Agenzia per la Cybersicurezza Nazionale

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) ver.3.1 rel. 5

Certificato n. *(Certificate No.)*	05/2026
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/13/2024/RC, v. 1.0
Decorrenza *(Date of 1st Issue)*	4 febbraio 2026
Nome e Versione del Prodotto *(Product Name and Version)*	MetaDefender Core v5.14.2 & MetaDefender Kiosk v4.7.6
Sviluppatore *(Developer)*	OPSWAT Inc.
Tipo di Prodotto *(Type of Product)*	Protezione Dati (Data Protection)
Livello di Garanzia *(Assurance Level)*	EAL4+ (ALC_DVS.2, ALC_FLR.2, AVA_VAN.5) conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto conforme a CC Parte 2 estesa

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 4 febbraio 2026

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando Metodologia Comune per la Valutazione di Sicurezza della tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility Common Methodology for Information Technology Security Evaluation version 3.1 release 5 for conformance to *Common Criteria for Information Technology Security Evaluation version 3.1 release 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

MetaDefender Core v5.14.2 & MetaDefender Kiosk v4.7.6

OCSI/CERT/CCL/13/2024/RC

Version 1.0

4 February 2026

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	04/02/2026

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

ACVP	Automated Cryptographic Validation Protocol
AES	Advanced Encryption Standard
AI	Artificial Intelligence

AMSI	Antimalware Scan Interface
API	Application Programming Interface
AV	Antivirus
CDR	Content Disarm and Reconstruction
DLP	Data Loss Prevention
IV	Initialization Vector
JSON	JavaScript Object Notation
LTS	Long Term Support
LTSC	Long-Term Servicing Channel
NGAV	Next Generation Antivirus
OS	Operating System
P.O.	Purchase Order
REST	Representational state transfer
SBOM	Software Bill Of Material
SDK	Software Development Kit
SKU	Stock Keeping Units
SQL	Structured Query Language
UI	User Interface
XSS	Cross Site Scripting

4 References

4.1 Normative references and national Scheme documents

[CC1] CCMB-2017-04-001, "Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model", Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, "Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components", Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, "Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components", Version 3.1, Revision 5, April 2017

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[CEM] CCMB-2017-04-004, "Common Methodology for Information Technology Security Evaluation – Evaluation methodology", Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Technical documents

[AGDv1.9] AGD Documentation MetaDefender Core & MetaDefender Kiosk Evaluation Assurance Level (EAL): EAL4+, augmented with ALC_DVS.2, ALC_FLR.2, AVA_VAN.5, Version v1.9, Date 2025-12-04.

[ETRv3] Evaluation Technical Report Evaluation of MetaDefender Core v5.14.2 & MetaDefender Kiosk v4.7.6 according to CC Assurance Level EAL4 augmented with ALC_DVS.2, ALC_FLR.2, AVA_VAN.5 based on ISO/IEC 18045:2008

Information technology – Security techniques – Methodology for IT security evaluation, OPSWATEVMD-042_ETR_v3, Version v3, 2026-01-09.

[MDCore_Man] MetaDefender Core v5.14.2 manual.

[MDKiosk_Man] MetaDefender Kiosk Windows v4.7.6 manual.

[ST] Security Target MetaDefender Core & MetaDefender Kiosk Evaluation Assurance Level (EAL): EAL4+, augmented with ALC_DVS.2, ALC_FLR.2, AVA_VAN.5, Version v1.10, Date 2025-12-04.

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT Products. A higher recognition level for evaluations beyond EAL4 is provided for IT Products related to specific Technical Domains only.

The current list of signatory nations and technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA for all claimed assurance components up to EAL4.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA]) was ratified on 8 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all claimed assurance components up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product "**MetaDefender Core v5.14.2 & MetaDefender Kiosk v4.7.6**", developed by OPSWAT Inc.

The TOE is composed of two parts: MetaDefender Kiosk and MetaDefender Core.

