Communications Security Establishment

Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Illumio Adaptive Security Platform v18.2.2

Illumio

12 July 2019

383-4-459

V1.0

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

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 Centre for Cyber Security (CCCS). 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 Canadian CC Scheme, 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 Canadian Centre for Cyber Security, 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 Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Contact Centre and Information Services
Edward Drake Building
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Scheme 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 Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCEF is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the 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.

The certification report, certificate of product evaluation and security target are listed on the Certified Products list (CPL) for the Canadian CC Scheme and posted on the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

EXECUTIVE SUMMARY 6

1 Identification of Target of Evaluation 7

1.1 Common Criteria Conformance 7

1.2 TOE Description 7

1.3 TOE Architecture 7

2 Security Policy 8

2.1 Cryptographic Functionality 8

3 Assumptions and Clarification of Scope 9

3.1 Usage and Environmental Assumptions 9

4 Evaluated Configuration 10

4.1 Documentation 10

5 Evaluation Analysis Activities 11

5.1 Development 11

5.2 Guidance Documents 11

5.3 Life-Cycle Support 11

6 Testing Activities 12

6.1 Assessment of Developer tests 12

6.2 Conduct of Testing 12

6.3 Independent Functional Testing 12

6.3.1 Functional Test Results 12

6.4 Independent Penetration Testing 13

6.4.1 Penetration Test results 13

7 Results of the Evaluation 14

7.1 Recommendations/Comments 14

8 Supporting Content 15

8.1 List of Abbreviations 15

8.2 References 15

LIST OF FIGURES

Figure 1: TOE Architecture 7

LIST OF TABLES

Table 1: TOE Identification 7

Table 2: Cryptographic Implementation(s) 8

EXECUTIVE SUMMARY

The Illumio Adaptive Security Platform v18.2.2 (hereafter referred to as the Target of Evaluation, or TOE), from Illumio , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

CygnaCom Solutions is the CCEF that conducted the evaluation. This evaluation was completed 12 July 2019 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for TOE, 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.

The Canadian Centre for Cyber Security, as the Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian CC Scheme and the Common Criteria portal (the official website of the International Common Criteria Project).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	Illumio Adaptive Security Platform v18.2.2
Developer	Illumio

1.1 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.

The TOE is claims the following conformance;

Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1, October 24, 2013

1.2 TOE DESCRIPTION

The TOE consists of the Policy Compute Engine and the Virtual Enforcement Node. Together, these components form a distributed software platform that is designed to continuously protect communications within and, across, tiers of applications and hosts. The TOE enables administrators to create access control policies to secure and to implement granular segmentation of hosts and applications within the enterprise network.

