Certification Report

EAL 3+ Evaluation of NetIQ® Sentinel™ Version 7.0.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-202-CR
Version: 1.0
Date: 20 December 2012
Pagination: i to iii, 1 to 11

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, the 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.

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 20 December 2012, 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 trademarks or registered trademarks:

- NetIQ® is a registered trademark of NetIQ Corporation.

TABLE OF CONTENTS

Executive Summary

NetIQ® Sentinel™ Version 7.0.1 (hereafter referred to as Sentinel 7.0.1), from NetIQ Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

Sentinel 7.0.1 is a Security Information and Event Management Solution (SIEM) as well as a compliance monitoring solution. Sentinel 7.0.1 acts as an aggregator, as well as a consolidator for information from multiple systems (applications, databases, servers, storage, and security devices). It analyzes and correlates the data, and reduces the data to the point where it can be acted on, either automatically or manually.

Sentinel 7.0.1 automates log collection, analysis, and the reporting processes to ensure that IT controls are effective in supporting threat detection and audit requirements. Sentinel 7.0.1 provides automated monitoring of security and compliance events as well as IT controls. Finally Sentinel 7.0.1 provides real‐time reporting which allows one to take immediate action if there is a security breach or non‐compliant event.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 28 November 2012 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 Sentinel 7.0.1, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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)[1] for this product provide sufficient evidence that it meets the EAL 3 *augmented* 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*. The following augmentation is claimed: ALC_FLR.1 – Basic Flaw Remediation

.

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

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Sentinel 7.0.1 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 (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation is NetIQ® Sentinel™ Version 7.0.1 (hereafter referred to as Sentinel 7.0.1), from NetIQ Corporation.

2 TOE Description

Sentinel 7.0.1 is a Security Information and Event Management (SIEM) Solution as well as a compliance monitoring solution. Sentinel 7.0.1 acts as an aggregator, as well as a consolidator for information from multiple systems (applications, databases, servers, storage, and security devices). It analyzes and correlates the data, and reduces the data to the point where it can be acted on, either automatically or manually.

Sentinel 7.0.1 automates log collection, analysis, and the reporting processes to ensure that IT controls are effective in supporting threat detection and audit requirements. Sentinel 7.0.1 provides automated monitoring of security and compliance events as well as IT controls. Finally Sentinel 7.0.1 provides real-time reporting which allows one to take immediate action if there is a security breach or non-compliant event.

A detailed description of the Sentinel 7.0.1 architecture is found in Section 1.7 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Sentinel 7.0.1 is identified in Section 6 of the ST.

4 Security Target

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

Title: Security Target: NetIQ® Sentinel™ Version 7.0.1
Version: 1.4
Date: November 6, 2012

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.*

Sentinel 7.0.1 is:

a. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
    - SIEM_ANL.1 (EXP) - Event Analysis; and
    - SIEM_RES.1 (EXP) - Incident Resolution

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

c. *Common Criteria EAL 3 augmented*, containing all security assurance requirements in the EAL 3 package, as well as the following: ALC_FLR.1 – Basic Flaw Remediation.

6 Security Policy

Sentinel 7.0.1 implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information entering the system; details of these security policies can be found in Section 7 of the ST.

In addition, Sentinel 7.0.1 implements policies pertaining to security audit, identification and authentication, and security management. Further details on these security policies may be found in Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Sentinel 7.0.1 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:

- Administrators of the TOE are appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.
- Administrators of the TOE and users on the local area network are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The processing platforms on which the TOE resides are located within a facility that provides controlled access.
- The TOE is configured to receive all events from network-attached devices.
- The TOE has a trusted source for system time via a NTP server.