MetaDefender Kiosk is a cybersecurity solution for protecting critical networks and assets against removable media threats. It is a front-end component that is used as a media scanning workstation. MetaDefender Core is a backend component that provides centralized file analysis orchestration capabilities. MetaDefender Core is powered by a suite of cybersecurity technologies such as Multiscanning, Deep CDR, Proactive DLP, Adaptive Sandbox and others to detect, analyze and eliminate malware and zero-day attacks.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]. The potential consumers of the product should also review the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC version 3.1 Revision 5 for the assurance level EAL4 augmented with ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5, according to the information provided in the Security Target [ST] and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA], and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product "MetaDefender Core v5.14.2 & MetaDefender Kiosk v4.7.6" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	MetaDefender Core v5.14.2 & MetaDefender Kiosk v4.7.6
Security Target	OPSWAT Security Target MetaDefender Core & MetaDefender Kiosk, v1.10, 2025-12-04 [ST]
Evaluation Assurance Level	EAL4 augmented with ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5
Developer	OPSWAT Inc. (Vietnam Site)
Sponsor	OPSWAT Inc. (USA Site)
LVS	CCLab - The Agile Cybersecurity Laboratory (Debrecen site)
CC version	3.1 Rev. 5
PP conformance claim	None
Evaluation starting date	26 June 2024
Evaluation ending date	9 January 2026

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled and, in the configuration, shown in "Annex B – Evaluated configuration" of this Certification Report.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description it is possible to refer to the Security Target [ST].

The Target of Evaluation (TOE) is the MetaDefender Core v5.14.2 & MetaDefender Kiosk v4.7.6. OPSWAT MetaDefender Kiosk is a file-based threat detection and prevention solution for protecting critical networks and assets against removable media threats. MetaDefender Core is the backend component that provides centralized file analysis orchestration capabilities. MetaDefender Core is powered by a suite of cybersecurity technologies such as Multiscanning, Deep CDR, Proactive DLP, Adaptive Sandbox and others to detect, analyze and eliminate malware and zero-day attacks.

MetaDefender Kiosk is the front-end component to the Core, that is used as a media scanning workstation. Based on scan results, files are handled according to administrator defined policies for 'Blocked Files' and 'Allowed Files'.

An example deployment of the TOE (framed in red) is shown in Figure 1. The figure below illustrates the TOE architecture containing TOE and non-TOE components, that also defines TOE boundary.

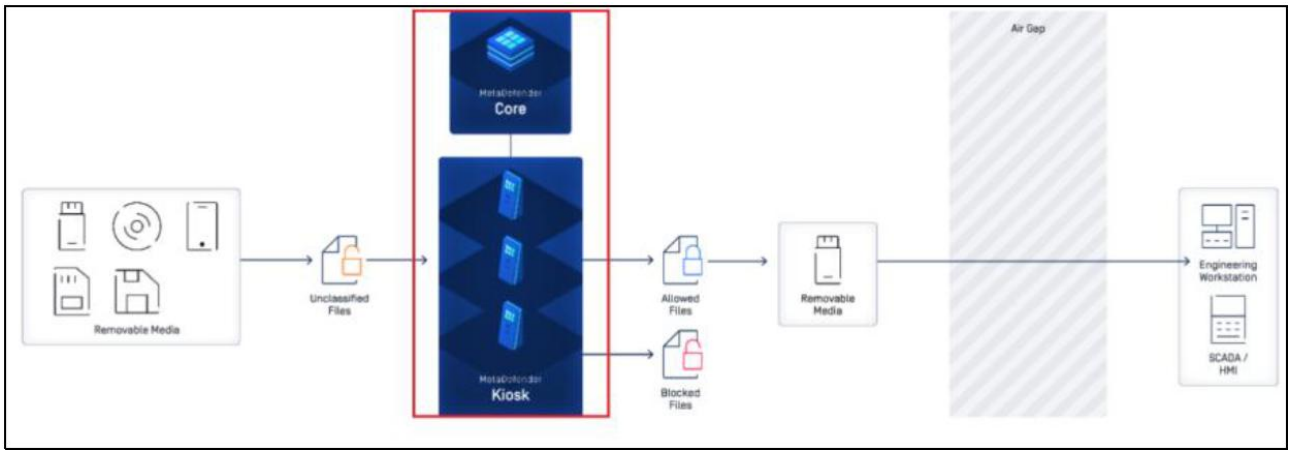

Figure 1 – TOE deployment and Boundary

The TOE in the red box includes two different components (applications): MetaDefender Kiosk and MetaDefender Core (with engines / technologies underneath). MetaDefender Kiosk picks up files from certain sources (removeable devices) and submit to MetaDefender Core for file analysis and further processing.

The TOE is typically deployed into secure environments that require all portable media to be scanned on entry and/or exit.

MetaDefender Kiosk

Media such as USB devices, DVDs, card readers, SD cards, flash drives, mobile phones, or floppy disks, are scanned by MetaDefender Kiosk by inserting the media device into the appropriate drive. After the scan is complete, Kiosk generates a detailed report.

