# Certification Report

## Trustwave SIEM Enterprise Version 2.3.3

Issued by:

**Communications Security Establishment**

**Certification Body**

**Canadian Common Criteria Evaluation and Certification Scheme**



**Document number**: 383-4-339-CR
**Version**: 1.0
**Date**: 14 April 2016
**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 14 April 2016, 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 Enterprise Version 2.3.3 is the Target of Evaluation (TOE). The results of this evaluation demonstrate that Trustwave SIEM Enterprise Version 2.3.3 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

Trustwave SIEM Enterprise Version 2.3.3 provides 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 Trustwave SIEM LME appliances, intrusion detection system/intrusion prevention system 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.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 14 April 2016 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 Enterprise Version 2.3.3, 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 Trustwave SIEM Enterprise Version 2.3.3 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).

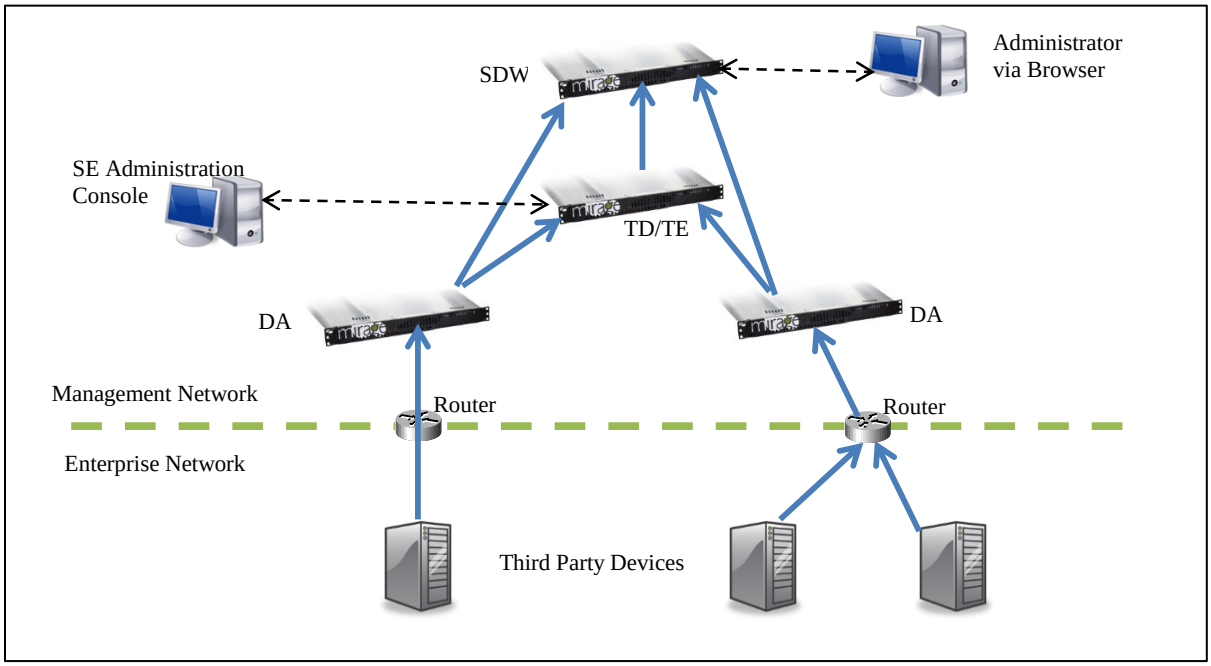
# 1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is Trustwave SIEM Enterprise Version 2.3.3, from Trustwave Holdings, Inc..

# 2 TOE Description

Trustwave SIEM Enterprise Version 2.3.3 provides 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 Trustwave SIEM LME appliances, intrusion detection system/intrusion prevention system 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.

A diagram of the Trustwave SIEM Enterprise Version 2.3.3 architecture is as follows:




# 3 Security Policy

Trustwave SIEM Enterprise Version 2.3.3 implements a role-based access control policy to control administrative access to the system. In addition, Trustwave SIEM Enterprise Version 2.3.3 implements policies pertaining to the following security functional classes:

- Security Audit,
- Identification and Authentication,
- Security Management,
- Protection of the TOE Security Functions (TSF), and
- Intrusion Detection.

