MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

C133 Certification Report

Trend Micro TippingPoint Security Management System (SMS) v6.2.0

File name: ISCB-5-RPT-C133-CR-v1
Version: v1
Date of document: 24 April 2024
Document classification : PUBLIC

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

C133 Certification Report

Trend Micro TippingPoint Security Management System (SMS) v6.2.0

24 April 2024

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C133 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C133-CR-v1
ISSUE:	v1
DATE:	24 April 2024
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

The copyright of this document, which may contain proprietary information, is the property of CyberSecurity Malaysia.

The document shall be held in safe custody.

©CYBERSECURITY MALAYSIA, 2024

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 201601006881 (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, 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 3rd May 2024, 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).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme 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	4 April 2024	All	Initial draft
v1	24 April 2024	All	Final Version

Executive Summary

The Target of Evaluation (TOE) is the Trend Micro TippingPoint Security Management System (SMS) v6.2.0 (herein after refer as TOE). TOE is a server-based solution that can act as the control center for managing large-scale deployments of TippingPoint Threat Protection System (TPS) and Intrusion Prevention System (IPS) products. It is also able to communicate threat data with TippingPoint Deep Discovery products. A single SMS can manage multiple TippingPoint devices—the maximum number depends on usage, network, and other environmental conditions.

The TOE provides security functions such as security audit, Identification and authentication, security management, protection of the TSF, TOE access and trusted path/channels.

The scope of the evaluation is defined by the Security Target (Ref [6]) which identifies 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 (EAL 2). 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 Securelytics SEF and the evaluation was completed on 20 March 2024.

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) v6.2.0 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 available as a rack-mountable hardware appliance or as a software-based product (vSMS) that operates in a virtual environment.

2 The core functionality provided by the TOE is the ability to create multiple filter profiles that are distributed to specific devices. Devices can be organized into groups or security zones to facilitate distribution and updating of security profiles, rather than doing this individually for each device.

3 The TOE provides centralized control for managing large-scale deployments of the following TippingPoint products:

- TippingPoint NX Series Next-Generation Intrusion Prevention System (IPS)—uses a combination of technologies, including deep packet inspection, threat reputation, and advanced malware analysis, on a flow-by-flow basis to detect and prevent attacks on the network.
- TippingPoint Threat Protection System (TPS)—a network security platform that offers comprehensive threat protection, shielding network vulnerabilities, blocking exploits, and defending against known and zero-day attacks.

4 The TOE also provides capabilities for communicating threat data with TippingPoint Deep Discovery (DD) devices. TippingPoint DD is a threat protection platform providing capabilities to detect, analyze and respond to network-based attacks. The platform includes the following products: The key features of the TOE are listed as below:

- DD Inspector—a network appliance that monitors all ports and over 100 different network protocols to discover advanced threats and targeted attacks
- DD Email Inspector—stops targeted ransomware attacks by blocking targeted spear phishing emails before they are delivered
- DD Analyzer—provides customized sandboxing for existing security solutions, including endpoint protection, web gateways, firewalls, and IPS products.

5 The SMS Client GUI provides the following work spaces that support the management of TippingPoint TPS and IPS deployments:

- Devices—the Devices workspace provides a dynamic view of the entire system, graphically depicting TippingPoint TPS and IPS devices currently under SMS

management, their segments, and the host and services on those segments. Through this workspace, an administrator can monitor and manage all the TippingPoint TPS and IPS devices in the deployment. Device management includes such activities as adding devices to the SMS system, combining devices into related groups, changing device or network configurations, installing TOS updates, temporarily unmanaging a device, replacing a device, or deleting a device from the deployment. When an administrator assumes management of a device, the administrator can control networking configuration, virtual segments and segment groups, filters and customizations, and distribution of filters and software. The administrator can also monitor traffic processing, health, and hardware status on each device and its segments.

