Certification Report

EAL 3 Evaluation of NetIQ® Security Manager™ 6.5.3

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-111-CR
Version: 1.0
Date: 4 April 2011
Pagination: i to iii, 1 to 8

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 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. 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 Canada, 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 Communications Security Establishment Canada, 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 Canada.

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/IEC 17025:2005, General requirements for the Competence of Testing and Calibration 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 EWA-Canada 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 4 April 2011, 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 (CPL) and the Common Criteria Portal (the official website of the Common Criteria Project).

This certification report makes reference to the following registered trademarks:

- NetIQ® and Security Manager™ are registered trademarks of NetIQ Corporation;
- Linux is a registered trademark of Linus Torvalds Inc.;
- Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

TABLE OF CONTENTS

Executive Summary

NetIQ® Security Manager™ 6.5.3 (hereafter referred to as SM 6.5.3), from NetIQ Corporation, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 evaluation.

SM 6.5.3 is a Security Information and Event Management Solution (SIEM)[1]. As such, SM 6.5.3 collects and reacts to security event data from targeted IT systems; standardizes and archives the collected data; and generates reports for the review of collected data.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 15 March 2011 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 SM 6.5.3, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in 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 (ETR)[2] for this product provide sufficient evidence that it meets the EAL 3 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the SM 6.5.3 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 (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] A SIEM acts as an aggregator/consolidator of information from Intrusion Detection Systems (IDS), operating systems, firewalls, and antivirus applications.

[2] The ETR 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) 3 evaluation is NetIQ® Security Manager™ 6.5.3 (hereafter referred to as SM 6.5.3), from NetIQ Corporation.

2 TOE Description

SM 6.5.3 is a software only TOE comprising the components: NetIQ Security Manager Agents, NetIQ Central Computer, NetIQ Log Archive Server, and NetIQ Security Manager Console. Detail on these components is found in Section 1.4.1 of the ST.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for SM 6.5.3 is identified in Section 6 of the Security Target (ST).

4 Security Target

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

Title: NetIQ® Security Manager™ 6.5.3 Security Target
Version: V1.04
Date: 13 January 2011

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*.

SM 6.5.3 is:

a. *Common Criteria Part 2 extended*, with functional requirements based on functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
   - SIEM_ADM.1(EX) - Data Review;
   - SIEM_ALR.1(EX) - Data Alarms;
   - SIEM_COL(EX) - Data Collection;
   - SIEM_COR.1(EX) - Data Correlation; and
   - SIEM_STG.1(EX) - Data Loss Prevention.

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

c. *Common Criteria EAL 3 conformant*, with all the security assurance requirements from EAL 3 package.

6 Security Policy

SM 6.5.3 implements policies pertaining to data review, data alarms, data collection, data correlation, data loss, identification and authentication, and security management. Details on these security policies may be found in Sections 5 and 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of SM 6.5.3 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

a. The TOE has access to all the IT System data it needs to perform its functions.

b. The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

c. The TOE is appropriately scalable to the IT System the TOE monitors.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

a. The server components of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

b. There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

c. The authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

d. The systems, networks and all components will be available for use.

e. The systems will be configured to allow for proper usage of the application.

f. All networks will allow for communications between the components.

g. The TOE will be installed in an IT environment with that has the capability to provide private and authenticated network communications.

7.3 Clarification of Scope

SM 6.5.3 is not intended to be placed or operated in a hostile environment, and should be protected by other products specifically designed to address sophisticated threats.

8 Evaluated Configuration

The evaluated configuration for SM 6.5.3 comprises:

a. NetIQ Security Manager Console 6.5.3 running on Windows Vista, XP, Server 2003, and Windows 7;

b. NetIQ Security Manager Central Computer 6.5.3 running on Windows Server 2003 and Server 2008;

c. NetIQ Security Manager Log Archive Server 6.5.3 running on Windows Server 2003; and

d. NetIQ Security Manager Agent 6.5.3 running on Windows Vista, XP, Server 2003, Server 2008, and RHEL 5.

9 Documentation

The NetIQ documents provided to the consumer are as follows:

a. Installation Guide NetIQ Security Manager™, October 2010;

b. Programming Guide NetIQ Security Manager™, October 2010;

c. User Guide, NetIQ Security Manager™ , October 2010; and

d. Trial Guide NetIQ Security Manager™, October 2010.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of SM 6.5.3, including the following areas:

Development: The evaluators analyzed the SM 6.5.3 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the SM 6.5.3 security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the SM 6.5.3 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-Cycle Support: An analysis of the SM 6.5.3 configuration management system and associated documentation was performed. The evaluators found that the SM 6.5.3 configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well developed.

During the site visit the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the SM 6.5.3 design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of SM during distribution to the consumer.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of SM 6.5.3. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the SM 6.5.3 in its operational environment.

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

11 ITS Product Testing

Testing at EAL 3 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[3].

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

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

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining 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.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach was the following list of EWA-Canada test goals:

a. Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration, as identified in the TOE Description of the Security Target, by following all instructions in the developer's Installation and Administrative guidance;

b. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests on the evaluator's TOE installation; and

c. Claimed Functionality: The objective of this test goal is to exercise the TOE claimed functionality by deploying an NetIQ Security Manager Agent and collecting and reviewing Agent data.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on port scanning. The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

11.4 Conduct of Testing

SM 6.5.3 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Testing (ITSET) Facility at EWA-Canada. 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 a separate Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that SM 6.5.3 behaves as specified in its ST, functional specification, TOE design, and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 3 level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

SM 6.5.3 includes a comprehensive Installation and Security Guide, and Users Guide. SM 6.5.3 is straightforward to configure, use and integrate into a corporate network.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
CVE	Common Vulnerabilities and Exposures
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IDS	Intrusion Detection Systems
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
QA	Quality Assurance
SIEM	Security Information and Event Management
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

15 References

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

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, September 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, September 2009.

d. NetIQ® Security Manager™ 6.5.3 Security Target, V1.04, 13 January 2011.

e. Evaluation Technical Report (ETR) NetIQ® Security Manager™ 6.5.3, EAL 3 Evaluation, Common Criteria Evaluation Number: 383-4-111, Document No. 1616-000-D002, Version 2.0, 15 March 2011.