MetaDefender Kiosk requires a 64-bit Windows OS. The evaluated configuration assumes Windows 10 and requires hardware that supports the above Windows OS and desired portable media peripherals. Hardware may be user supplied or purchased from OPSWAT.

Note: the consumer version of Windows 10 reached end of life and is no longer supported. Microsoft provides a Windows 10 IoT Enterprise LTSC 2021 for enterprise customers which has a mainstream end of life until January 12, 2027, while an extended end of life until January 13, 2032 can be obtained: https://learn.microsoft.com/en-us/lifecycle/products/windows-10-iot-enterprise-ltsc-2021

MetaDefender Core

MetaDefender Kiosk uses MetaDefender Core to process files. MetaDefender Core has the following usage characteristics:

- REST API: MetaDefender Core implements a REST API over HTTPS. All file processing (e.g. Kiosk or Web UI) occurs via this JSON-based interface.
- Core Management Console: The MetaDefender Core Management Console Web UI allows remote management via HTTPS.

- File Processing: MetaDefender Core has the following file processing capabilities: Scanning with multiple anti-malware engines (using over 30 anti-malware engines), Deep Content Disarm and Reconstruction (CDR) / Data sanitization, File-based vulnerability assessment, Proactive Data Loss Prevention (DLP).

MetaDefender Core requires any appropriate hardware that supports Windows and Unix based deployments: Windows Server 2022; Ubuntu 20.04 and 22.04.

The evaluated configuration assumes a network environment that provides connectivity between the Core and Kiosk.

The following Table 1 lists the modules composing the TOE.

Name	Type	Version for Windows	Version for Linux
Metascan Engine	Module	5.14.2	5.14.2
Proactive DLP	Module	2.22.1-1738248658	2.22.1-3958
Deep CDR	Module	7.3.2-21425	7.3.2-21425
InSights Threat Intelligence	Module	2.1.0-293	2.1.0-293
Sandbox	Module	2.2.0-280	2.2.0-326
SBOM	Module	3.1.0-351	3.1.0-351
Reputation	Module	2.1.2-1728564486	2.1.2-1728562722
File Based Vulnerability Assessment	Module	4.2.416.0-154	4.57-236
Country of Origin	Module	1.1.0-292	1.1.0-292
Archive Extraction	Utility	7.3.2-6679	7.3.2-6679
Archive Compression	Utility	7.3.2-6679	7.3.2-6679
File Type	Utility	7.3.1-7712	7.3.1-7712
Yara	Utility	4.2.0-370	4.2.0-370

Table 1 - Modules

7.3.1 TOE architecture

The TOE includes the following subsystems and modules.

MetaDefender Core (Subsystem):

- *Core Main Service*: it serves as the backend of the system. It acts as the primary interface for receiving requests from clients, as a central point for task distribution, coordinating and

assigning jobs to different modules, consolidating results. It receives requests from clients, such as file scans, and determines the appropriate actions to be taken. When a file is submitted for scanning, the Core Main service is responsible for routing the file to the appropriate engines according to the specified workflow rule for analysis.

- *PostgreSQL Service*: the Core Main Service incorporates a PostgreSQL service as a backend database. This PostgreSQL service is responsible for storing and managing critical data such as scan results, history, statistics, workflow rules and system configurations.
- *Engines*: a collection of OPSWAT technology modules. The relationship and communication between the Core Main service and Engines is crucial for the system's functionality. The TOE orchestrates these engines, aggregates their outputs, and enforces defined responses based on configurable security policies. These engines are designed to perform analysis, inspection and sanitization of files and data. Some engines focus on a specific aspect of analysis such as malware scanning, behaviour analysis, or file type verification. It can detect a wide range of threats such as malware, vulnerabilities, and sensitive data. It also can sanitize and prevent possibilities of malicious content. Each engine process integrates one third-party antivirus SDK or library as a linked component (static or dynamic) within its in-house implementation. These SDKs (listed in the following Table 2) are invoked programmatically through well-defined APIs. They do not operate as standalone products, services, or independently configured software in the operational environment.

