MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

C105 Certification Report

Durio UTM version 3.2.5

File name: ISCB-5-RPT-C105-CR-v1
Version: v1
Date of document: 10 July 2020
Document classification: PUBLIC

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

C105 Certification Report

Durio UTM version 3.2.5

10 July 2020

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:	C105 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C105-CR-v1
ISSUE:	v1
DATE:	10 July 2020
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED 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. 726630-U

Printed in Malaysia

Foreword

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

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

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 14 July 2020, 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	30 Jun 2020	All	Initial draft
v1	10 July 2020	All	Final version

Executive Summary

The Target of Evaluation (TOE) is Durio Unified Threat Management (UTM) version 3.2.5. The TOE is a hardware appliance that includes several features such as firewall, antivirus software, content filtering and a spam filter in a single integrated package. The TOE is designed to provide firewall services ensuring network protection for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) networks. The TOE is capable of robust filtering based on information contained in IPv4, IPv6, ICMPv4, ICMPv6, TCP and UDP headers as specified by their respective RFC's. Additionally, the TOE is capable of content inspection of FTP and H.323 protocols to work with the dynamic nature of these protocols. The TOE has extensive logging capabilities. These audit logs are capable of being exported to an external syslog server over a protected channel for further analysis and inspection.

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

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

The evaluation was performed by Securelytics SEF and the evaluation was completed on 26 June 2020.

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 Durio Unified Threat Management version 3.2.5 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

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The TOE is Durio Unified Threat Management (UTM) version 3.2.5.

2 The TOE is a hardware appliance that includes several features such as firewall. antivirus software, content filtering and a spam filter in a single integrated package.

3 The TOE is a comprehensive security product that includes protection against multiple threats.

4 The TOE is designed to provide firewall services ensuring network protection for Internet Protocol version 4(IPv4) and Internet Protocol version (IPv6) networks.

5 The TOE is capable of robust filtering based on information contains in IPv4, IPv6, ICMPv4, ICMPv6, TCP and UDP headers as specified by their respective RFC's.

6 Additionally, the TOE is capable of content inspection of FTP and H.323 protocols to work with the dynamic nature of these protocols.

7 The TOE has extensive logging capabilities. These audit logs are capable of being exported to an external syslog server over a protected channel for further analysis and inspection.

8 The major security features of the TOE include:

a) Security Audit

b) Identification and Authentication

c) Security Management

d) Trusted Path

1.2 TOE Identification

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

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C105
TOE Name	Durio Unified Threat Management (UTM)
TOE Software Version	3.2.5
Security Target Title	Open Kod Durio Security Target
Security Target Version	1.0
Security Target Date	14 April 2020
Assurance Level	EAL2
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
Sponsor	Open Kod Sdn Bhd Suite 3-3A 4805, CBD Perdana 2, Jalan Perdana Cyber 12 Cyberjaya 63000 Selangor
Developer	Open Kod Sdn Bhd Suite 3-3A 4805, CBD Perdana 2, Jalan Perdana Cyber 12 Cyberjaya 63000 Selangor
Evaluation Facility	Securelytics SEF A-19-06, Tower A, Atria SOFO Suites, Petaling Jaya, Selangor Darul Ehsan

1.3 Security Policy

10 No organisational security policies have been defined regarding the use of the TOE.

1.4 TOE Architecture

11 The TOE includes both physical and logical boundaries which are described in Section 1.6 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

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

a) Security Audit

The TOE collects generates audit records for security events. Only Admin has the ability to view/export the audit logs.

b) Identification and Authentication

The TOE requires that each user is successfully identified (user IDs) and authenticated before any interaction with protected resources is permitted.

c) Security Management

The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.

d) Trusted Path

The TOE can protect the user data from disclosure and modification by using Secure Socket Layer (SSL) as a secure communication.