- Profiles—a profile is a collection of filters or rules that provides a method for setting up security configuration options for TippingPoint solutions. The TOE ships with a default profile, along with a standard Digital Vaccine with filters that address known security issues. TippingPoint provides regular updates to the Digital Vaccine along with other tools and services to monitor and respond to security threats to the network. The Profiles workspace provides capabilities to create, view, modify, distribute and delete profiles.
- Responder—responder features provide security mitigation to block infected or malicious traffic, inform the administrator of possible threats, and place the host into remediation. Responder policies monitor all traffic according to devices, and use filters to enact another layer of protection. Filters include action sets with options to automatically redirect users and halt trigger traffic flows. The Responder workspace provides a centralized environment for managing security response actions, policies, switches, and response history.
- Events—as the TOE responds to traffic triggered by the filters defined in profiles, data is logged in the SMS database. The Events workspace provides capabilities to filter, view, and save events for all or specific devices, segment groups, and event filter elements. The administrator can save, run, and manage queries through the Events workspace. Saved queries display in the Saved Queries sections in the navigation screen.
- Reports—as the TOE detects malicious attacks and manages network usage, event data is logged in the database. This information details the system's behavior as it responds to network traffic. The TOE provides a set of options to generate reports about the compiled and stored log information. The

administrator can use reports in the TOE to generate up-to-the-moment data analysis to help in measuring network data. The Reports workspace enables the administrator to customize existing reports or build them from scratch.

- Admin—the Admin workspace enables the administrator to manage user access, system and audit logs, and system settings. Options available through the Admin workspace are limited to users with the appropriate role and access level.

1.2 TOE Identification

6 The details of the TOE are identified in table below.

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C133
TOE Name	Trend Micro TippingPoint Security Management System (SMS)
TOE Version	v6.2.0
Security Target Title	Trend Micro TippingPoint Security Management System (SMS) v6.2.0 Security Target
Security Target Version	v1.0
Security Target Date	15 March 2024
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 Methodology 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 CC Part 3 Conformant Package conformant to EAL 2
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive, Columbia, Maryland 21046, The United States of America

Developer	Trend Micro Incorporated 11305 Alterra Parkway, Austin, Texas 78758 USA
Evaluation Facility	Securelytics SEF A-19-06, Tower A, Atria SOFO Suites, Petaling Jaya, Selangor Darul Ehsan

Table 1: TOE Identification

1.3 Security Policy

7 No Organisational Security Policy (OSP) declared for the TOE.

1.4 TOE Architecture

8 The TOE consist of logical and physical boundaries which are described in Section 2.3 and 2.4 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

9 The logical boundary of the TOE is summarized below:

- **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 unauthorized 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

- **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.

- **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.

- **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.

- **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 authorized administrator must enable this function.

  The administrator can configure the TOE to terminate interactive sessions after a period of inactivity. By default, interactive sessions are terminated after 30 minutes of inactivity. The administrator can also configure the TOE to lock interactive SMS

client sessions after a period of inactivity. The TOE also allows user-initiated termination of the user's own interactive session by explicitly logging off.

- **Trusted Path/Channel**

  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; Threat Management Center (TMC).

1.4.2 Physical Boundaries

10 The TOE comprises the SMS Server and the SMS Client. The SMS Server is provisioned as an appliance-based solution and also as a virtual appliance, while the SMS Client is a Java-based application that is downloaded from the SMS Server (regardless whether the deployed SMS Server is a hardware or virtual appliance). Physically, the SMS Server is available in four hardware form-factors: SMS H3 appliance; SMS H3 XL appliance; SMS H4 appliance; and SMS H4 XL appliance. The following table summarizes each appliance.

Model	SMS H3	SMS H3 XL	SMS H4	SMS H4 XL
Capacity	Up to 200 million historical events	Up to 600 million historical events Provides additional processing and storage recommended for deployments larger than 150 devices.	Up to 200 million historical events	Up to 600 million historical events Recommended for deployments larger than 150 devices
Form factor	1U Rack-mount (19 in)	2U Rack-mount (19 in)	1U Rack-mount (19 in)	1U Rack-mount (19 in)
Management ports	2 x 10/100/1000 BASE-T RJ45	2 x 10/100/1000 BASE-T RJ45	2 x 10/100/1000 BASE-T RJ45	2 x 10/100/1000 BASE-T RJ45

Hard drives	2 x 600GB 6G SAS 10krpm 2.5 in	6 x 600GB 6G SAS 10krpm 2.5 in	2 x 800GB SSD, SAS 12 Gbps	6 x 800GB SSD, SAS 12 Gbps
RAID configuration	RAID 1	RAID 1+0	RAID 1	RAID 1+0

Table 2: TOE Hardware Specification

11 The Virtual Security Management System (vSMS) virtual appliance is a software-based

SMS appliance that operates within a virtual environment. The vSMS platform supports management of an unlimited number (of any model) of TippingPoint devices. With few exceptions, the vSMS platform provides the same functionality, the same user interfaces, and operates the same as a physical SMS appliance. A supported virtual environment must already be installed and configured before vSMS is deployed.