Name	Version for Windows	Version for Linux
Ahnlab	3.27.0.8-2308	3.26.1.4-2253
Antiy	3.0.3.1-1880	--
Avira	4.15.23-2168	4.15.23-2163
Bitdefender	3.0.1.306-2122	3.0.1.297-1800
Bkav Pro	8.2.25-422	--
ClamAV	1.4.1-2297	1.4.1-2392
CMC	2.3.5-353	2.3.5-150
Comodo	6.5.0.1195-2241	--
CrowdStrike	1.10.1-1691	1.10.1-1482
Cylance	1.2.1-484	1.2.0-539
Emsisoft	2021.05.7597-2001	--
Eset	1.0.0-2093	1.0.0-1933
Filseclab	1.0.2.2123-1948	--
Gridinsoft	1.0.203-281	--
Huorong	1.0.0-1800	--
Ikarus	6.3.23-2165	6.3.23-2110
K7	4.0.0.6-2240	4.0.0.5-2276
Lionic	8.23-1793	8.23-1600

Name	Version for Windows	Version for Linux
McAfee	6700-2106	6700-1866
NANOAV	1.0.146.25796-1701	1.0.38.74417-29-18
NETGATE	25.0.650.0-1397-35	--
Quick Heal	18.0-2046	18.0-1539
RocketCyber	12_02_2021-1818	22_05_2024-262
Scrutiny	3.2.4-1278	--
Sophos	4.20-3.92.0-1996	4.18-3.90.0-1798
Systweak	1.0.0.2-1785	--
Tachyon	2020.4.22.1-2115	20240927-1951
Varist	6.6.1-2178	6.6.1-2095
Vir.IT eXplorer	9.5.80-2229	--
VirusBlokAda	5.3.1-1932	--
Webroot SMD	1.4.114-1770	1.4.114-1767
Microsoft Defender	1.0.0-1329	--
XVirus	4.2.3-1717	4.2.3-354
Zillya!	1.2.0.11-1992	--

Table 2 – AV SDKs

- *Core Management Console Module*: This console serves a user-friendly interface for authorized users such as system administrators to monitor and manage MetaDefender Core system. From the console, authorized users can configure system settings, define workflow rules, monitor processing history, check statistics, generate reports and perform various administrative tasks.

MetaDefender Kiosk:

- *User Interface*: this is a Windows application used to display the user interface. It shows the UI for users to interact and scan peripheral devices. When users perform actions from the UI, it calls several APIs through the Kiosk Main Service to retrieve the necessary information and display the results to the user.
- *Kiosk Main Service*: this is the background service of Kiosk running on Windows. It handles various Kiosk system tasks (authentication, scanning, performing post actions, etc.). It provides protocols for other components to communicate with and returns results for display to the end user.
- *Kiosk Management Console Module*: this is a webpage for administrators to configure system settings. The console calls APIs to the Kiosk Main Service to load the current configurations. After the administrator makes adjustments, the Kiosk Console calls APIs through the Kiosk Main Service to update the new configurations. The MetaDefender Kiosk Management Console TSFI allows you to manage the MetaDefender Kiosk system through a web browser. The Management Console can be accessed through http(s)://<MetaDefender Kiosk system>:8009. After an initial, fresh installation, a configuration wizard is displayed to setup the Kiosk Management Console Module.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in section 3 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult section 1.3.3 and Chapter 7 of the Security Target [ST].

The major security features are the following:

- File Threat Analysis.
- Protected Communications.
- User Authentication Support.
- Security Management.

Security functionalities are summarized in the following sections.

7.3.2.1 File Threat Analysis

The TOE orchestrates the analysis of files for threats and generates associated scanning session reports. Based on scan results, files are handled according to administrator defined policies for 'Blocked Files' and 'Allowed Files'. Scan types include:

- **Scanning with multiple anti-malware engines:** file scanning in critical environment (no data is shared outside) using over 30 anti-malware engines, including signature-based detection, AI/NGAV and heuristic detection.
- **Deep CDR / Data sanitization:** remove active content from common types of document and image files by either converting the file format or removing hidden exploitable objects such as scripts and macros.
- **File-based Vulnerability Assessment:** ability to identify all known vulnerabilities in binaries (applications, patches, firmware updates) that might be used to exploit and compromise the end-user system once installed/deployed.
- **Proactive DLP:** detect, redact, watermark, or block sensitive data in supported file types. Sensitive data may include credit card numbers, social security numbers or any specific data pattern using a regular expression.
- **File Handling:** the Kiosk manages file handling actions for both blocked and allowed files during processing. For blocked files, actions include reporting, stopping the session, removal, sanitization, and copying to specified locations. For allowed files, actions include reporting, wiping and copying back to original media, sanitization, and copying to specified locations.
- **Reporting:** after media processing, the session results show completion status, counts of allowed and blocked files, and total files processed. If any file wasn't processed by MetaDefender, a warning is displayed.