1.4.2 Physical Boundaries

13 The physical scope of the TOE includes the TOE hardware and software.

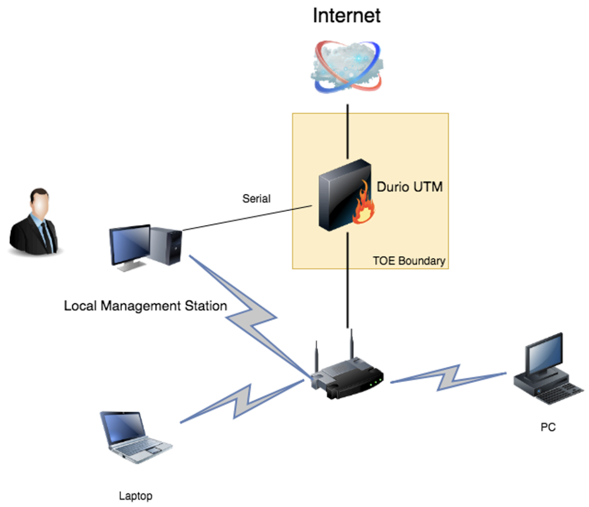


Figure 1: TOE physical boundary

1.5 Clarification of Scope

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

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

16 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

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

1.6.1 Environmental assumptions

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

a) A.PLATFORM

The TOE relies upon a trustworthy platform and local network from which it provides administrative capabilities. The TOE relies on this platform to provide logon services via a local or network directory service, and to provide basic audit log management functions. The platform is expected to be configured specifically to provide TOE services, employing features such as a host-based firewall which limits its network role to providing TOE functionality.

b) A.ADMIN

One or more competent, trusted personnel who are not careless, willfully negligent, or hostile, are assigned and authorized as the Admin, and do so using and abiding by guidance documentation.

c) A.USER

TOE users are not wilfully negligent or hostile and use the application within compliance of a reasonable enterprise security policy.

d) A. TIMESTAMP

The platforms on which the TOE operate shall be able to provide reliable timestamps.

e) A. PHYSICAL

The appliance hosting the firmware and database are in a secure operating facility with restricted physical access and non-shared hardware.

1.7 Evaluated Configuration

19 The following hardware models are capable of running in the evaluated configuration:

a) 1U hardware model. The TOE 1U models are:

- Durio 2H
- Durio 5H
- Durio 1K

b) 2U hardware model. The TOE 2U models are:

- Durio 2K
- Durio 5K

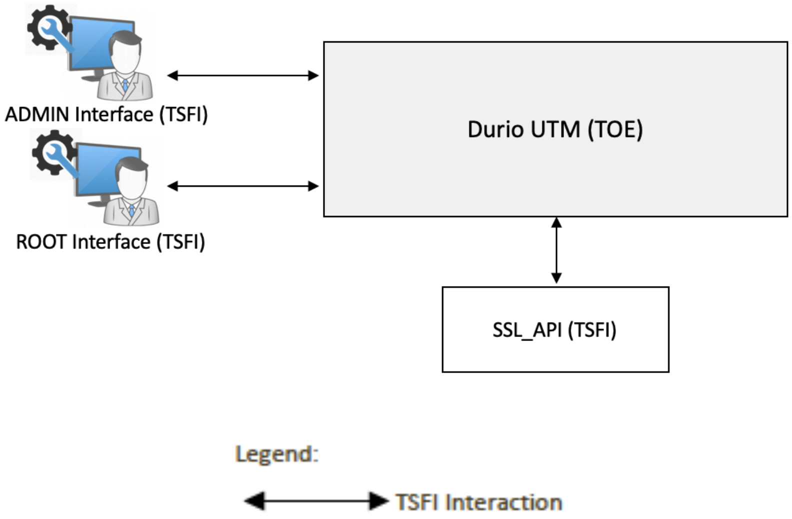
20 The evaluated configuration of the TOE, shown in Figure 2 The TOE has the following TSFI:

I. ADMIN Interface (SFR-enforcing). The ADMIN interface provides user interface for Admin to interface with TOE and perform security management functionality and operational functions via the web-based interface

II. ROOT Interface (SFR-enforcing). The ROOT interface provides Root users interface for Users to login and perform security management functionality and operational functions via the web-based interface and command line interface

III. SSL_API (SFR-enforcing). The programming interface used to engage the SSL functionality of the TOE and provide secure communication channel between the TOE and server

Figure 2 : Evaluated Deployment Configuration of the TOE



1.8 Delivery Procedures

21 The evaluators examined the delivery procedure, in which provide guidance for the developer to initiate delivery process of the TOE and its components to the intended recipient(s). It is also provide direction on the methods used to deliver the TOE to consumers and users of the product.

