# C097 Certification Report

## Trend Micro TippingPoint Security Management System

File name: ISCB-5-RPT-C097-CR-v1
Version: v1
Date of document: 9 October 2018
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan

# C097 Certification Report

## Trend Micro TippingPoint Security Management System

9 October 2018

ISCB Department

**CyberSecurity Malaysia**

Level 5, Sapura@Mines,
No 7 Jalan Tasik,The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 □Fax: +603 8992 6841
http://www.cybersecurity.my

# Document Authorisation

| | |
|---|---|
| ***DOCUMENT TITLE:*** | C097 Certification Report |
| ***DOCUMENT REFERENCE:*** | ISCB-5-RPT-C097-CR-v1 |
| ***ISSUE:*** | v1 |
| ***DATE:*** | 9 October 2018 |

| | |
|---|---|
| ***DISTRIBUTION:*** | UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION |

# Copyright and Confidentiality Statement



Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Limited by Guarantee

Company No. 726630-U

*Printed in Malaysia*

# Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB 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 09 October 2018 and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

# Disclaimer

The Information Technology (IT) product identified in this certification report and its associated certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (Ref [2]). 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 MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

# Document Change Log

| RELEASE | DATE | PAGES AFFECTED | REMARKS/CHANGE REFERENCE |
|---|---|---|---|
| d1 | 19 September 2018 | All | Initial draft of certification report |
| v1 | 2 October 2018 | All | Final Certification report |

# Executive Summary

The Target of Evaluation (TOE) is Trend Micro TippingPoint Security Management System (SMS) version 5.1.0. The TOE provides a server-based solution that acts as the control center for managing large-scale deployments of TippingPoint devices, including TippingPoint Threat Protection System (TPS) and TippingPoint Intrusion Prevention System (IPS). A single SMS can manage multiple TippingPoint devices—the maximum number depends on usage, network, and other environmental conditions.

The scope of the evaluation is defined by the Security Target (Ref [6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by BAE Systems Applied Intelligence MySEF (Malaysia Security Evaluation Facility) and completed on 3 September 2018.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at http://www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that Trend Micro TippingPoint Security Management System (SMS) v5.1.0 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

# Table of Contents

# Index of Tables

# 1 Target of Evaluation

## 1.1 TOE Description

1 The TOE is TippingPoint Security Management System (SMS) v5.1.0 from Trend Micro. The TOE provides a server-based solution that acts as the control center for managing large-scale deployments of TippingPoint devices, including TippingPoint Threat Protection System (TPS) and TippingPoint Intrusion Prevention System (IPS). A single SMS can manage multiple TippingPoint devices—the maximum number depends on usage, network, and other environmental conditions.

2 The functionality defined in the Security Target (Ref [6]) that was subsequently evaluated is as follows:

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

## 1.2 TOE Identification

3 The details of the TOE are identified in Table 1 below.

Table 1: TOE Identification

| | |
|---|---|
| **Evaluation Scheme** | Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme |
| **Project Identifier** | C097 |
| **TOE Name** | Trend Micro TippingPoint Security Management System |
| **TOE Version** | 5.1.0 |
| **Security Target Title** | Trend Micro TippingPoint Security Management System Security Target |
| **Security Target Version** | Version 1.0 |
| **Security Target Date** | 21 August 2018 |
| **Assurance Level** | Evaluation Assurance Level 2 |
| **Criteria** | Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2]) |

| | |
|---|---|
| **Methodology** | Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3]) |
| **Protection Profile Conformance** | None |
| **Common Criteria Conformance** | CC Part 2 Conformant<br>CC Part 3 Conformant<br>Package conformant to EAL 2 |
| **Sponsor** | Leidos Inc.<br>6841 Benjamin Franklin Drive, Columbia, Maryland 21046 USA |
| **Developer** | Trend Micro Incorporated<br>11305 Alterra Parkway, Austin, Texas 78758 USA |
| **Evaluation Facility** | BAE Systems Applied Intelligence – MySEF (Malaysia Security Evaluation Facility)<br>Level 28, Menara Binjai, 2 Jalan Binjai, 50450 Kuala Lumpur, Malaysia |

## 1.3 Security Policy

4 There are no organisational security policies that have been defined regarding the use of the TOE.

## 1.4 TOE Architecture

5 The TOE includes both logical and physical boundaries as described in Section 2.3 and 2.4 of the Security Target (Ref [6]).