7.3.2.2 Protected Communications

The TOE makes use of HTTPS/TLS to protect communication with remote administrators and between the Kiosk and Core.

7.3.2.3 User Authentication Support

The TOE supports authenticating users as follows:

- **Kiosk Scanning User**: Kiosk scanning users are authenticated using Windows Login (i.e. the TOE invokes Windows Login) Guest users may also perform scans depending on the defined policy.
- **Kiosk Management Console User**: Kiosk administrators are authenticated by means of a username and password against a local database.
- **Core REST API / Management Console User:** Core users are authenticated by means of a username and password against a local database.

7.3.2.4 Security Management

The TOE enables secure management of its security functions, including enforcing role-based access control, generating security audit events and performing trusted software updates, including updates to engines and signatures, using digital signatures. The TOE generates keys according to the referred standards and also provides key destruction.

7.3.3 Excluded Functionalities

As per section 1.3.5 of [ST], the following functionalities available in MetaDefender Core & MetaDefender Kiosk have not been evaluated:

- Use with Vault Server.
- Email password recovery.
- Custom scanners.
- Yara rule sources.
- Cloud based scanning by 3rd party malware engines.
- Sending files to MetaDefender Cloud.
- Decryption / unlock of password protected files.
- Kiosk visitor management.
- Single Sign-On.
- Integration with Active Directory.

7.4 Documentation

The guidance documentation specified in “Annex A – Guidelines for the secure usage of the product” is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration, and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile (PP).

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3] and are from EAL 4 assurance package, augmented with the CC part 3 components ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5.

All the SFRs have been selected or derived by extension from CC Part 2 [CC2].

Security Target [ST] provides a complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab - The Agile Cybersecurity Laboratory (Debrecen site).

The evaluation was completed on 9th January 2026, with the delivery by LVS of the Evaluation Technical Report v3 [ETRv3], which was approved by the Certification Body on 13th January, 2026. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in “Annex B – Evaluated configuration”. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; there is a probability (lower as the assurance level increases), that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETRv3] issued by the LVS CCLab - The Agile Cybersecurity Laboratory (Debrecen site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "MetaDefender Core v5.14.2 & MetaDefender Kiosk v4.7.6" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4 augmented with ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in "Annex B – Evaluated configuration".

Table 3 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4 augmented with ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5 (augmentations are represented in italics in Table 3).

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass
Sufficiency of security measures	*ALC_DVS.2*	*Pass*
Developer defined life-cycle model	ALC_LCD.1	Pass

Assurance classes and components		Verdict
Well-defined development tools	ALC_TAT.1	Pass
Flaw reporting procedures	*ALC_FLR.2*	*Pass*
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Advanced methodical vulnerability analysis	*AVA_VAN.5*	*Pass*

Table 3 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the product "MetaDefender Core v5.14.2 & MetaDefender Kiosk v4.7.6" are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the "Security Objectives for the Operational Environment" specified in section 4 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions and Organizational Security Policies described in section 3.1 and 3.3 of the Security Target [ST] shall be satisfied.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, "Annex A – Guidelines for the secure usage of the product" includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE (CC guidance [AGDv1.9] and the manuals [MDCore_Man], and [MDKiosk_Man]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

The following procedural steps define how the TOE is delivered to the customer:

1. Receive P.O. – After the contact is established between the customer and OPSWAT, the customer sends a purchase order to the OPSWAT department, the purchase order is received within OPSWAT's fulfilment department.
2. Review P.O. – The Developer verifies whether the SKUs (Stock Keeping Units) within the PO are correct.
3. Issue license keys – The license keys are issued based on number of product instances purchased and software subscription terms.
4. Notify the customer – The customer is invited to register and login to the my.opswat.com portal to download the software installation packages and to activate the product license. Download links to the TOE are the following:

    - Windows:

      https://installer-cdn.opswat.com/Metadefender/Core/v5/5.14.2-1/windows/ometascan-5.14.2-1-x64.msi

      The customer can check the validity of the installation package by verifying that the SHA256 hash is the following:

      `02221a37df0f45f80de475386829e56957fa0a908c61cbf8b937f1a49781cf4b`

      It is possible to verify by checking the hash posted on the my.opswat.com portal as shown in the following Figure 2.