22 The TOE is delivered by Open Kod authorized representative to the customer.

23 It is sealed in a box (along with the user manuals) using a packaging tape.

24 Before the TOE is delivered, the following steps are performed by an Authorized Representative:

- Ensuring that the underlying software/hardware platforms meet the required specifications; A schedule is given to customers via email or phone call regarding the delivery of the TOE to allow customer to know when the TOE is expected to be delivered by the Authorized Representative.
- The TOE configuration will be performed by the Authorized Representative. The configuration process include the TOE configuration, credentials configuration, IP address, zone upload and license generation.
- Default accounts and passwords are created by Open Kod's representative.
- Upon completion of installation and configuration of the TOE, customer needs to complete the
- Application Installation Acceptance & Sign-off.

25 The Acceptance process for the TOE is as follows:

- Upon acknowledging the receipt of the appliance and the TOE, the customer will cross check the delivery order (DO) with the labelling, appliance part number and the version of the TOE.

26 If any problems occurs, the customer can directly approach the Authorized Representative during the setup phase or contact Open Kod support via email or phone for guidance.

2 Evaluation

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

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

29 The evaluators checked that the TOE provided for evaluation is labelled with its reference.

30 The evaluators checked that the TOE references used are consistent.

31 The evaluators examined the method of identifying configuration items to determine that it describes how configuration items are uniquely identified.

32 The evaluators examined the configuration items to determine that they are identified in a way that is consistent with the CM documentation.

33 The evaluators checked that the configuration list includes the

a) the TOE itself;

b) the parts that comprise the TOE;

c) the evaluation evidence required by the SARs in the ST

34 The evaluators examined the configuration list to determine that it uniquely identifies each configuration item.

35 The evaluators checked that the configuration list indicates the developer of each TSF relevant configuration item.

2.1.2 TOE Delivery

36 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.

37 The evaluators examined aspects of the delivery process to determine that the delivery procedures are used.

2.1.3 Development

38 The evaluators examined the functional specification and determined that the TSF is fully represented, it states the purpose of each TSF interface and method of use for each TSFI is given.

39 The evaluators examined the presentation of the TSFI to determine that it completely identifies all parameters associated with every TSFI.

40 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes the SFR-enforcing actions associated with the SFR-enforcing TSFIs.

41 The evaluators examined that the developer supplied tracing links of the SFRs to the corresponding TSFIs.

42 The evaluators examined the functional specification to determine that it is a complete and an accurate instantiation of the SFR.

43 The evaluators examined the security architecture description to determine 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 document

44 The evaluators examined the security architecture description to determine that it describes the security domains maintained by the TSF

45 The evaluators examined the security architecture description to determine that it presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

46 The evaluators examined the TOE design to determine that the structure of the entire TOE is described in terms of subsystems and all subsystems of the TSF are identified.

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

48 The evaluators examined the TOE design to determine that it provides a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

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

2.1.4 Guidance documents

50 The evaluators examined the operational user guidance and determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

51 The evaluators examined the operational user guidance to determine that it describes, for each user role, the secure use of the available interfaces provided by the TOE.

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

53 The evaluators the operational user guidance to determine that it is clear and reasonable.

54 The evaluators examined the provided acceptance procedures to determine that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

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

56 The evaluators performed all user procedures necessary to prepare the TOE to determine that the TOE and its operational environment can be prepared securely using only the supplied preparative procedures.

2.1.5 IT Product Testing

57 Testing at EAL 2 consists of assessing developer tests, sufficiency test and conducting penetration tests. The TOE testing was conducted by evaluators from Securelytics SEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.5.1 Assessment of Developer Tests

58 The evaluators verified that the developer has met their testing responsibilities by repeating the 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.

2.1.5.2 Independent Test

59 At EAL 2, independent test demonstrates the correspondence between the security functional requirements (SFRs) defined in Security Target, and the test cases that test the functions and behaviour of the TOE that meets those requirements. The evaluators have decided to perform testing based on the TOE Security Functions.

