Certification Report

EAL 3+ Evaluation of Trustwave SIEM Operations Edition Version 5.9.0 and Trustwave SIEM LP Software Version 1.2.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-210-CR
Version: 1.0
Date: 19 July 2012
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 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 located in Ottawa, 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 19 July 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).

TABLE OF CONTENTS

Executive Summary

Trustwave SIEM Operations Edition Version 5.9.0 and Trustwave SIEM LP Software Version 1.2.1 (hereafter referred to as Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1), from Trustwave Holdings, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 augmented, evaluation.

Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 provide Security Information and Event Management (SIEM) functionality to normalize and correlate security information received from third party security devices. These third party security devices may include IDS/IPS sensors and/or scanners, firewalls, servers, or other types of systems capable of sending security information to the TOE. The received information is correlated and analyzed by the TOE to determine if any alerts should be generated. The TOE consists of software only.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 04 July 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 Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1, 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.2 – Flaw Reporting Procedures.

Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 is conformant with the U.S. Government Protection Profile Intrusion Detection System Analyzer for Basic Robustness Environments, version 1.3, dated July 25, 2007.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1

[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.

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 Trustwave SIEM Operations Edition Version 5.9.0 and Trustwave SIEM LP Software Version 1.2.1 (hereafter referred to as Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1), from Trustwave Holdings, Inc.

2 TOE Description

Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 provide Security Information and Event Management (SIEM) functionality to normalize and correlate security information received from third party security devices. These third party security devices may include Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) sensors and/or scanners, firewalls, servers, or other types of systems capable of sending security information to the TOE. The received information is correlated and analyzed by the TOE to determine if any alerts should be generated. The TOE consists of software only.

A detailed description of the Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 architecture is found in Section 1.5 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 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: Trustwave SIEM LP Software and SIEM Operations Edition Security Target
Version: Version 1.12
Date: June 28, 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.*

Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 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:

- IDS_ANL.1 - Analyser Analysis;
- IDS_RCT.1 - Analyser React;
- IDS_RDR.1 - Restricted Data Review;
- IDS_STG.1 - Guarantee of Analyser Data Availability; and
- IDS_STG.2 - Prevention of Analyser Data Loss.

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.2 – Flaw Reporting Procedures.
d. Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 claims demonstrable conformance to the *U.S. Government Protection Profile Intrusion Detection System Analyzer for Basic Robustness Environments, version 1.3,* dated July 25, 2007.

6 Security Policy

Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 implement a restricted data review policy which restricts access to alert and event information collected by the TOE to authorized administrators. Details of this security policy can be found in Section 6 of the ST.

In addition, Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 implement policies pertaining to security audit, identification and authentication, security management; protection of the TOE Security Functionality (TSF), and intrusion detection. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 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:

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

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

- The TOE can only be accessed by authorized users.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- The TOE has access to all the IT System resources necessary to perform its functions.

7.2 Environmental Assumptions

The following Environmental Assumptions listed in the ST:

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The TOE components will be interconnected by a segregated management network that protects the intra-TOE traffic from disclosure or modification by untrusted systems or users.

7.3 Clarification of Scope

Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 offer protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. SIEM OE Version 5.9.0 and SIEM LP Version 1.2.1 are 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 Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 comprises the following:

- Trustwave SIEM Operations Edition Version 5.9.0 build 44 with hot fixes 1-6 server components running on Red Hat Enterprise Linux 5.
- Trustwave SIEM Operations Edition Version 5.9.0 build 44 with hot fixes 1-6 administration and operations consoles running on Windows XP SP3.
- Trustwave SIEM LP Software Version 1.2.1 build 269 pre-installed on dedicated appliances supplied by Trustwave Holdings, Inc.

The publication entitled *Trustwave SIEM LP Software V1.2.1 and SIEM Operations Edition V5.9 Common Criteria Supplement, Version 1.4, 28 June 2012* describes the procedures necessary to install and operate SIEM OE Version 5.9.0 and SIEM LP Version 1.2.1 in its evaluated configuration.

9 Documentation

The Trustwave Holdings, Inc. documents provided to the consumer are as follows:

a. Trustwave SIEM Operations Edition - Installation Guide – Version 5.9;

b. Trustwave SIEM Operations Edition - Getting Started Guide – Version 5.9;

c. Trustwave SIEM Operations Edition - Configuration Guide - Version 5.9;

d. Trustwave SIEM Operations Edition - Administration Guide – Version 5.9;

e. Trustwave SIEM Operations Edition - Alert Management User Guide - Version 5.9;

f. Trustwave SIEM Operations Edition - Reporting Guide - Version 5.9;

g. Trustwave SIEM Administration Guide for LP and XL;

h. Trustwave SIEM User Guide for LP and XL;

i. Trustwave SIEM Quick Start Guide;

j. Trustwave SIEM Administration Guide for LP and XL;

k. Trustwave SIEM Notifications Guide; and

l. Trustwave SIEM LP Software V1.2.1 and SIEM Operations Edition V5.9 Common Criteria Supplement, Version 1.4, 28 June 2012.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1, including the following areas:

Development: The evaluators analyzed the Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 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 Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 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 Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 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 Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 configuration management system and associated documentation was performed. The evaluators found that the Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 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 Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 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 Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Trustwave Holdings, Inc. for Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1. 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 Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1. 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 Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 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.

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. Security Audit – The objective of this test goal is to exercise the audit functionality of the TOE;

c. Security Management – The objective of this test goal is to verify that he TOE provides functionality for administrators to configure and monitor the operation of the TOE;

d. Identification and Authentication – The objective of this test goal is to demonstrate the administrator identification and authorization process and the disabling of the administrator account after 3 consecutive login failures; and

e. Data Collection and Display – The objective of this test goal is to demonstrate the TOE's functionality related to the collection and display of event data and verify that the viewing of event data is restricted to authorized administrators.

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:

[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.

a. Port scanning: The objective of this test goal was to scan the TOE using a port scanner to determine what ports were open and what services were running;

b. Banner Grabbing: The objective of this test goal was to attempt to capture any identification banner or response that may reveal the operating system or TOE that is running; and

c. Leakage: The objective of this test goal was to examine captured login information to determine if the TOE leaks sensitive information during login.

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

11.4 Conduct of Testing

Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 were 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 Trustwave SIEM OE Version 5.9.0 and Trustwave SIEM LP Version 1.2.1 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 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

Acronym/Abbreviation/ Initialization	Description
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
OE	Operations Edition
PALCAN	Program for the Accreditation of Laboratories - Canada
SIEM	Security Information and Event Management
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

14 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. U.S. Government Protection Profile Intrusion Detection System Analyzer for Basic Robustness Environments, version 1.3, July 25, 2007.

e. Trustwave SIEM LP Software and SIEM Operations Edition Security Target, Version 1.12, June 28, 2012.

f. Evaluation Technical Report for EAL 3+ Common Criteria Evaluation of Trustwave SIEM LP Software Version 1.2.1 and SIEM Operations Edition Version 5.9.0, Document No. 1732-000-D002 Version 1.1, 4 July 2012.