### 1.4.1 Physical Boundaries

6 The TOE architecture consists of the following components:

- SMS Server: The SMS server can be provisioned as a rack-mountable appliance (SMS H3 or SMS H3 XL) or as a virtual server (vSMS). The server is built on top of CentOS and includes a MariaDB database and JBoss 5.1 GA application server. Section 2.3.1 of the ST (Ref. [6]) details the hardware specifications for both appliance models and the minimum system requirements for the vSMS platform. It also incorporates Network Security Services and OpenSSL cryptographic modules to provide support respectively for Transport Layer Security (TLS) and Secure Shell (SSH) cryptographic protocols.
- SMS Client: A Java-based application for Windows, Linux or Mac workstations. The SMS client provides a Graphical User Interface (GUI) enabling administrators to configure and manage the SMS and the TippingPoint devices installed on the network.

### 1.4.2 Logical Boundaries

7 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

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

8 **Security Audit:** The TOE is able to generate audit records of security-relevant events that occur on the TOE. Each generated audit record includes the following information: date and time of the event; identity of the subject that caused the event (username if the event resulted from the action of an identified user); description of the event; and its outcome. Audit records are stored within the MariaDB database on the SMS Server and are protected from unauthorised modification and deletion. The TOE restricts access to the audit trail to users in the superuser role, who are able to view all the records in the audit trail and to select audit records for display at the SMS Client GUI and sort the displayed records based on date/time, user name, host name, description, or result.

9 **Identification & Authentication:** Users must be identified and authenticated to the TOE prior to gaining access to the functions provided by the TOE, regardless of the access method being used (i.e., SMS client or CLI). The TOE supports five types of user authentication: local; RADIUS; Active Directory; TACACS+; and CAC. The TOE can be configured to lock a user account after a number (configurable by the administrator) of consecutive failed authentication attempts. The TOE can be configured to enforce a password policy that specifies a minimum length for passwords and requirements for the composition of passwords and to re-authenticate the user after a configurable period of time. During the authentication process, the TOE provides only obfuscated feedback to the user.

10 **Security Management:** The TOE provides the capabilities necessary for administrators to manage the TOE security functionality. The TOE provides three predefined security management roles: superuser; admin; and operator. The superuser role has full capabilities to manage the TOE's security functionality, and specific capabilities are restricted to the superuser role.

11 **Protection of the TSF:** The SMS Server can be configured to obtain its date and time from a network-based Network Time Protocol (NTP) server, or the administrator can set the date and time manually. The SMS Server can also be configured as an NTP server and the TippingPoint devices it manages can be configured to obtain their date and time from the SMS Server. The administrator can then configure the SMS Server to obtain its time from another NTP Server. The TOE uses TLS to protect communication between the SMS Client and SMS Server.

12 **TOE Access**: The TOE allows the administrator to configure a banner message to be displayed when a user attempts to log in at any of the TOE user interfaces. The administrator can also configure the TOE to display the access history of a user account, including unsuccessful and successful login attempts, when the user successfully logs in to the TOE. The TOE can limit the number of concurrent sessions belonging to a single user to a value configured by the administrator. The default value when this function is enabled is 4 but can subsequently be set

to other values. In the evaluated configuration, an authorised administrator must enable this function. The TOE will terminate interactive sessions after a period of inactivity configurable by an administrator. By default, interactive sessions are terminated after 30 minutes of inactivity. The TOE also allows user-initiated termination of the user's own interactive session by explicitly logging off.

13 **Trusted Path/Channels:** The TOE provides a trusted path for administrators of the TOE to communicate with the SMS Server. The trusted path is implemented using SSH for access to the CLI. Administrators initiate the trusted path to the CLI by establishing an SSH connection using an SSH client (e.g., putty). The TOE uses TLS to provide a trusted channel between the SMS Server and the following trusted IT products: external TippingPoint devices it manages; external RADIUS and Active Directory authentication servers; external syslog server; and Threat Management Center (TMC).

## 1.5 Clarification of Scope

14 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, trained personnel and secure communication in accordance with user guidance that is supplied with the product.

15 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

16 The TOE also provides a web-based interface (the web management console) that enables administrators to install or upgrade SMS client software, monitor the TippingPoint devices installed on the network, and access Threat Insights. However, except for its role in the installation of the SMS Client on a management workstation, the web management console is excluded from the scope of evaluation.