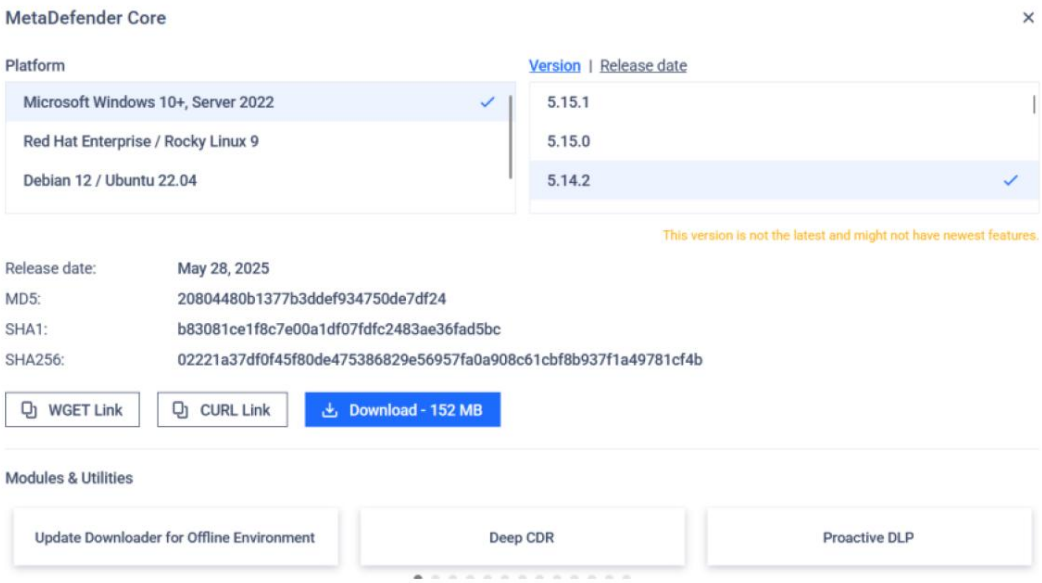

Figure 2 – SHA256 for MetaDefender Core Windows Version

- Debian based:

  https://installer-cdn.opswat.com/Metadefender/Core/v5/5.14.2-1/debian/ometascan_5.14.2-1_amd64.deb

  The customer can check the validity of the installation package by verifying that the SHA256 hash is the following:

  `0d619e8fff19548027e9af01f4b0b5929f9e394c2f2503e7c799c8e1777754e9`

  It is possible to verify by checking the hash posted on the my.opswat.com portal as shown in the following Figure 3.

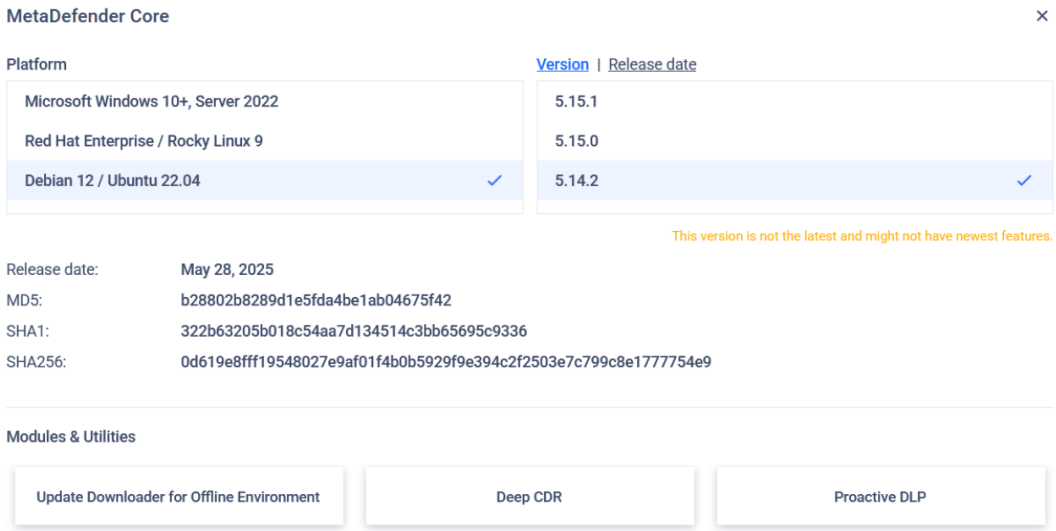

Figure 3 – SHA256 for MetaDefender Core Debian/Ubuntu Version

- Kiosk (only Windows):

  https://installer-cdn.opswat.com/kiosk/MetaDefender_Kiosk_4.7.6.3642.exe

  The customer can check the validity of the installation package by verifying that the SHA256 hash is the following:

  `b89a255fc7218a4ecb3b2f8ee6d4673450148cf79bca0d986c1b990a70e570ad`

It is possible to verify by checking the hash posted on the my.opswat.com portal as shown in the following Figure 4.

