MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

M023 Assurance Maintenance Report Trend Micro TippingPoint Security Management System v6.5.0

File name: ISCB-5-RPT-M023-AMR-v1
Version: v1
Date of document: 3 April 2026
Document classification: PUBLIC

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

M023 Assurance Maintenance Report

Trend Micro TippingPoint Security Management System v6.5.0

3 April 2026

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:	M023 Assurance Maintenance Report
DOCUMENT REFERENCE:	ISCB-5-RPT-M023-AMR-v1
ISSUE:	v1
DATE:	3 April 2026
DISTRIBUTION:	CONTROLLED COPY - FOR LIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1,
Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor, Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 200601006881 (726630-U)

Printed in Malaysia

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	31 March 2026	All	Initial draft
v1	3 April 2026	All	Final version

Table of Contents

1 Introduction

1 The TOE is Trend Micro TippingPoint Security Management System (SMS), v6.5.0. The 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.

2 The TOE is available as a rack-mountable hardware appliance or as a software-based product (vSMS) that operates in a virtual environment.

3 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. Administrators can also use the TOE to keep managed devices updated with the latest TippingPoint Operating System (TOS) software and Digital Vaccine (DV) packages.

4 The main components of the TOE are:

- 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.

5 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.

6 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:

- 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.

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

8 MyCB has assessed the Impact Analysis Report (Ref [1]) according to the requirements outlined in the document Assurance Continuity: CCRA Requirements (Ref [4])

9 This is supported by the evaluator's verification test plan report (Ref [10]).

10 The purpose of this document is to enable developers to provide assured products to the IT consumer community in a timely and efficient manner against the certified and updated version of the TOE as in Table 1 identification below.

Table 1 – Identification Information

Assurance Maintenance Identifier	M023
Project Identifier	C133
Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Impact Analysis Report	Trend Micro TippingPoint Security Management System (SMS) v6.5.0 Impact Analysis Report (IAR), Version 1.1 27 March 2026
New TOE	Trend Micro TippingPoint Security Management System (SMS) v6.5.0
Certified TOE	Trend Micro TippingPoint Security Management System (SMS) v6.2.0
New Security Target	Trend Micro TippingPoint Security Management System (SMS) v6.4.0 Security Target, Version 1.3 22 December 2025
Evaluation Level	EAL2
Evaluation Technical Report (ETR)	Evaluation Technical Report – TippingPoint Security Management System (SMS) v6.2.0, V1.0, 02 April 2024
Criteria	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, April 2017, Revision 5, Version 3.1 Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, April 2017, Revision 5, Version 3.1 Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, April 2017, Revision 5, Version 3.1 Assurance Continuity: CCRA Requirements version 3.1, 29 February 2024

Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, April 2017, Revision 5, Version 3.1
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL2
Protection Profile Conformance	None
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive Columbia, MD 21046, USA
Developer	Trend Micro Inc 11305 Alterra Parkway, Austin, Texas 78758, USA
Evaluation Facility	Securelytics SEF A-17-01, Tower A, ATRIA SOFO Suites, Jalan SS 22/23, Damansara Utama, 47400 Petaling Jaya Selangor, Malaysia.

2 Description of Changes

11 Trend Micro has issued a new release which is Trend Micro TippingPoint Security Management System (SMS) v6.5.0. There were a series of minor updates to the Trend Micro TippingPoint Security Management System (SMS) since its certification version 6.2.0 on 03 May 2024 and Assurance Maintenance for Trend Micro TippingPoint Security Management System (SMS) v6.4.0 on 17 June 2025 (Ref[11].

2.1 Changes to the product associated with the certified TOE

12 The following features have been added in Trend Micro TippingPoint Security Management System (SMS) v6.5.0. The details changes have been documented in the Impact Analysis Report (IAR).