## 1.6 Assumptions

17 This section summarises the assumptions regarding the operational environment and the intended usage of the TOE as described in the Security Target (Ref [6]).

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

19 A.Protect – The TOE software critical to security policy enforcement will be protected from unauthorised physical modification.

## 1.7 Evaluated Configuration

20 As stated in the ST (Ref [6]), there are two (2) main components of the TOE that make up the evaluated configuration, namely the SMS Server and SMS Client.

21 The SMS Server in its evaluated configuration provides the following administrative interfaces:

- SMS Client—a Java-based application for Windows, Linux or Mac workstations. The SMS Client provides a Graphical User Interface (GUI) enabling administrators to configure and manage the SMS and TippingPoint TPS and IPS devices installed on the network.
- SMS Command Line Interface (CLI)—a text-based interface that enables users with superuser rights to log on to and configure the SMS Server.

22 The evaluated configuration requires that all communications between distributed components of the TOE occur over TLS, which provides confidentiality and integrity of transmitted data. The TOE includes a FIPS-compliant mode of operation that can be enabled or disabled based on individual site requirements. Application of this setting is recommended as a best practice but the security functionality claimed by the TOE does not explicitly require this setting to be enabled or disabled. Under the TOE's evaluated configuration, FIPS-complaint mode was disabled.

23 The TOE supports the following components in the operational environment, however they are not required in the evaluated configuration:

- SSH client application to access the SMS Server CLI.
- NTP server to provide time source for SMS Server.
- Syslog server to act as a repository for exported audit records.
- Active Directory, RADIUS or TACACS+ server to support external user identification and authentication.

## 1.8 Delivery Procedures

24 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

25 The delivery procedures should consider, if applicable, issues such as:

- ensuring that the TOE received by the consumer corresponds precisely to the evaluated version of the TOE;
- avoiding or detecting any tampering with the actual version of the TOE;
- preventing submission of a false version of the TOE;
- avoiding unwanted knowledge of distribution of the TOE to the consumer: there might be cases where potential attackers should not know when and how it is delivered;
- avoiding or detecting the TOE being intercepted during delivery; and
- avoiding the TOE being delayed or stopped during distribution.

26 The TOE delivery procedures include two forms:

- TOE Software: SMS virtual appliance (vSMS) images, TippingPoint Operating System (TOS) updates and Digital Vaccine (DV) updates are posted on Trend Micro's Threat Management Center (TMC) website which requires authentication via customer assigned credentials. The vSMS images and TOS encrypted package files are downloaded from the TMC website via a SSL connection. For Digital Vaccine (DV) updates, a MD5 checksum occurs during the installation of the DV. When product updates are released, a release e-mail is sent out to customers to notify them of the update availability.
- TOE Hardware: The Trend Distribution Center uses a private distribution service to distribute the package to the customer. On every TOE chassis, a security label has been affixed to ensure that the chassis is not tampered with. If the unit is opened, then the label is broken, indicating the unit may have been tampered with and all warranties are void.

## 1.9 Documentation

27 It is important that the TOE is used in accordance with the guidance documentation in order to ensure secure usage of the product.

The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product.

- Release Notes, Version 5.1
- URL Reputation Filtering Deployment Guide, June 2018
- Identity Agent Deployment Guide, October 2017
- SMS Command Line Interface (CLI) Reference, June 2018
- SMS H3 – Install Your Security Appliance, May 2017
- SMS H3 XL – Install Your Security Appliance, May 2017
- SMS User Guide, July 2018
- SMS Web API Guide, July 2018
- vSMS Getting Started Guide, July 2018
- SMS Responder User Guide, June 2018

# 2 Evaluation

28 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the ISCB Product Certification Schemes Policy (PRODUCT_SP) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

## 2.1 Evaluation Analysis Activities

29 The evaluation activities involved a structured evaluation of the TOE, including the following components:

- The evaluators testing consisted of independent testing efforts, which comprise both functional and penetration test cases to address testing requirements for the ATE_IND.2 and AVA_VAN.2 evaluation components.
- The testing approach for both testing was commensurate with the respective assurance components (ATE_IND.2 and AVA_VAN.2). For functional testing the focus was on testing the claimed security functionality (SFRs within the ST) through the interfaces specified in the functional specification (TSFI). For the penetration testing, the effort was limited to those attacks that are commensurate to an attacker with equal or less than Basic attack potential.