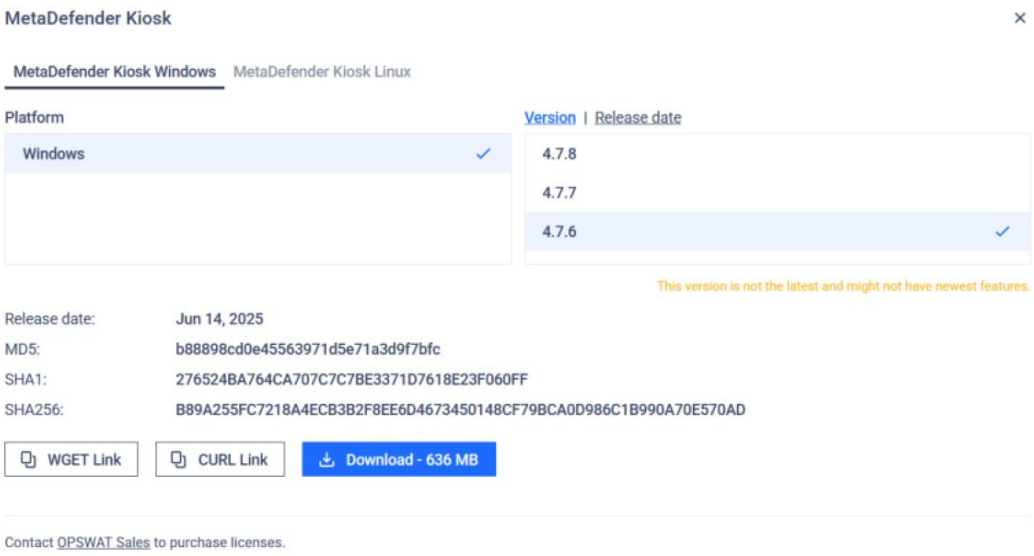

Figure 4 – SHA256 for MetaDefender Kiosk (Windows only)

9.2 Installation, configuration, and secure usage of the TOE

TOE installation, configuration and operation should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the Common Criteria guidance [AGDv1.9], [MDCore_Man], and [MDKiosk_Man] contain detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST].

The AGD Documentation [AGDv1.9], [MDCore_Man], and [MDKiosk_Man] are available on the following pages:

- https://www.opswat.com/docs/mdcore/v5.14.2/installation/metadefender-core-documentation
- https://www.opswat.com/docs/mdkiosk/v4.7.6/release-notes/release-notes

Every other product related documentation is available through the OPSWAT's Technical Documentation for OPSWAT Products page (https://www.opswat.com/docs/mdcore, https://www.opswat.com/docs/mdkiosk), where always the latest documentation is published.

10 Annex B – Evaluated configuration

The Evaluator has followed the preparation steps for the TOE defined in [AGDv1.9], [MDCore_Man], and [MDKiosk_Man] for the evaluated configuration.

The evaluated configuration of the TOE consists of the following installation packages:

- MetaDefender Core:
  - metascan-5.14.2-1-x64.msi (Windows version)
  - metascan_5.14.2-1_amd64.deb (Debian/Ubuntu version)
- MetaDefender Kiosk:
  - MetaDefender_Kiosk_4.7.6. 3642.exe (Windows only)

Note: MetaDefender Core running on Red Hat Enterprise / Rocky Linux 9 has not been evaluated.

For more details, please consult section 1.4 of the Security Target [ST] and [AGDv1.9].

10.1 TOE operational environment

The LVS reproduced the operational environment consistent with [ST], [AGDv1.9], [MDCore_Man], and [MDKiosk_Man].

The operational environment consists of the following:

- A Windows 2022 Server running:
  - A modern graphical web browser – Google Chrome.
  - MetaDefender Core v5.14.2 (Windows version) with local PostgreSQL Database.
- An Ubuntu 22.04.5 LTS (Jammy Jellyfish) desktop version running:
  - A modern graphical web browser – Google Chrome.
  - MetaDefender Core v5.14.2 (Debian/Ubuntu version) with local PostgreSQL Database.
- A Windows 10 IoT Enterprise LTSC 2021 workstation running:
  - A modern graphical web browser – Google Chrome.
  - MetaDefender Kiosk v4.7.6 using MongoDB.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

Testing activities have been carried out at LVS premises.