12 The vSMS can be deployed in VMware or KVM virtual environments. The following are the minimum system requirements for the vSMS platform:

- 300 GB virtual disk size. For a larger disk partition, this size can be dynamically increased. A size of 600 GB is recommended. The maximum supported size is 1800 GB.
- 8 virtual CPUs
- 2.27 GHz CPU speed
- 32 GB memory
- 2 virtual network adapters.

Note, two virtual network adapters are required to match a physical SMS. One of the virtual network adapters is for management. The second one is required for High Availability out of band replication, even if replication is not in use.

13 For a VMware deployment, a supported VMware vSphere environment must already be set up before the vSMS can be installed and used. The vSMS platform uses a VMware Open Virtualization Format (OVF) file to operate, and runs on:

- VMware vSphere Client version 6.7, 7.0.2, or 8.0
- VMware ESX/ESXi version 6.7, 7.0.2, or 8.0.

14 For a KVM deployment, a supported KVM environment must already be set up before the vSMS can be installed and used. KVM deployment of vSMS is supported in the following environments:

- RHEL version 6 (for three cores); libvirt version 0.10.2; Quick Emulator (QEMU) version 0.12.0
- RHEL version 7 with the KVM hypervisor (for four cores); libvirt version 1.1.0; QEMU version 1.5.3.

15 The KVM environment must have the following tar packages installed:

- qemu-kvm
- virt-install
- virt-viewer.

16 After the SMS Server (hardware or virtual appliance) has been installed, the SMS Client can be downloaded from the SMS Server and installed onto a physical or virtual workstation running Windows, Linux or Mac OS X.

17 Note that the SMS Server includes a FIPS-compliant mode of operation. 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. Therefore, it is neither required by nor excluded from the TOE's evaluated configuration and can be enabled or disabled based on individual site requirements.

1.5 Clarification of Scope

18 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

19 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]).

20 Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

21 This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand the requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

1.6.1 Operational Environmental assumptions

22 Assumptions for the TOE environment as described in the Security Target (Ref [6]):

Environment	Statement
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.PROTECT	The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

Table 3: Assumptions for the TOE Environment

1.7 Evaluated Configuration

23 This section describes the evaluated configurations of the TOE that are included within the scope of the evaluation.

24 The evaluated configuration of the TOE comprises the following main components:

- SMS Server—provisioned as a rack-mountable appliance or as a virtual server (vSMS)
- SMS Client—a Java-based application for Windows, Linux or Mac workstations.

25 Note that SMS 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, as are its associated HTTP and REST APIs.

26 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.

1.8 Delivery Procedures

27 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.

28 The evaluators also examined the aspects of the delivery process and determined that the delivery procedures are used.

1.8.1 TOE Delivery Procedures

29 Delivery requirements call for system controls and procedures that provide assurance in the delivery of the TOE without any undetected tampering or interference. For a valid delivery, what is received by the end customer must correspond precisely to the TOE master copy, thus avoiding any tampering with the actual version, or substitution of a false version. Several procedures are necessary for TippingPoint to maintain security when distributing versions of the TOE or parts of it to a user's site.

1.8.2 Delivery to Customers

30 Hardware

Once a hardware appliance instance of the TOE is manufactured, it is securely packaged. Packaging tape is used to seal the packages containing the TOE hardware appliance and associated accessory kit. The manufacturing facility (Benchmark Angleton) sends the packaged TOE appliance to Trend's Distribution Center (Panalpina Dallas). The Trend Distribution Center holds the packaged TOE appliances in a secure area before an order is shipped to prevent tampering. When an order for the TOE is received, the Trend Distribution Center uses a private distribution service (e.g., UPS) 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.

31 Software Download and Updates

As part of the delivery process, TOE software updates are posted on the Threat Management Center (TMC) website (https://tmc.tippingpoint.com), whence they can be downloaded by customers over a TLS connection. This site requires authentication via the customer assigned credentials.