7.3 Clarification of Scope

Sentinel 7.0.1 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. Sentinel 7.0.1 is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for Sentinel 7.0.1 comprises:

Component	Requirement
Sentinel 7.0.1 Server	GPC running SUSE Linux Enterprise Server (SLES) 11 SP1 64-bit and; VMWare ESX 4.0; Xen 4.0; or Hyper‑V Server 2008 R2 with the DVD ISO file only
Sentinel Log Manager 1.2.0	GPC running SUSE Linux Enterprise Server (SLES) 11 SP1 64-bit and; VMWare ESX 3.5 or 4.0; or Xen 3.1.1
Data Collector	GPC running SUSE Linux Enterprise Server (SLES) 11 SP1 64-bit
Correlation Engine	GPC running SUSE Linux Enterprise Server (SLES) 11 SP1 64-bit
Console	GPC running Windows 7 (Firefox 3.6 or IE 8) or SLED 11 SP1 / RHEL 6 (Firefox 3.6)

The publication entitled “Operational User Guidance and Preparative Procedures Supplement: NetIQ Sentinel 7.0.1 Document Version 1.3” describes the procedures necessary to install and operate Sentinel 7.0.1 in its evaluated configuration.

9 Documentation

The NetIQ Corporation documents provided to the consumer are as follows:

a. Operational User Guidance and Preparative Procedures Supplement: NetIQ Sentinel 7.0.1 Document Version 1.3, September 2012

b. User Guide: Sentinel 7.0.1, April 2012;

c. Administration Guide: Sentinel 7.0.1, April 2012;

d. Overview Guide: Sentinel 7.0.1, April 2012;

e. NetIQ Sentinel 7.0.1 Quick Start Guide, April 2012; and

f. Installation and Configuration Guide: NetIQ Sentinel 7.0.1, April 2012

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Sentinel 7.0.1, including the following areas:

Development: The evaluators analyzed the Sentinel 7.0.1 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 Sentinel 7.0.1 security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Sentinel 7.0.1 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes 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 Sentinel 7.0.1 configuration management system and associated documentation was performed. The evaluators found that the Sentinel 7.0.1 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 Sentinel 7.0.1 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 Sentinel 7.0.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by NetIQ Corporation for Sentinel 7.0.1. During a site visit, the evaluators examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of Sentinel 7.0.1. 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 Sentinel 7.0.1 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[2].

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.

[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.

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 is the following list of EWA-Canada test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Identification and Authentication: The Objective of this test goal is to test the verification of user attributes and identification and authentication of TOE users.

c. Security Management: The objective of this test goal is to confirm the TOE's ability to maintain security attributes and that only administrators, and not users, may manage users.

d. Incident Management: The objective of this test goal is to confirm that the TOE can manage incidents that occur using filtering, correlation; and work flows.

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:

a. Port Scan: The objective of this test goal is to scan the TOE using a port scanner to reveal an potential avenues of attack;

b. Vulnerability Identification: Tool Scanning: The objective of this test goal is to scan the TOE for vulnerabilities using automated tools;

c. Information Leakage Verification: The objective of this test goal is to monitor the TOE for leakage during start-up, shutdown, login, and other scenarios using a packet sniffer; and

d. Privilege escalation: The objective of this test goal is to confirm that the TOE is not vulnerable to the privilege escalation attack identified during the public domain search.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

11.4 Conduct of Testing

Sentinel 7.0.1 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 Test (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 Sentinel 7.0.1 behaves as specified in its ST and functional specification and TOE design.

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

Sentinel 7.0.1 is a mature, well documented product. The documentation provides valuable advice for implementing the TOE in a secure manner, and should be followed, particularly with respect to the database implementation. Note that the use of the Command Line Utility is not included in the evaluated configuration.

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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada

Acronym/Abbreviation/ Initialization	Description
SFR	Security Functional Requirement
SIEM	Security Information 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, July 2009.

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

d. Security Target: NetIQ® Sentinel™ Version 7.0.1, 1.4, November 6, 2012

e. Evaluation Technical Report for EAL 3+ Common Criteria Evaluation of NetIQ® Sentinel™ 7.0.1, Version 1.1, 28 November 2012