Certification Report

Securonix Security Intelligence Platform 4.0.5

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-269-CR
Version: 1.0
Date: 13 February 2015
Pagination: i to iii, 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 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. This certification report, and its associated certificate, applies 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, 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, 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/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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 13 February 2015, 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).

TABLE OF CONTENTS

Executive Summary

Securonix Security Intelligence Platform 4.0.5 (hereafter referred to as Securonix SIP 4.0.5), from Securonix, is the Target of Evaluation. The results of this evaluation demonstrate that Securonix SIP 4.0.5 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

Securonix SIP 4.0.5 is an enterprise application written in Java and supports major databases. The TOE has native integration with products in the security industry – Log Management, SIEM, Database Monitoring, Identity Management, DLP and Privileged Access Management solutions. The TOE type is a security incident and event management (SIEM) system used to manage risk.

The TOE uses a signature-less threat detection and flexible risk scoring algorithms to detect and score rogue transactions, access privileges and security events. The technology utilizes behavior based risk analytics and peer group analysis techniques that are capable of detecting unseen attacks launched from within or outside the perimeter of the organization.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 13 February 2015 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 Securonix SIP 4.0.5, and the security functional/assurance 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.

Communications Security Establishment, as the CCS Certification Body, declares that the Securonix SIP 4.0.5 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

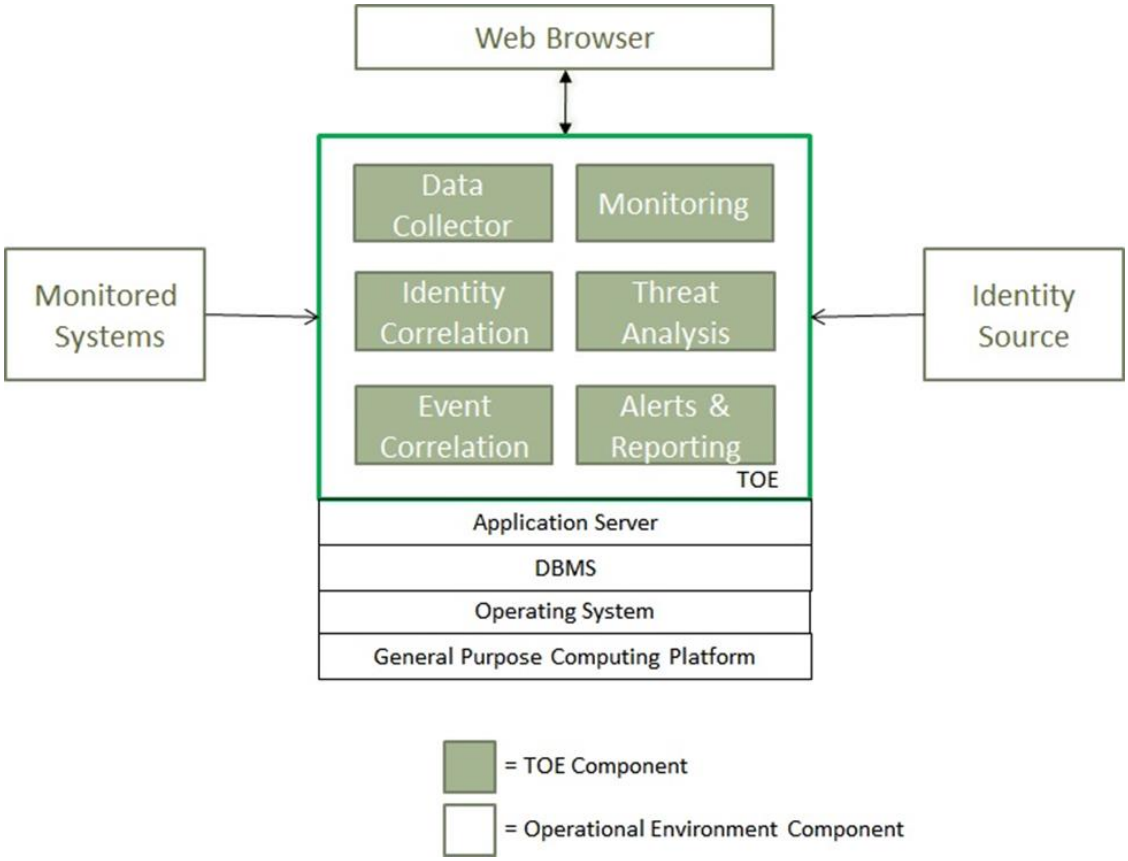
The Target of Evaluation (TOE) for this EAL 2+ evaluation is Securonix Security Intelligence Platform 4.0.5 (hereafter referred to as Securonix SIP 4.0.5), from Securonix.

