Certification Report

EAL 2 Evaluation of Intellitactics™ Incorporated

Network Security Manager™ (NSM™)

v4.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document Number:	383-4-17-CR
Version:	1.0
Date:	1 December 2004
Pagination:	i to iv, 1 to 10

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.1*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment (CSE), or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the CSE, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 1 December 2004, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at:

http://www.cse-cst.gc.ca/en/services/common criteria/trusted_products.html

This certification report makes reference to the following trademarked names: Network Security Manager and NSM which are trademarks of Intellitactics™ Incorporated; Windows 2000 and MS SQL Server 2000 which are trademarks or registered trademarks of Microsoft Corporation; and Java, which is a trademark of Sun Microsystems.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

The Network Security Manager™ (NSM™) v4.1, from Intellitactics™ Incorporated, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation.

The Intellitactics™ NSM™ is a threat management platform that processes, stores, and displays security event data collected within the network(s) that it monitors. The NSM™ can provide the user with a graphical visualisation of events as they happen in real time, and can correlate event information and provide the user a visualization of trends happening over time.

Electronic Warfare Associates-Canada, Ltd. is the CCEF that conducted the evaluation. This evaluation was completed on 24 November 2004, and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for the NSM™, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the NSM™ are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report[1] for this product provide sufficient evidence that it meets the EAL 2 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 1.0* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.1.*

The Communications Security Establishment, as the CCS Certification Body, declares that the NSM™ v4.1 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list.

[1] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation is the Network Security Manager™ (NSM™) v4.1, from Intellitactics™ Incorporated.

2 TOE Description

The Intellitactics™ NSM™ is a threat management platform that processes, stores, and displays security event data collected within the network(s) that it monitors. The NSM™ can provide the user with a graphical visualisation of events as they happen in real time, and can correlate event information and provide the user a visualization of trends happening over time.

NSM™ event data comprises the data collected from third-party security devices such as firewalls, routers, and Intrusion Detection System (IDS) sensors deployed within the monitored network(s). The Event Consolidators collect the event data from the third-party devices, consolidate the data, and forward the data to the Central Server. The Central Server processes the data into a format meaningful to users, and forwards the data to the Database. The Database provides permanent storage for the event data. Users review the data in the Database using either the Remote Console or the Reporting System Server.

Figure 1 of the Security Target (ST) shows NSM™ components in a typical installation configuration. The Remote Console, Central Server, Event Consolidator, and the Reporting System Server are proprietary to Intellitactics™ Incorporated and are developed in the Java® programming language. The Database component uses Microsoft® SQL Server™ 2000.

Communications between NSM™ components is over Ethernet using TCP/IP. The event data communicated between the Central Server and the Remote Console, between the Event Consolidator(s) and the Remote Console, and between the Event Consolidator(s) and the Central Server is protected by the SSL protocol.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the NSM™ is identified in Sections 5.1 and 5.2 of the ST.

4 Security Target

The ST associated with this Certification Report (CR) is identified by the following nomenclature:

Title: Security Target for the Intellitactics™ Incorporated Network Security Manager™ (NSM™) v4.1
Version: v1.13
Date: 18 November 2004

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.1*, incorporating all final interpretations issued prior to 21 July 2003. The NSM™ v4.1 is:

a. Common Criteria Part 2 extended, with security functional requirements based upon functional requirements in Common Criteria Part 2 and additional security functional requirements as defined in section 5.2 of the ST;

b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and

c. Common Criteria EAL 2 conformant, with all the security assurance requirements in the EAL 2 package.

6 Security Policy

The complete NSM™ Security Policy is identified in the ST. The following statements are representative of the Security Policy:

Authentication. Users must authenticate to the NSM™ to be able to access its security functions, event data, and audit data. A user authenticating to the NSM™ must provide a user name and password for a valid user account. When authenticating, the user name is displayed in plain text and each character of the password is masked.