Table 2 – General changes/additions

Version	Description of Changes	Rationale	Impact
Trend Micro TippingPoint Security Management System (SMS) v6.5.0	[New Feature] The TOE version has been updated to v6.5.0. The vSMS is now supported on the Microsoft Hyper-V platform for Microsoft Windows Server 2022 and Microsoft Windows Server 2025.	The updates do not affect the Security Functional Requirements (SFR) of the TOE. The Microsoft Hyper-V platform serves as a supporting platform on which the TOE is provisioned, and as such, changes to the underlying platform do not impact the TOE's security functionality or its compliance with the defined SFRs.	Certification Body consider it as **Minor**
	[New Feature] The TOE version has been updated to v6.5.0. This release expands SMS management support to include the new TPS 5600TXE model.	The updates do not affect the Security Functional Requirements (SFR) of the TOE. FMT_MTD.1 grants the TOE the capability to manage both TPS and IPS devices. Therefore, the introduction of the new TPS 5600TXE model does not affect	Certification Body consider it as **Minor**

Version	Description of Changes	Rationale	Impact
		the TOE's security functionality or its compliance with the specified SFR	
	[New Feature] The TOE version has been updated to v6.5.0. A Certificate Expiration Summary page has been added to Admin > Certificate Management. You can view up-to-the minute counts of your certificates that have expired or are about to expire and configure the frequency of the notifications you receive.	The updates do not affect the Security Functional Requirements (SFR) of the TOE. The Certificate Expiration Summary page is a minor graphical user interface enhancement that displays an overview of upcoming certification expirations.	Certification Body consider it as **Minor**
	[New Feature] The TOE version has been updated to v6.5.0. This release expands application layer protocol capabilities for sharing threat intelligence by embedding a TAXII 2.1 server, in addition to a TAXII 2.0 server, in the SMS.	The updates do not affect the Security Functional Requirements (SFR) of the TOE as it has been reflected to be out-of-scope.	Certification Body consider it as **Minor**
	[New Feature] The TOE version has been updated to v6.5.0. This release updates the implementation of the Certificate Revocation List (CRL) to use the SMS proxy.	The updates do not affect the Security Functional Requirements (SFR) of the TOE as it has been reflected to be out-of-scope.	Certification Body consider it as **Minor**
	[New Feature] The TOE version has been updated to v6.5.0. This release expands the File Reputation feature by enabling SMS to process File Hashes from Deep Discovery Analyzer (DDAN).	The updates do not affect the Security Functional Requirements (SFR) of the TOE as it has been reflected to be out-of-scope.	Certification Body consider it as **Minor**

Version	Description of Changes	Rationale	Impact
	[New Feature] The TOE version has been updated to v6.5.0. The SMS now sends notifications and administrator emails when the SMS is not able to update package file versions or download package files from TMC for any reason. This happens for both automatic and user-initiated package requests, and includes Digital Vaccines, Threat DV IP/Domain Reputation, Threat DV URL Feed, Auxiliary DV. Capacity License, Entitlement, FIPS Keys, Geo Locator DB, and SMS & TOS software packages.	The updates do not affect the Security Functional Requirements (SFR) of the TOE. The SMS now alerts administrators via notifications and emails if it cannot update or download package files from TMC.	Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. Backup restorations from unsupported releases are no longer supported. Only backups from supported SMS versions from SMS v5.5.4.205331 and newer can be restored.	The updates are limited to bug fixes from the prior functional release and do not affect the Security Functional Requirements (SFR) of the TOE.	Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. When you edit a stack name using the SMS client's Edit button, configuring resilience and SRD values now works as expected.	The updates are limited to bug fixes from the prior functional release and do not affect the Security Functional Requirements (SFR) of the TOE.	Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. This release contains security updates, including a kernel update for CVE-2024-	The updates are limited to bug fixes from the prior functional release and do not affect the Security Functional	Certification Body consider it as **Minor**