2 TOE Description

Securonix SIP 4.0.5 is an enterprise application written in Java and supports major databases. The TOE has native integration with products in the security industry – Log Management, SIEM, Database Monitoring, Identity Management, DLP and Privileged Access Management solutions. The TOE type is a security incident and event management (SIEM) system used to manage risk.

The TOE uses a signature-less threat detection and flexible risk scoring algorithms to detect and score rogue transactions, access privileges and security events. The technology utilizes behavior based risk analytics and peer group analysis techniques that are capable of detecting unseen attacks launched from within or outside the perimeter of the organization.

A diagram of the Securonix SIP 4.0.5 architecture is as follows:



3 Security Policy

Securonix SIP 4.0.5 implements a role-based access control policy to control administrative access to the system. In addition, Securonix SIP 4.0.5 implements policies pertaining to the following security functional classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Incident Management

4 Security Target

The ST associated with this Certification Report is identified below:

Security Target: Securonix Security Intelligence Platform 4.0, Version 1.12, 9 January 2015

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

Securonix SIP 4.0.5 is:

a. *EAL 2 augmented, containing all security assurance requirements listed, as well as the following:*
    - *ALC_FLR.2 – Flaw Reporting Procedures*

b. *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:*
    - *SIM_ANL.1 - Event Analysis (EXT)*
    - *SIM_RES.1 - Incident Resolution (EXT)*
    - *SIM_SDC.1 - Security Data Collection (EXT)*

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

6 Assumptions and Clarification of Scope

Consumers of Securonix SIP 4.0.5 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- *Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner; and*
- *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.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The processing platforms on which the TOE resides are assumed to be located within a facility that provides controlled access;*
- *The processing platforms on which the TOE resides and the TOE software critical to security policy enforcement will be protected from unauthorized physical modification;*
- *The TOE is configured to receive all events from network-attached devices; and*
- *The TOE has a trusted source for system time via NTP server.*

7 Evaluated Configuration

The evaluated configuration for Securonix SIP 4.0.5 comprises:

The TOE software running on a server platform with the following specs:

OS: CentOS 64 bit v6.5

JRE: 1.7

CPU: Intel i7 Processor

Memory: 16GB RAM

Storage: 1TB Internal Storage

With support from a MySQL 64 bit v5.5 database and a Securonix hardened Apache Tomcat server v7.0.

The publication entitled Operational User Guidance: Securonix Security Intelligence Platform 4.0, Version 1.6, 7 January 2015 describes the procedures necessary to install and operate Securonix SIP 4.0.5 in its evaluated configuration.

8 Documentation

The Securonix documents provided to the consumer are as follows:

a. Operational User Guidance: Securonix Security Intelligence Platform 4.0, Version 1.6, 7 January 2015

b. Securonix Administrator Guide Version 4.0, (available online);

c. Securonix Deployment Guide, Version 4.0, (available online);

d. Securonix Install Guide, Version 4.0, (available online);

e. Securonix Release Notes, Version 4.0, (available online); and

f. Securonix User Guide, Version 4.0, (available online).

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Securonix SIP 4.0.5, including the following areas:

Development: The evaluators analyzed the Securonix SIP 4.0.5 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 Securonix SIP 4.0.5 security architectural description and determined that the initialization process is secure, 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 Securonix SIP 4.0.5 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 Securonix SIP 4.0.5 configuration management system and associated documentation was performed. The evaluators found that the Securonix SIP 4.0.5 configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Securonix SIP 4.0.5 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the Securonix SIP 4.0.5. During a site visit, the evaluators also 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

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

10 ITS Product Testing

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

10.1 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[1].

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.

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

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 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. Concurrent Login Behaviour: The objective of this test goal is to determine how the TOE responds to concurrent logins

c. Authentication Failure, Security Management, and Audit Data Generation and Review: The objective of this test goal is to test the authentication failure, security management and audit generation/review functionality; and

d. Audit Event Tampering: The objective of this test goal is to attempt to tamper with the audit log.

10.3 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. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities.

b. Heartbleed scan: The objective of this test goal is to scan the TOE for susceptibility to Heartbleed vulnerability;

[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.

c. Poodle scan: The objective of this test goal is to scan the TOE for susceptibility to the Poodle vulnerability;

d. Shellshock scan: The objective of this test goal is to scan the TOE for susceptibility to the Shellshock vulnerability; and

e. GHOST scan: The objective of this test goal is to scan the TOE for susceptibility to the GHOST vulnerability.

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

10.4 Conduct of Testing

Securonix SIP 4.0.5 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 Facility. 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.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that Securonix SIP 4.0.5 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

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

12 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
JRE	Java Runtime Environment
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

13 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 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Security Target: Securonix Security Intelligence Platform 4.0, Version 1.12, 9 January 2015

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of Securonix Security Intelligence Platform 4.0 Document No. 1834-000-D002 Version 1.0, 13 February 2015.