### 2.1.1 Life-cycle support

#### 2.1.1.1 Configuration Management Capability

30 The evaluators confirmed that the TOE provided for evaluation is labelled with its reference.

31 The evaluators confirmed that the TOE references used are consistent.

32 The evaluators examined the method of identifying configuration items and determined that it describes how configuration items are uniquely identified.

33 The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the CM documentation.

#### 2.1.1.2 Configuration Management Scope

34 The evaluators confirmed that the configuration list includes the following set of items:

- the TOE itself;
- the parts that comprise the TOE; and
- the evaluation evidence required by the SARs in the ST.

35 The evaluators confirmed that the configuration list uniquely identifies each configuration item.

36 The evaluators confirmed that the configuration list indicates the developer of each TSF relevant configuration item.

#### 2.1.1.3 TOE Delivery

37 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

### 2.1.2 Development

#### 2.1.2.1 Architecture

38 The evaluators examined the security architecture description and determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

39 The security architecture description describes the security domains maintained by the TSF.

40 The initialisation process described in the security architecture description preserves security.

41 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

#### 2.1.2.2 Functional Specification

42 The evaluators examined the functional specification and determined that:

- the TSF is fully represented,
- it states the purpose of each TSF Interface (TSFI),
- the method of use for each TSFI is given,

43 The evaluators also examined the presentation of the TSFI and determined that:

- it completely identifies all parameters associated with every TSFI,
- it completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI,

44 The evaluators also confirmed that the developer supplied tracing that links the SFRs to the corresponding TSFIs.

#### 2.1.2.3 TOE Design Specification

45 The evaluators examined the TOE design and determined that the structure of the entire TOE is described in terms of subsystems. The evaluators also determined that all subsystems of the TSF are identified. The evaluators determined that interactions between the subsystems of the TSF were described.

46 The evaluators examined the TOE and determined that each SFR-non interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is SFR-non interfering.

47 The evaluators found the TOE design to be a complete, accurate and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

48 The evaluators examined the TOE design and determined that it provided a complete and accurate high-level description of the SFR-supporting and SFR-non interfering behaviour of the

SFR-enforcing subsystems. The evaluators determined that the TOE design provided a complete and accurate high-level description of the behaviour of the SFR-supporting subsystems.

49 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification of the subsystems of the TSF described in the TOE design.

50 The evaluators determined that all SFRs were covered by the TOE design and concluded that the TOE design was an accurate instantiation of all SFRs.

### 2.1.3 Guidance documents

#### 2.1.3.1 Operational Guidance

51 The evaluators examined the operational user guidance and determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

52 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

53 The evaluators examined the operational user guidance (in conjunction with other evaluation evidence and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

54 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

55 The evaluators found that the operational user guidance is clear and reasonable.

#### 2.1.3.2 Preparation Guidance

56 The evaluators examined the provided delivery acceptance documentation and determined that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

57 The evaluators determined that the provided installation procedures describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.

58 The evaluators performed all user procedures necessary to prepare the TOE during testing and determined that the TOE and its operational environment can be prepared securely using only the supplied preparative user guidance.

### 2.1.4 IT Product Testing

59 Testing at EAL2 consists of assessing developer tests, performing independent functional tests, and conducting penetration tests. The TOE testing was conducted by the evaluators of BAE

Systems Applied Intelligence MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

#### 2.1.4.1 Assessment of Developer Tests

60 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

#### 2.1.4.2 Independent Functional Testing

61 At EAL2, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan and creating test cases that are independent of the developer's tests.