# 4 Security Target

The ST associated with this Certification Report is identified below:

Trustwave SIEM Enterprise Security Target, Version 2.7, April 11, 2016.

# 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.

Trustwave SIEM Enterprise Version 2.3.3 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:
    - IDS_ANL.1 - Analyser Analysis
    - IDS_RCT.1 - Analyser React
    - IDS_RDR.1 - Restricted Data Review
    - IDS_STG.1 - Guarantee of Analyser Data Availability
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 Trustwave SIEM Enterprise Version 2.3.3 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.

## 6.1 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.*

## 6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The TOE has access to all the IT System resources necessary to perform its functions.*
- *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 to or modification by untrusted systems or users, and limits traffic from the enterprise network entering the management network to security information from third party security devices being sent via UDP to the DA components of the TOE.*
- *The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.*

# 7 Evaluated Configuration

The evaluated configuration for Trustwave SIEM Enterprise Version 2.3.3 comprises Trustwave SIEM Enterprise Version 2.3.3 (Build 856) software running on the LME 2 and the LME 3 physical and virtual appliances and the Trustwave SIEM Enterprise Administration Console Version 2.3.3 (Build 197) running on Windows 7.

The publication entitled Trustwave SIEM Enterprise Common Criteria Supplement, Version 1.1, March 27, 2016 describes the procedures necessary to install and operate Trustwave SIEM Enterprise Version 2.3.3 in its evaluated configuration.

# 8 Documentation

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

a. Trustwave SIEM Quick Start Guide, Version 2.3.1, March 2015

b. Trustwave SIEM Enterprise Administration Guide, Version 2.3.1, March 2015

c. Trustwave SIEM Enterprise User Guide, Version 2.3, November 2014

d. Trustwave SIEM Enterprise TD/TE Configuration Guide, Version 2.3, November 2014

e. Trustwave SIEM Enterprise Common Criteria Supplement, Version 1.1, March 27, 2016

f. Trustwave SIEM Enterprise/Log Management Enterprise - Deploying and Resizing the Virtual Appliance, March 2014

g. Trustwave SIEM Enterprise VM Quick Start, December 2013

# 9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Trustwave SIEM Enterprise Version 2.3.3, including the following areas:

**Development:** The evaluators analyzed the Trustwave SIEM Enterprise Version 2.3.3 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 Trustwave SIEM Enterprise Version 2.3.3 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 Trustwave SIEM Enterprise Version 2.3.3 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 Enterprise Version 2.3.3 configuration management system and associated documentation was performed. The evaluators found that the Trustwave SIEM Enterprise Version 2.3.3 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 Trustwave SIEM Enterprise Version 2.3.3 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the Trustwave SIEM Enterprise Version 2.3.3. 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: The objective of this test goal is to demonstrate that the TOE permits concurrent user login and that they do not conflict;

c. Password Strength: The objective of this test goal is to demonstrate that the TOE enforces password complexity rules;

d. Authentication Failure Handling: The objective of this test goal is to demonstrate how the TOE handles an authentication failure; and

e. Session Locking: The objective of this test goal is to verify that the TOE will lock an administrator session after a defined period of inactivity.

## 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; and

b. Big 5 scan: The objective of this test goal is to scan for the current "Big 5" vulnerabilities (Heartbleed, Shellshock, POODLE, GHOST, and FREAK).

[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.

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

### 10.4 Conduct of Testing

Trustwave SIEM Enterprise Version 2.3.3 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. 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 Trustwave SIEM Enterprise Version 2.3.3 behaves as specified in its ST and functional specification.

## 11 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.

# 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 |
| DA | Data Acquisition |
| 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 |
| SDW | Secure Data Warehouse |
| SE | SIEM Enterprise |
| SIEM | Security Information and Event Management |
| SFR | Security Functional Requirement |
| ST | Security Target |
| TD | Threat Detector |
| TE | Threat Evaluator |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |
| UDP | User Datagram Protocol |

# 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. Trustwave SIEM Enterprise Security Target, Version 2.7, April 11, 2016.

e. Evaluation Technical Report Trustwave Holdings, Inc. SIEM Enterprise Version 2.3, Version 1.0, April 14, 2016.