Version	Description of Changes	Rationale	Impact
	43856.	Requirements (SFR) of the TOE.	
	[Bug Fix] The TOE version has been updated to v6.5.0. This release fixes an issue that caused Named IP Address Group to be duplicated when the profile was distributed.	The updates are limited to bug fixes from the prior functional release and do not affect the Security Functional Requirements (SFR) of the TOE.	Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. After an upgrade to v6.4.0, Dell H4 platforms no longer show an amber LED and return the following hardware system error in iDRAC: A fatal error was detected on a component at bus 2 device 0 function 0.	The updates are limited to bug fixes from the prior functional release and do not affect the Security Functional Requirements (SFR) of the TOE.	Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. A table showing the device snapshots for all devices is now available in the Snapshots tab under Devices > All Devices > Member Summary. If the Show All Devices checkbox is selected, users with appropriate permissions can view and export snapshot data for all devices to a file (select Export to File > All Rows from the context menu).	The updates are limited to bug fixes from the prior functional release and do not affect the Security Functional Requirements (SFR) of the TOE.	Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0.	The updates are limited to bug fixes from the prior functional release and do not affect the Security Functional	Certification Body consider it as **Minor**

Version	Description of Changes	Rationale	Impact
	OpenSSH has been upgraded to version 9.9p2 for security fixes and addresses the following vulnerabilities: CVE-2025-26465 and CVE-2025-26466.	Requirements (SFR) of the TOE.	
	[Bug Fix] The TOE version has been updated to v6.5.0. The Access SMS Web Services capability (Edit Role > Capabilities > Admin > Admin Section> SMS Management > Access Management) is no longer required for downloading the client install image, upgrading or patching the client or accessing files from Exports and Archives through the Web UI.	The updates are limited to bug fixes from the prior functional release and do not affect the Security Functional Requirements (SFR) of the TOE.	Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. An issue where some users could not access the SMS client after upgrading to SMS v6.4.0 or later has been fixed.		Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. A startup issue that occurred after expanding the virtual disk on an SMS has been fixed.		Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. This release fixes a problem that caused the SMS to stop pulling Suspicious Objects from Trend Vision One if more than 1000 Suspicious Objects were added between polls.		Certification Body consider it as **Minor**

Version	Description of Changes	Rationale	Impact
	[Bug Fix] The TOE version has been updated to v6.5.0. This release fixes an issue where the passive device of an SMS High Availability (HA) pair would stay connected to Trend Vision One™ when the SMS HA was disabled. Now the passive device disconnects from Trend Vision One™.		Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. The reputation setting to HTTP requests with matching domain names now defaults to false for file distributions.		Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. When the Reputation Entries TTL capability is enabled, three bulk deletion operations are now visible: IP/Domain, URL, and File Hash.		Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. This release added hardware controller support to allow collection of physical disk, logical disk, and RAID controller battery status.		

3 Affected Developer Evidence

13 The affected developer evidence submitted for the assurance continuity required by the CCRA Assurance Continuity: CCRA Requirements Version 3.1 Feb 2024 (Ref [4]) are as below:

Table 3 – Affected Developer Evidence

Evidence Identification	Description of Changes	Rationale	Impact
Security Target: Trend Micro TippingPoint Security Management System v6.5.0 Security Target, v1.3, 22 December 2025.	Changes in the Security Target document are: Front Page - The ST version and date have been updated. · Section 1 & Section 2- TOE reference has been updated to reflect the change in TOE version from the developer. · Section 1.1 - ST Title, ST Version, ST Date and TOE identification has been updated to reflect the change in TOE version from the developer. · Section 2.5 - The TOE documentation has been updated to the latest documents	The changes or updates made do not affect the SFRs or the functionality included in the scope of the previous evaluation.	CB consider it as **Minor**
Design Documentation: Trend Micro TippingPoint Security Management System v6.5.0 Design Documentation, v1.3, 22 December 2025.	Changes in the Design document are: Trend Micro TippingPoint Security Management System v6.4.0 Design Documentation, v1.3, 22 December 2025 The changes are: · Front Page - The Design Documentation version and date have been updated · Section 1 - TOE reference has been updated to	The changes or updates made do not impact the SFRs or the functionality included in the scope of the previous evaluation.	CB consider it as **Minor**

