	Red Hat Linux 7.1 (Kernel 2.4.9), Solaris 8
nF Provider	Red Hat Linux 7.1 (Kernel 2.4.9), Solaris 8
nF Security Portal	Red Hat Linux 7.1 (Kernel 2.4.9), Solaris 8
nF Universal Agent	Red Hat Linux 7.1 (Kernel 2.4.9) Sun Solaris 8 Microsoft 2000 Sever/Advanced Server (SP2)
nF Report Scheduler	Red Hat Linux 7.1 (Kernel 2.4.9), Solaris 8
Database	Oracle 9i Standard or Enterprise
Java Virtual Machines	Java 2 Runtime Environment, Standard Edition 1.4.1 or higher
	Java Web Start 1.2

Specific hardware requirements must also be addressed depending on the operating system in use and the component support. The processor requirements are as follows:

Red Hat Linux: Intel Pentium III 733 MHz (Server class)

Solaris: UltraSPARC-IIi 444 MHz (Server class)

The table below summarizes the free hard disk and minimum system memory requirements for each individual component.

Table 4 - Hardware Requirements

Component	Free Hard Disk Space	Memory
Full Install	18 GB	4 GB
nF Engine	1 GB	System memory + 256 MB for Engine
nF Master	1 GB	System memory + 256 MB for Master
nF Agents	100 MB	System memory + 64 MB per Agent
nF Report Scheduler	1 GB	System memory + 128 MB for Engine
nF Security Portal	500 MB	System memory + 64 MB per Agent
nF WebServer	1 GB	System Memory + 64 MB for WebServer (384 MB min recommended)

VALIDATION REPORT
netForensics netForensics V3.1.1

nF Provider and Database	18 GB	System Memory + 1 GB for Provider and Oracle DB (1536 MB min recommended)
--------------------------	-------	--

9 Results of the Evaluation

The evaluation was carried out in accordance to the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the netForensics TOE meets the security requirements contained in the Security Target.

The criteria against which the netForensics TOE was judged are described in Common Criteria for Information Technology Security Evaluation, Version 2.1. The evaluation methodology used by the evaluation team to conduct the evaluation is Common Methodology for Information Technology Security Evaluation, Version 1.0. The COACT, Inc. CAFE Lab determined that the evaluation assurance level (EAL) for the netForensics TOE is EAL 2. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

A Validator on behalf of the CCEVS Validation Body monitored the evaluation carried out by the COACT, Inc. CAFE Lab. The evaluation was completed in April, 2005. Results of the evaluation and associated validation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report.

10 Validator Comments/Recommendations

The product is a security event collection, aggregation, correlation, and analysis tool. It does not react to security problems itself. It provides information to system and network administrators in order that they may respond to situations, hopefully in a more timely manner than they would be able to without it.

The TOE is software only. It is dependent upon the underlying operating system to protect it from other applications and users on the platforms upon which it is deployed. This does allow for many deployment options. They range from all the components residing on a single system to multiple copies of every component spread over an entire network. These options were tested to a degree. Even in a single system configuration the “agents” – those components which receive the volumes of raw data from the (untrusted) third-party devices – are necessarily exposed to all the dangers inherent in whatever network is being protected. This is not necessarily the actual Internet itself. It could be a well-protected corporate internal network; yet one must assume that any network this product is being deployed on will have a significant amount of danger; which means that the communications between those devices and the agents are subject to the usual variety of Internet attacks: man-in-the-middle and denial-of-service for starters. This evaluation does not include defenses for those. No claims for data transmission encryption are made, for example. There are only objectives for and requirements levied on the environment.

The situation worsens the more distributed the deployment becomes. There are more communication paths between components open to attack. The agents, one can assume, have at least a modicum of “bad data” resistance because they are receiving that data from outside the TOE. The other parts of the product being evaluated do not “face the outside”. They only expect data from other parts of the TOE. It becomes, then, just that much more necessary for users to fulfill, in some fashion, the requirements levied upon the environment.

11 Annexes

Not applicable.

12 Security Target

The security target for this product's evaluation is **netForensics Version 3.1.1 With Point Update 45149 Security Target**, "Initial release", dated March 8, 2005

13 Glossary

The following definitions may be used in this document:

DBMS	Database Management System
SIM	Security Information Management
SOF	Strength of Function

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- **Common Criteria for Information Technology Security Evaluation**, Version 2.1, August 1999, Parts 1, 2, and 3.
- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, **Guidance to Validators of IT Security Evaluations**, Scheme Publication #3, Version 1.0, January 2002.
- **Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model**, Version 0.6, 11 January 1997.
- **Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology**, Version 1.0, August 1999.
- **netForensics Version 3.1.1 With Point Update 45149 Security Target**, Document No. F2-0305-003, March 8, 2005.
- **Evaluation Technical Report for the netForensics 3.1.1 With Point Update 45149**, Document No. F2-0305-006(1), March 18, 2005.