1.3 TOE ARCHITECTURE

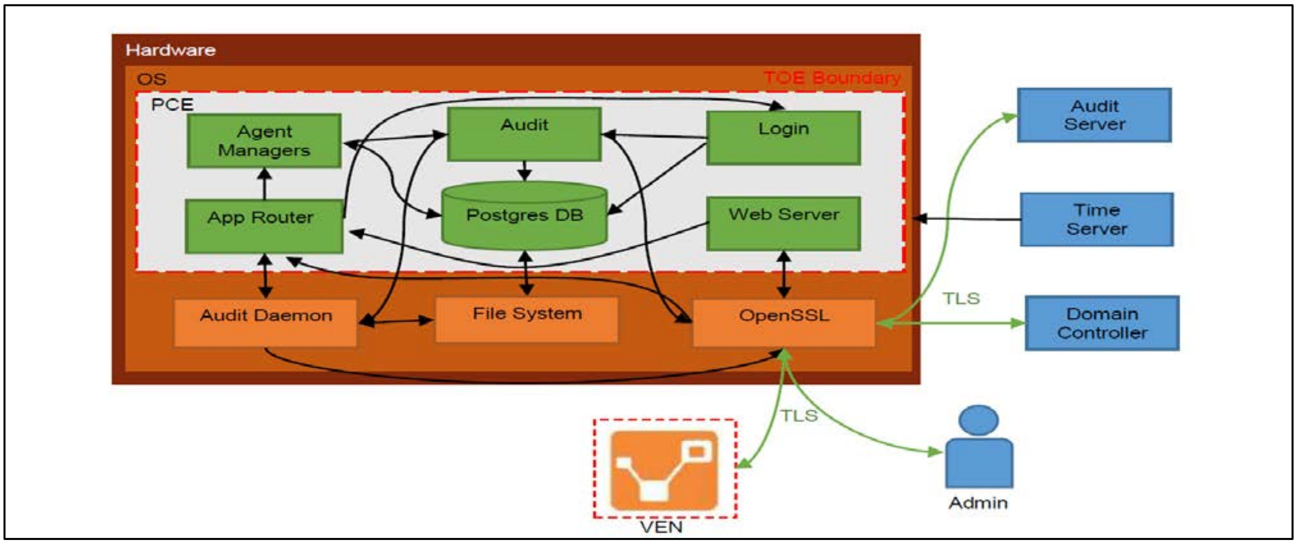

Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Enterprise Security Management
- Cryptographic Support
- Security Audit
- Identification and Authentication
- Security Management
- TOE Access
- Protection of the TSF
- Trusted Path/Channels

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementations have been evaluated by the CMVP and are used by the TOE:

Table 2: Cryptographic Implementation(s)

Cryptographic Module	Certificate Number
Red Hat Enterprise Linux OpenSSL Cryptographic Module	3016
Windows Server 2016 Cryptographic Primitives Library	2937
Windows Server 2012 R2 Cryptographic Primitives Library	2357

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE 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.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
- The TOE will be able to establish connectivity to other ESM products in order to share security data.
- The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
- The TOE will receive reliable time data from the Operational Environment.
- The TOE will receive identity data from the Operational Environment.
- There will be one or more competent individuals assigned to install, configure, and operate the TOE.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

- Policy Compute Engine v18.2.2-13462 running on Red Hat Enterprise Linux 7.4 installed on Intel Core i7 with AES-NI, Intel Core i5 with AES-NI and Intel Xeon E5 with AES-NI.
- Virtual Enforcement Node v18.2.2-4339 running on Windows Server 2016 installed on Intel Xeon E5 with AES-NI and running on Windows Server 2012 installed on Intel Xeon E5 with AES-NI.

The TOE requires the following components in the operational environment:

- Audit Server
- Authentication Server
- DNS Server
- NTP Server

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a) Illumio Adaptive Security Platform 18.2.2 PCE Operations Guide 03/20/2019
b) Illumio Adaptive Security Platform 18.2.2 PCE Deployment Guide 03/20/2019
c) Illumio Adaptive Security Platform 18.2.2 PCE Web Console User Guide Version 18.2.2
d) Illumio Adaptive Security Platform 18.2.2 VEN Operations Guide 03/20/2019
e) Illumio Adaptive Security Platform 18.2.2 VEN Deployment Guide 03/20/2019
f) Illumio Adaptive Security Platform (ASP) Common Criteria Administrator Guide, Document Version 0.8, 03/06/2019

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements (SFRs). The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE 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.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE 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 the TOE during distribution to the consumer.

6 TESTING ACTIVITIES

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

6.1 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. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE 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.

6.3 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. The following testing activities were performed:

a. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP; and

b. Verification of Cryptographic Modules: The evaluator confirmed that the claimed cryptographic modules are present in the operational environment.

6.3.1 FUNCTIONAL TEST RESULTS

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

6.4 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 such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST;

b) SQL Injection Attacks: The purpose of this test is to observe how the Policy Compute Engine handles attempted SQL attacks via changes to the URL; and

c) Session Cookie Inspection: The purpose of this test case is to observe how the Policy Compute Engine handles attempts to hijack web session cookies.

6.4.1 PENETRATION TEST RESULTS

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

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

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 Centre for Cyber Security (CCCS). This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CCCS or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CCCS or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CCCS	Canadian Centre for Cyber Security
EAL	Evaluation Assurance Level
ESM	Enterprise Security Management
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
Illumio Adaptive Security Platform Security Target, Version 1.3, July 9, 2019.
Illumio Adaptive Security Platform Evaluation Technical Report, Version 1.0, July 12, 2019.
Illumio Adaptive Security Platform Assurance Activity Report, Version 1.6, July 12, 2019.