Access Control. The access control policy is enforced on all authenticated NSM™ users. User access to NSM™ event data is allowed based upon the user name of the account to which the user has authenticated, the event data permissions set (view, add, delete, modify), and the status of the data (locked, unlocked).

Protection of Event Data Transmitted Between NSM™ Components. Event data communicated between the physically-separated components of the Central Server and the Remote Console, between the physically-separated components of the Event Consolidator(s) and the Remote Console, and between the physically-separated Event Consolidator(s) and Central Server must be protected by SSL v3.0.

7 Assumptions and Clarification of Scope

Consumers of the NSM™ product should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of the NSM™.

7.1 Secure Usage Assumptions

It is assumed that administrators understand the correct use of the product and will abide by the instructions provided in the NSM™ documentation. The NSM™ must be installed and configured using the guidance specified in: *NSM™ Installation Guide Version 4.1*; *NSM™ Administration Guide Version 4.1;* and *NSM™ Basics Guide Version 4.1.*

7.2 Environmental Assumptions

The following assumptions are made about the operating environment of the NSM™:

a. the components of the NSM™ are located within controlled access facilities that will prevent unauthorised physical access; and

b. administrators are non-hostile and do not attempt to compromise the NSM™ functionality.

For more information about the NSM™ security environment, refer to Sections 3.1 and 5.3 of the ST.

7.3 Clarification of Scope

The NSM™ consolidates and manages event data received from security devices in the domain of deployment. The threat is considered to be unsophisticated attackers; the resources to be protected are considered to be system resources and event data. The NSM™ will not prevent an administrator from carelessly configuring, or using the NSM™, such that network protection is compromised.

8 Architectural Information

Figure 1 of the ST shows the NSM™ components in a typical installation configuration. The Remote Console, Central Server, Event Consolidator, and the Reporting System Server are proprietary to Intellitactics™ Incorporated and are developed in the Java® programming language. The Database component uses Microsoft® SQL Server™ 2000.

The Database stores audit data and the event data received from the security devices. Figure 1 of the ST shows a typical Database installation where only a single instance of the

Database is used. Separate Database instances can be used to store event data. These would be installed on the Event Consolidator platforms or on platforms directly connected to each Event Consolidator.

Audit data may be reviewed using either the Remote Console or a web browser launched by the Reporting System Server. The Remote Console displays the last 100 audit records and allows access to the records to users in the audit-review role. The web browser, through the use of the Reporting System Server, displays and allows searching of all audit records stored in the Database, but only allows access to the records to the audit-review role.

The Remote Console is a Graphical User Interface (GUI) that allows interaction between the NSM™ and the user. Through the Remote Console users can view, create, modify, and delete rules on the Central Server and any of the Event Consolidators, as allowed by their privileges. The Remote Console also allows users to view a visual representation of event data to help understand the activity on the monitored network.

The Central Server is the centre of the NSM™. It primarily processes messages received from Event Consolidators, but also has the ability to process messages received from other Central Servers and directly from third-party security devices. The Central Server performs user authentication, enforces any rules it contains, and generates audit data for all user-initiated actions performed on the server.

The Event Consolidator primarily processes messages from third-party security devices but also has the ability to process messages received from other Event Consolidators and the Central Server. The Event Consolidator enforces any rules it contains; thus it can be used to actively reduce resource utilisation on the Central Server. The Event Consolidator also generates audit data for all user-initiated actions performed on it.

The Reporting System Server is a World Wide Web (WWW) server that allows users to review, search, sort, and generate reports on audit data and stored event data.

9 Evaluated Configuration

The minimum evaluated configuration for the NSM™ comprises:

1. NSM™ v4.1 Remote Console running on a Windows® 2000 Server SP4/ Intel® platform with Internet Explorer® 6 SP1.

2. NSM™ v4.1 Central Server running on a Windows® 2000 Server SP4 / Intel® platform with Internet Explorer® 6 SP1.

3. NSM™ v4.1 Event Consolidator running on a Windows® 2000 Server SP4 / Intel® platform with Internet Explorer® 6 SP1.

4. NSM™ v4.1 Reporting System Server running on a Windows® 2000 Server SP4 / Intel® with Internet Explorer® 6 SP1.

5. NSM™ v4.1 Database running on a Windows® 2000 Server SP4 / Intel® platform with Internet Explorer® 6 SP1 and Microsoft SQL Server 2000.