Trend Micro generates a digital signature of the package by first calculating the SHA-256 hash of the package, then encrypting the generated hash using its 2048-bit RSA private key. The package includes the digital signature and the public key is included in

the software image. The TOE verifies the digital signature prior to installing the package. The process is as follows: the TOE calculates its own SHA-256 hash of the package, then decrypts the digital signature accompanying the package using the RSA public key matching the vendor's private key and comparing the hash it calculated with the decrypted hash value. If they are equal, the package is valid and has not been modified. The TOE starts the update process once it verifies the signature/hash. A package with an invalid signature will not be installed by the TOE.

When product updates are released, a release e-mail is sent out to customers to notify them of the update availability.

SMS virtual appliance (vSMS) images are made available on TMC. These are downloaded by the customer via an SSL connection. The image itself is signed using Trend Micro certificate. The customers install the image into their own server hardware running supported hypervisors.

1.8.3 Method of Packaging and Shipment

32 Packaging

Trend Micro packages and labels the product in accordance with the current bill of material (BOM) and any applicable package specification for the product to be shipped.

All products are enclosed in cardboard shipping boxes and sealed with tape. A shipping label identifying the exact product (including the serial number for the included device) and the customer name is provided on the outside of the shipping box.

Each hardware device is wrapped in a plastic bag and sealed with a warning label. The device cannot be removed from the plastic bag without damaging either the bag or the label.

33 Shipping

Trend Micro employs its current default carrier to deliver the product to customers. Trend Micro determines the best carrier, routing, and cost for the shipment.

Trend Micro's default carrier is currently UPS. Unless otherwise specified, all items are sent via UPS.

34 Tracking

Packages are tracked via the carrier's tracking numbers. The tracking number allows any party to find the status of the package either by calling the toll-free number or logging into the website. Tracking numbers are only provided to customers upon request.

2 Evaluation

35 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 MyCC Scheme Requirement (MyCC_REQ) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

37 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

38 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.

2.1.2 Development

39 The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).

40 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

41 The evaluators examined the TOE security architecture description; they 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.

42 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.3 Guidance documents

43 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

44 The evaluators confirmed that the TOE guidance has fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

45 Testing at EAL 2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by Securelytics SEF. 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

46 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, 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). The results of the evaluators tests are consistent with the developers test results defined in their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

47 At EAL 2, 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.

48 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	Security Function	Results
F001 – Identification and Authentication	1. To test that the TOE requires user to be successfully identified and authenticated before allowing any TSF-mediated actions on behalf of that user. 2. To test that the TSF's ability to detect and lock user when unsuccessful authentication attempts occur attempting to authenticate remotely using a password. 3. To test the TSF's ability to provide the password management capabilities meet requirements. 4. To test the TSF's ability to provide only obscured feedback to the administrative user while the authentication is in progress at the local console. 5. To test the TSF's ability to provides local password-based, remote authentication using RADIUS, remote authentication using Active Directory, remote authentication using TACACS+, Common Access Card (CAC) for administrative user authentication. 6. To test the TSF's ability to maintain list of attributes belonging to users.	FIA_AFL.1 FIA_ATD.1 FIA_SOS.1 FIA_UAU.2 FIA_UAU.5 FIA_UAU.6 FIA_UAU.7 FIA_UID.2	Passed

Test ID	Description	Security Function	Results
	7. To test the TSF's ability to provides mechanism for secrets verification. 8. To test the TSF's ability to reauthenticate due to inactivity for a configurable period of time.		
F002 – Security Audit	1. To test that the TOE able to generate the auditable records meets the FAU_GEN.1.1. 2. To test that the TOE restrict the ability to read the audit records. 3. To test that the TOE provide the ability to perform filtering to the audit records. 4. To test that the TOE capable of performing the management function meets FMT_SMF.1.1 5. To test that the TOE able to protect the audit records from unauthorised user.	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_SAR.2 FAU_SAR.3 FAU_STG.1	Passed.
F003 – Security Management	1. To test that the TOE able to performing management functions meets the FMT_MOF.1.1 (1), FMT_MOF.1.1 (2), FMT_MOF.1.1 (3). 2. To test that the TOE restrict the ability to modify, delete, add, create, manage and unmanage the device. 3. To test that the TOE restrict the ability to add responder device to Superuser 4. To test that the TOE restrict the ability to modify, query, delete, create and distribute the profiles to Superuser.	FMT_MOF.1(1) FMT_MOF.1(2) FMT_MOF.1(3) FMT_MTD.1(1) FMT_MTD.1(2) FMT_MTD.1(3) FMT_MTD.1(4) FMT_MTD.1(5) FMT_MTD.1(6) FMT_SMF.1 FMT_SMR.1	Passed.