62 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

| Test ID | Description | SFRs |
|---|---|---|
| TEST-IND-001-CLIENT | • To test the TOE identification and authentication process and security roles.<br>• To test that only authorised users are able to configure and perform TOE security management functions.<br>• To test that the TSF shall allow user-initiated termination of interactive sessions.<br>• To test whether the TSF is able to generate audit records, provide reliable time stamps and allow authorised personnel to configure audit settings and review audit records.<br>• To test that the TSF shall protect/prevent the stored audit records from unauthorised deletion and unauthorised modification. | FAU_GEN.1.1,<br>FAU_GEN.1.2,<br>FAU_GEN.2.1,<br>FAU_SAR.1.1,<br>FAU_SAR.1.2,<br>FAU_SAR.2.1,<br>FAU_SAR.3.1,<br>FAU_STG.1.1,<br>FAU_STG.1.2,<br>FIA_ATD.1.1,<br>FIA_SOS.1.1,<br>FIA_UAU.2.1,<br>FIA_UAU.5.1,<br>FIA_UAU.5.2,<br>FIA_UAU.7.1,<br>FIA_UID.2.1,<br>FMT_MOF.1.1(2),<br>FMT_MOF.1.1(3),<br>FMT_MTD.1.1(1),<br>FMT_MTD.1.1(4),<br>FMT_MTD.1.1(5),<br>FMT_MTD.1.1(6),<br>FMT_SMF.1.1,<br>FMT_SMR.1.1,<br>FMT_SMR.1.2,<br>FPT_STM.1.1,<br>FTA_SSL.4.1 |

| Test ID | Description | SFRs |
|---|---|---|
| TEST-IND-002-CLIENT | • To test the TOE identification and authentication process, security management function behaviours, security roles, and audit data generation.<br>• To test whether TSF data is protected from disclosure or modification when it is transmitted between separate parts of the TOE.<br>• To test the TOE authentication failure handling functions which should disable a user account after a configured amount of invalid logins and terminate an inactive user session after a configured amount of time.<br>• To test whether the TOE displays an advisory warning before establishing a user session and displays the date, time and location of a user's last successful/unsuccessful session establishment upon login. | FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FIA_AFL.1.1, FIA_AFL.1.2, FIA_ATD.1.1, FIA_SOS.1.1, FIA_UAU.2.1, FIA_UAU.7.1, FIA_UID.2.1, FMT_SMR.1.1, FMT_SMR.1.2, FPT_ITT.1.1, FPT_STM.1.1, FTA_SSL.3.1, FTA_TAB.1.1, FTA_TAH.1.1, FTA_TAH.1.2, FTA_TAH.1.3 |
| TEST-IND-003-CLIENT | • To test the TOE identification and authentication process, security management function behaviours, security roles, and audit data generation.<br>• To test different authentication mechanism provided by the TOE.<br>• To test the TSF management functions related to devices, responder policies, responder actions, profiles and event queries. | FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FIA_ATD.1.1, FIA_SOS.1.1, FIA_UAU.2.1, FIA_UAU.5.1, FIA_UAU.5.2, FIA_UAU.7.1, FIA_UID.2.1, FMT_MOF.1.1(1), FMT_MTD.1.1(2), FMT_MTD.1.1(3), FMT_MTD.1.1(4), FMT_MTD.1.1(5), FMT_SMF.1.1, FMT_SMR.1.1, FMT_SMR.1.2, FPT_STM.1.1 |
| TEST-IND-004-CLI | • To test the TOE identification and authentication process, security management function behaviours, security roles, and audit data generation.<br>• To test whether the TSF provides a trusted communication path between itself and remote users.<br>• To test whether the TSF is able to generate audit records, provide reliable time stamps | FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FIA_AFL.1.1, FIA_AFL.1.2, FIA_ATD.1.1, FIA_SOS.1.1, FIA_UAU.2.1, FIA_UAU.5.1, FIA_UAU.5.2, |

| Test ID | Description | SFRs |
|---|---|---|
| | and allow authorised personnel to review audit records.<br>• To test whether the TOE is able to limit the number of concurrent sessions of a user.<br>• To test the TOE authentication failure handling functions which should terminate an inactive user session after a configured amount of time.<br>To test whether the TOE displays an advisory warning before establishing a user session and displays the date, time and location of a user's last successful/unsuccessful session establishment upon login. | FIA_UAU.7.1, FIA_UID.2.1, FMT_MOF.1.1(3), FMT_MTD.1.1(6), FMT_SMF.1.1, FMT_SMR.1.1, FMT_SMR.1.2, FPT_STM.1.1, FTA_MCS.1.1, FTA_MCS.1.2, FTA_SSL.3.1, FTA_SSL.4.1, FTA_TAB.1.1, FTA_TAH.1.1, FTA_TAH.1.2, FTA_TAH.1.3, FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3 |

63 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

#### 2.1.4.3 Penetration Testing

64 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, and TOE design and security architecture description.