The Evaluators verified the configuration of the test environment, including the TOE, and found it to be consistent with the AGD documentation [AGDv1.9], the relevant manual documentation [MDCore_Man], [MDKiosk_Man] and the Security Target [ST].

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer provided 30 manual test cases, covering the whole TSF:

- File Threat Analysis.
- Protected Communications.
- User Authentication.
- Security Management.

11.2.2 Test coverage

The Evaluators have reviewed the test plan presented by the Developer and verified the complete coverage of the functional requirements (SFRs) and the TSFIs described in the functional specification. The Evaluators verified that the test cases are sufficient to demonstrate the correct internal behaviour and the properties of the TSF.

11.2.3 Test results

The actual test results of all Developer's tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

Before initiating the testing activity, the Evaluators verified that the TOE was configured correctly.

Evaluator executed all the 30 test cases.

The Evaluator has already examined that the Developer's testing effort was to cover the whole TSF. Since no security feature is missing from the Developer's testing effort, the Evaluator created and performed 3 more independent test cases to test the TSF more in depth:

- Verification that the TOE uses the proper ciphers between the MetaDefender Core WebUI/REST API and Kiosk Management Console WebUI.
- Verification that the TOE protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE.
- Verification of threat detection and prevention features on the TOE.

11.3.2 Test results

All Developer's tests were run successfully; the Evaluators verified the correct behaviour of the TSFIs and TSFs and correspondence between expected results and achieved results for each test.

All test cases devised by the Evaluators were passed successfully and the actual test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked with the TOE already used for the functional test activities and verified that the TOE and the test environment were properly configured.

A search on public vulnerabilities on TOE has been conducted. The analysis confirmed that there are no public vulnerabilities exploitable with the TOE implementation and configuration.

Then the Evaluators designed and executed the following attack scenarios:

- Inject malicious XSS and HTML injection payload into an input field.
- Escalate privileges, performing unauthorized actions under a lower-privilege account in the MetaDefender Core
- Escalate privileges, performing unauthorized actions under a lower-privilege account in the MetaDefender Kiosk
- Enumerate/Brute-force users and exploit poor session management that could lead to possible vulnerabilities in MetaDefender Core
- Enumerate/Brute-force users and exploit poor session management that could lead to possible vulnerabilities in MetaDefender Kiosk
- Intercept, decrypt, or manipulate sensitive information being transmitted between a user and the server.
- Test for common server-side weaknesses such as File inclusion or Path traversal by sending malicious input to the TOE's graphical user (MetaDefender Core) interface.
- Test for common server-side weaknesses such as File inclusion or Path traversal by sending malicious input to the TOE's graphical user (MetaDefender Kiosk) interface.
- Search for and exploit NoSQL injection vulnerability entry points, especially in login forms, search functions, and endpoints of MetaDefender Kiosk.
- Search for and exploit SQL injection vulnerability entry points, especially in login forms, search functions, and endpoints of MetaDefender Core.
- Find hidden or not listed directories, secret files or other resources in MetaDefender Core.
- Find hidden or not listed directories, secret files or other resources in MetaDefender Kiosk.
- Gain sensitive information from backup files if it is not protected properly in the MetaDefender Kiosk.
- Escape the MetaDefender Kiosk restricted screen for the scanning by various escape techniques.
- Submit malicious, oversized files, or specially crafted payloads utilizing basic AV evasion methods to see if they can bypass scanning or crash the system in the MetaDefender Core.

- Attempt to bypass signature-based AV scanning using XOR based encryption with a single-byte key.
- Attempt to bypass signature-based AV scanning using XOR based encryption with a multiple-byte keyword.
- Attempt to bypass signature-based AV scanning using AES encryption with 32-bit key and 16-bit IV.
- Attempt to bypass signature- and heuristic-based AV scanning using encryption mixed with sleep-based and memory allocation based heuristic bypass.
- Attempt to bypass signature-and heuristic-based AV scanning using encryption mixed with various heuristic-bypass techniques.
- Attempt to bypass signature-and heuristic-based AV scanning using encryption mixed with various heuristic-bypass techniques embedded in process hollowing attack.
- Attempt to bypass AV scanning with AMSI-disabling PowerShell script.
- Attempt to bypass signature-and heuristic-based AV scanning using an obfuscated dropper, triggering attacks via HTTP using encryption mixed with various heuristic-bypass techniques embedded in process hollowing.

The Evaluators could then conclude that the TOE is resistant to a high attack potential in its intended operating environment. No exploitable or residual vulnerabilities have been identified.