Test ID	Description	Security Function	Results
	5. To test that the TOE restrict the ability meets the FMT_MTD.1.1(4), FMT_MTD.1.1(5) and FMT_MTD.1.1(6), FMT_SMF.1.1 and FMT_SMR.1		
F004 – Protection of TSF	1. To test that the TSF able to protect TSF data from disclosure and modification when the data transmitted between separate parts of the TOE. 2. To test that the TSF able to provide reliable time stamps.	FPT_ITT.1 FPT_STM.1	Passed.
F005 – TOE Access	1. To test that the TSF restrict the restrict the minimum number of concurrent sessions. 2. To test that the TSF shall lock and terminate an interactive SMS client session after an administrator-configurable period of inactivity. 3. To test that the TSF able to display the warning messages before establishing user session. 4. To test that the TOE able to display date, time and location of the last successful and unsuccessful attempt sessions.	FTA_MCS.1 FTA_SSL.3 FTA_SSL.1 FTA_SSL.4 FTA_TAB.1 FTA_TAH.1	Passed.
F006 – Trusted Path	1. To test that the TSF able to provide trusted communication path between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the	FTP_ITC.1 FTP_TRP.1	Passed.

Test ID	Description	Security Function	Results
	communicated data from modification or disclosure. 2. To test that the TSF able to initiate communication via the trusted channel for [communication with managed devices, remote RADIUS or Active Directory authentication requests, export of syslog records, communication with TMC		

Table 4: Independent Functional Test

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

2.1.4.3 Vulnerability Analysis

50 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, TOE design, and security architecture description.

51 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack 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 (specialised 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

2.1.4.4 Vulnerability testing

52 The penetration tests focused on:

a) TOE Connectivity Check

b) Traceroute IP

c) Port Scanning

d) Banner Grabbing

e) Nessus Scanning

f) Firewalk Scanning

g) Denial of Service

h) TCP SYN Flood Attack

i) ICMP Smurf Attack

j) SSH Port Brute force Attack

k) Search Vulnerability in Public Vulnerabilities repositories

l) Information Leakage via unencrypted network traffic

m) Binary Manipulation

n) Manual Review of config files

o) Information leakage via registry

p) Data Dump for sensitive information leakage

q) Improper error Handling

r) SQL Injection

s) DLL Hijacking

t) SSH port brute force attack (CLI)

53 The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment as specified in the Security Target (Ref [6]).

2.1.4.5 Testing Results

54 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all the test conducted were **PASSED** as expected.

3 Result of the Evaluation

55 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) v6.2.0 which is performed by Securelytics SEF.

56 Securelytics SEF found that Trend Micro TippingPoint Security Management System (SMS) v6.2.0 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2.

57 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

58 EAL 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and interface specifications, guidance documentation and a description of the design of the TOE and the implementation to understand the security behaviours.

59 The analysis is supported by 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 penetration attackers with a basic attack potential.

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

3.2 Recommendation

61 The Malaysian Certification Body (MyCB) is strongly recommended that:

a) The users should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

b) The users must maintain the confidentiality, integrity, and availability of security relevant data for TOE initialization, start-up and operation if stored or handled outside the TOE.

c) System Auditor should review the audit trail generated and exported by the TOE periodically.

d) The users must ensure appropriate network protection is maintained, the network on which the TOE is installed must be both physically and logically protected.

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 Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] MyCC Scheme Requirement (MYCC_REQ), v1b, July 2023.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v3, January 2023.

[6] Trend Micro TippingPoint Security Management System (SMS) v6.2.0 Security Target, v1.0, 15th March 2024.

[7] Evaluation Technical Report, Version 1.0, 02 April 2024.

A.2 Terminology

A.2.1 Acronyms

Table 5: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body

Acronym	Expanded Term
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 6: 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

Term	Definition and Source
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.
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 ---