Evidence Identification	Description of Changes	Rationale	Impact
	reflect the change in TOE version from the developer. · Section 5.1 and Section 5.2 – References have been updated to include the latest document version and date		
Configuration Management Documentation: Trend Micro TippingPoint Security Management System Configuration Management Documentation v6.5.0 v1.5, 22 December 2025.	Changes in the Configuration Management document are: · Front Page - The Configuration Management document version and date have been updated. · Section 1 & Section 2 & Section 3 - TOE reference has been updated · Section 3 – TOE Configuration List have been updated to include the updated TOE version and latest document version and date	The changes or updates made do not impact the SFRs or the functionality included in the scope of the previous evaluation.	CB consider it as **Minor**
Delivery Procedures Documentation: Trend Micro TippingPoint Security Management System Delivery Procedures, v1.3, 22 December 2025.	Changes made to the Delivery Procedures are: · Front Page - The Delivery Procedures document version and date have been updated. · Section 1 - TOE reference has been updated	The changes or updates made do not impact the SFRs or the functionality included in the scope of the previous evaluation.	CB consider it as **Minor**
User guidance documentation: Trend Micro TippingPoint Security Management System (SMS) User Guide v6.5.0, August 2025.	Changes made to the User guidance document are: Page ii - The user guide release date has been updated. · Member summary, Page 3-12 - The device configuration has been updated; 'Servers' has been removed and add 'Snapshots'	The changes or updates made do not impact the SFRs or the functionality included in the scope of the previous evaluation.	CB consider it as **Minor**

Evidence Identification	Description of Changes	Rationale	Impact
	· View AFC filters, Page 3-17 - The procedure have been updated on the TPS devices TOS version. · Log Configuration, Page 3-73 – Log Configuration screen to configure remote system have been updated. · Roll back to a previous version, Page 3-97 - Next steps have been updated (TOS 5.x.x and later images only) · Advanced DDoS supported models, Page 3-109 - The SMS supports DDoS devices have been added; 5600TXE (TOS 6.5 and later) Prerequisites, Page 6-25 - The devices that support HTTP have been added; TPS (5600TXE) — TOS v6.5.0 or later · Configure URL Threat Analysis procedure, Page 6-27 - Tags have been added; Trend Micro Detection Category: Suspicious Object, Trend Micro Publisher: Trend Micro Deep Discovery Analyzer, Trend Micro Severity: High and Trend Micro Source: (DD Analyzer IP Address)		
Command Line Interface Reference: Trend Micro TippingPoint Security Management System (SMS) Command Line Interface Reference, v6.5.0, December 2024.	The SMS CLI documentation, v6.5.0, December 2024 has been reviewed, and no changes have been identified in the current version.	The changes or updates made do not impact the SFRs or the functionality included in the scope of the previous evaluation.	CB consider it as **Minor**

4 Result of Analysis

14 The outcome of the review determined that none of the modifications significantly affects the security mechanisms that implement the functional requirements defined in the Security Target (Ref [2]), in accordance with the Assurance Continuity Procedure (Ref [4]).

15 The nature of the changes leads to the conclusion that they are classified as MINOR changes. Therefore, based on the evidence provided, it is agreed that assurance is maintained for this version of the product.

Annex A References

[1] Trend Micro TippingPoint Security Management System (SMS) v6.5.0 Impact Analysis Report (IAR) Version 1.1, 23 Mar 2026

[2] Trend Micro TippingPoint Security Management System (SMS) v6.4.0 Security Target, Version 1.3, 22 December 2025

[3] Evaluation Technical Report – Trend Micro TippingPoint Security Management System (SMS) v6.2.0, V1.0, 02 April 2024

[4] Assurance Continuity: CCRA Requirements Version 3.1, Feb 2024

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

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

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

[8] MyCC Scheme Requirement (MyCC_REQ), v2, 24 April 2025.

[9] ISCB Evaluation Facility Manual (ISCB_EFM) v4, 24 April 2025.

[10] Verification Test Plan Report Version 1.0, 18 Mar 2026

[11] M022 Assurance Maintenance Report Trend Micro TippingPoint Security Management System v6.4.0 version 1, 17 June 2025

--- END OF DOCUMENT ---