Specific hardware requirements for each of the NSM™ components and the installation instructions for a secure configuration are specified in the NSM™ Installation Guide Version 4.1.

10 Documentation

The documentation for the NSM™ consists of:

a. NSM™ Installation Guide Version 4.1;

b. NSM™ Basics Guide Version 4.1; and

c. NSM™ Administration Guide Version 4.1.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the NSM™, including the following areas:

Configuration management: An analysis of the NSM™ development environment and associated documentation was performed. The evaluators found that the NSM™ configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the NSM™ during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the NSM™ functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the NSM™ user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Vulnerability assessment: The NSM™ Security Target's strength of function claims were validated and the developer's vulnerability analysis were validated by the evaluators. Limited penetration testing was conducted by evaluators, which exposed residual vulnerabilities not exploitable in the intended operating environment of the NSM™.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent vulnerability tests.

12.1 Assessing Developer Tests

The evaluators verified that the developer met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Technical Report (ETR)[2].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

12.2 Independent Functional Testing

As part of the test of a sample of the developer's tests, the evaluators repeated the entire installation, generation and start-up of the TOE on the supporting Windows® 2000 operating system.

During the evaluation, the evaluators developed independent functional tests by examining the design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

The testing focused on:

[2] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

a. Access control;

b. Boundary testing of the external interface supported by the TOE as defined in the functional specification;

c. Misuse by authorized personnel; and

d. Installation, generation, and start-up.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis and test activities, limited independent evaluator penetration testing was conducted. Penetration testing did not uncover any exploitable vulnerabilities for the NSM™ in the anticipated operating environment.

12.4 Conduct of Testing

The NSM™ was subjected to a comprehensive suite of formally-documented, independent, functional and penetration tests. The testing took place at the Intellitactics™ Incorporated facility in Kitchener, Ontario, and the IT Security Evaluation and Testing (ITSET) facility at Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario. The CCS Certification Body witnessed a portion of the independent testing.

The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in the ETR.

12.5 Testing Results

The developer tests and the independent functional tests yielded the expected results, giving assurance that the NSM™ behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 2** level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The complete documentation for the NSM™, v4.1 includes comprehensive Installation, Administration and User Guides.

The NSM™ v4.1 is straightforward to configure, use and integrate into a corporate network.

The NSM™ v4.1 graphical user interface is intuitive and easy to use.

Intellitactics™ Incorporated Quality Assurance (QA) provides the requisite controls for managing all QA testing.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
IDS	Intrusion Detection System
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NSM	Network Security Manager
QA	Quality Assurance
SSL	Secure Sockets Layer
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
WWW	World Wide Web

16 References

This section lists all documentation used as source material for this report:

a) Common Criteria for Information Technology Security Evaluation, CCIMB-99-031/032/033, Version 2.1, August 1999, incorporating all final interpretations issued prior to 28 February 2002.

b) Common Methodology for Information Technology Security Evaluation, CEM-99/045, Part 2: Evaluation and Methodology, Version 1.0, August 1999, incorporating all final interpretations issued prior to 28 February 2002.

c) CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002.

d) Security Target for the Intellitactics™ Incorporated Network Security Manager™ (NSM™) Version 4.1, Version v1.13, 18 November 2004.

e) Evaluation Technical Report (ETR), Intellitactics™ Incorporated Network Security Manager™ (NSM™) Version 4.1, EAL 2 Evaluation, Common Criteria Evaluation Number, 383-4-17, Document No. 1447-000-D002, Final Version 1.1, 24 November 2004.