60 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 developed and performed by the evaluators to verify the functionality as follows:

Table 2: Functional Test

Test ID	Description	SFRs	Results
F001 – Identification and Authentication Security Management ADMIN Interface ROOT Interface	1. To test that each user to be successfully authenticated and identified before allowing any other TSF-mediated actions on behalf of that user. 2. To test that the TOE maintains the roles Admin and Root 3. To test that the TOE enforces the access control SFP to restrict the ability to change default, modify and delete the security attributes Admin Account, TOE Configuration and Users Account to Admin 4. To test that the TOE maintains the following list of security attributes belonging to individual users; Username, Password 5. To test that the TOE enforce access control SFP to provide permissive default values for security attributes that are used to enforce the SFP. 6. To test that the TOE performs the following management functions: Refer to objects listed in Section 5.2.4 of the ST. 7. To test that the TOE restricts the ability to modify the TSF data on the Durio Unified Threat Management (UTM) to Admin. 8. To test that the TOE enforces the access control SFP on objects listed in Section 5.2.4 of the ST. 9. To test that TOE Admin is successfully authenticated accordingly, then access is granted based on privilege allocated, else is denied.	FIA_ATD.1 FIA_UID.2 FIA_UAU.2 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_MOF.1 FMT_SMF.1 FMT_SMR.1 FDP_ACC.1 FDP_ACF.1	Pass
F002 – Trusted Path SSL_API	1. To test that the TOE provides a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure. 2. To test that the TOE permits remote users to initiate communication via the trusted path. 3. To test that the TOE requires the use of the trusted path for initial user	FTP_TRP.1	Pass

	authentication and other services for which trusted path is required.		
F003 – Security Audit ADMIN Interface ROOT Interface	1. To test that the TOE able to generate audit record of the following auditable events: a. Traffic monitoring - the ntopng graphic interface gives a real time overview of the network traffic using charts. b. Summary - get daily summaries of all logs c. Logs from the intrusion detection system (IDS), OpenVPN, and antivirus d. Firewall - logs from iptables rules e. Proxy - logs from the HTTP, SMTP, and content filter proxies 2. To test that the TOE record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST 3. To test that the TOE provides the Admin with the capability to read all audit information from the audit records and provide the audit records in a manner suitable for the user to interpret the information.	FAU_GEN.1 FAU_SAR.1	Pass

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

2.1.5.3 Vulnerability Analysis

62 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.

63 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing a

basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapse 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

2.1.5.4 Vulnerability testing

64 The penetration tests focused on:

i) SQL Injection

ii) Information Disclosure

iii) Failure to restrict URL Access

iv) Weak Password Policy

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

2.1.5.5 Testing Results

66 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 tests conducted were PASSED as expected.

3 Result of the Evaluation

67 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 Durio UTM version 3.2.5 which is performed by Securelytics SEF.

68 Securelytics SEF found that Durio UTM version 3.2.5 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.

69 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

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

71 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 an attacker possessing a Basic attack potential.

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

3.2 Recommendation

73 It is strongly recommended that:

a) Even though the identified vulnerabilities are out of scope of the evaluation, the developer should address all residual vulnerabilities by:

I. Preventing XSS malicious scripts from being executed in the ‘Description’ parameter within the ‘Network Uplink Editor’ menu. Effectively preventing XSS vulnerabilities is likely to involve a combination of the following measures:

- Filter input on arrival. At the point where user input is received, filter as strictly as possible based on what is expected or valid input.
- Encode data on output. At the point where user-controllable data is output in HTTP responses, encode the output to prevent it from being interpreted as active content. Depending on the output context, this might require applying combinations of HTML, URL, JavaScript, and CSS encoding.
- Content Security Policy. As a last line of defense, you can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.

II. Configuring the cookies from ‘HTTPOnly’ flag to ‘Secure’ flag in the ‘Dashboard Settings’ menu page

III. Implementing a secure HTTP header such as X-Frame-Options, Cross-Origin-Resource-Sharing, HTTP Strict Transport Security (HSTS), Cache-Control and Pragma or Content Security Policy (CSP) in the ‘Backup Settings’ page

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

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), v1, CyberSecurity Malaysia, Dec 2019.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v2, Dec 2019.

[6] Open Kod Durio Security Target, Version 1.0, 14 April 2020.

[7] Evaluation Technical Report Durio UTM, Version 1.0, 26 June 2020.

A.2 Terminology

A.2.1 Acronyms

Table 3: 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
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 4: Glossary of Terms

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

Term	Definition and Source
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 ---