65 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialist expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation.

66 The penetration tests focused on:

a) Unnecessary Open Ports

b) Input Validation

c) Broken Authentication Attack

d) Broken Access Control

e) Insecure Communication

67 The results of the penetration testing demonstrate that the TOE is resistant to an attacker possessing a basic attack potential. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref [6]).

#### 2.1.4.4 Testing Results

68 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target (Ref [6]) and its functional specification. In addition, the documentation supplied as evidence for the EAL2 Common Criteria evaluation of the TOE was analysed to identify possible vulnerabilities.

# 3 Result of the Evaluation

69 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of Trend Micro TippingPoint Security Management System (SMS) v5.1.0 performed by BAE Systems Applied Intelligence MySEF.

70 BAE Systems Applied Intelligence MySEF found that Trend Micro TippingPoint Security Management System v5.1.0 upholds the claims made in the Security Target (Ref [6]) and supporting documentation and has met the requirements of the Common Criteria (CC) assurance Level 2 (EAL2).

71 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

## 3.1 Assurance Level Information

72 EAL 2 provides assurance by a full Security Target and analysis of the SFRs in that Security Target (Ref [6]), using functional and interface specifications, guidance documentation and a basic description of the design and architecture of the TOE, to understand the security behaviours of the TOE.

73 The analysis is supported by an independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to an attacker possessing a Basic attack potential.

74 EAL 2 also provides assurance through use of a configuration management system and, evidence of secure delivery procedures.

## 3.2 Recommendation

75 The following recommendations are made:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

b) Potential purchasers of the TOE should ensure that the administrators responsible for the TOE are provided sufficient training and are familiar with the guidance supplements prior to configuring and administering the TOE.

# Annex A References

## A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] ISCB Product Certification Schemes Policy (PRODUCT_SP), v1a, CyberSecurity Malaysia, June 2017.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v1, June 2017.

[6] Trend Micro TippingPoint Security Management System Security Target, Version 1.0, 21 August 2018

[7] EAU000426.07-S046-ETR, Evaluation Technical Report, Version 1.0, 10 September 2018

## A.2 Terminology

### A.2.1 Acronyms

Table 2: List of Acronyms

| Acronym | Expanded Term |
|---|---|
| CB | Certification Body |
| CC | Common Criteria (ISO/IEC15408) |
| CEM | Common Evaluation Methodology (ISO/IEC 18045) |
| CLI | Command Line Interface |
| CCRA | Common Criteria Recognition Arrangement |
| DV | Digital Vaccine |
| IPS | Intrusion Prevention System |
| ISO | International Organisation for Standardization |
| ISCB | Information Security Certification Body |
| MyCB | Malaysian Common Criteria Certification Body |
| MyCC | Malaysian Common Criteria Evaluation and Certification Scheme |
| MyCPR | MyCC Scheme Certified Products Register |

| Acronym | Expanded Term |
|---|---|
| MySEF | Malaysian Security Evaluation Facility |
| NTP | Network Time Protocol |
| SMS | Security Management System |
| SSH | Secure Shell |
| ST | Security Target |
| TMC | Threat Management Center |
| TOE | Target of Evaluation |
| TOS | TippingPoint Operating System |
| TPS | Threat Protection System |
| TSF | TOE Security Functionality |
| TSFI | TOE Security Functionality Interface |

### A.2.2 Glossary of Terms

Table 3: Glossary of Terms

| Term | Definition and Source |
|---|---|
| CC International Interpretation | An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants. |
| Certificate | The official representation from the CB of the certification of a specific version of a product to the Common Criteria. |
| Certification Body | An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA |
| Consumer | The organisation that uses the certified product within their infrastructure. |
| Developer | The organisation that develops the product submitted for CC evaluation and certification. |
| Evaluation | The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65 |
| Evaluation and Certification Scheme | The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA. |

| Term | Definition and Source |
|---|---|
| Interpretation | Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**. |
| Certifier | The certifier responsible for managing a specific certification task. |
| Evaluator | The evaluator responsible for managing the technical aspects of a specific evaluation task. |
| Maintenance Certificate | The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme. |
| National Interpretation | An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only. |
| Security Evaluation Facility | An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy |
| Sponsor | The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer. |

--- END OF DOCUMENT ---