MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C111 Certification Report

Invisiron Cyber Defence Platform 3.1.0

File name: ISCB-5-RPT-C111-CR-v1a
Version: v1a
Date of document: 16 April 2020
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999
www.cybersecurity.my

C111 Certification Report

Invisiron Cyber Defence Platform 3.1.0

10 April 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:	C111 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C111-CR-v1a
ISSUE:	v1a
DATE:	16 April 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 16 April 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).

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 March 2020	All	Initial draft
v1	10 April 2020	All	Final version
v1a	16 April 2020	vii,1,4	1) Removed the word “reputation-based” in Paragraph 1 of Executive Summary and in Section 1.1 TOE Description 2) Removed the word “ Ref[4]” in Paragraph 3 of Executive Summary 3) Removed the word “implement” in Section 1.1 TOE Description

Executive Summary

The Target of Evaluation (TOE) is Invisiron Cyber Defence Platform 3.1.0 executing on S-1000, S-2000, S-4000, S-6000, S-6000DNS, S-6000DDoS and microDefender appliances. The TOE is a software and hardware appliance. Each appliance model operates using an identical software image with identical functionality. The TOE is used as a network monitoring and incident management platform. They implement an intrusion and prevention system and reputation-based detection. The intrusion detection and prevention engine implement a full deep packet inspection capability (DPI). This engine is controlled by rules that are similar to the industry standard SNORT rules. These rules allow for performing deep packet inspection of the network traffic at full line rate. The reputation-based detection engine is built around blacklists. These blacklists contain malicious IP addresses, domain names, DGA domains, Tor exit nodes, URLs and SSL certificates. In addition to the security engines the TOE also provides security event logging and packet capture. This data is stored in files which can be exported out from the platforms. The TOE physical boundary defines all hardware and software that is required to support the TOE's logical boundary as well as the TOE's security functionality.

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 28 March 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 Invisiron Cyber Defence Platform 3.1.0 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The TOE is Invisiron Cyber Defence Platform 3.1.0 executing on S-1000, S-2000, S-4000, S-6000, S-6000DNS, S-6000DDoS and microDefender appliances.

2 The TOE is a software and hardware appliance. Each appliance model operate using an identical software image with identical functionality.

3 The TOE is used as a network monitoring and incident management platform. They implement an intrusion and prevention system and reputation-based detection.

4 The intrusion detection and prevention engine implement a full deep packet inspection capability (DPI).

5 This engine is controlled by rules that are similar to the industry standard SNORT rules.

6 These rules allow for performing deep packet inspection of the network traffic at full line rate.

7 The reputation-based detection engine is built around blacklists. These blacklists contain malicious IP addresses, domain names, DGA domains, Tor exit nodes, URLs and SSL certificates.

8 In addition to the security engines the TOE also provides security event logging and packet capture.

9 This data is stored in files which can be exported out from the platforms. The TOE physical boundary defines all hardware and software that is required to support the TOE's logical boundary as well as the TOE's security functionality.

10 The major security features of the TOE include:

a) Intrusion and Packet Content Detection System

b) Security Audit

c) Identification and Authentication

d) Security Management

e) Secure Communication

1.2 TOE Identification

11 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	C111
TOE Name	Invisiron Cyber Defence Platform 3.1.0 executing on S-1000, S-2000, S-4000, S-6000, S-6000DNS, S-6000DDoS and microDefender appliances
TOE Software Version	3.1.0
TOE Hardware Models	S-1000, S-2000, S-4000, S-6000, S-6000DNS, S-6000DDoS and microDefender appliances
Security Target Title	Invisiron Cyber Defence Platform Security Target
Security Target Version	Version 1.0
Security Target Date	13 March 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 Extended CC Part 3 Conformant
Sponsor	Invisiron Pte Ltd 1 Pemimpin Drive #08-03, One Pemimpin Singapore 576151
Developer	Invisiron Pte Ltd 1 Pemimpin Drive #08-03, One Pemimpin Singapore 576151
Evaluation Facility	Securelytics SEF A-19-06, Tower A, Atria SOFO Suites, Petaling Jaya, Selangor Darul Ehsan

1.3 Security Policy

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

1.4 TOE Architecture

13 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

14 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) Intrusion and Packet Content Detection System

The TOE collects network traffic and subjects it to statistical and signature-based analysis, depending on configured security filters. If the analysis of collected network traffic indicates a potential intrusion attempt or the presence of malicious content in a packet, an action set associated with the detecting filter is triggered.

b) Security Audit

The TOE generates audit records for security events. Admin and Authorised User has the ability to view and export the audit and transaction logs.

c) Identification and Authentication

Admin is a user that is allowed to perform both TOE configuration and monitoring. Authorised user is a user that has the privilege to perform either TOE monitoring only or both TOE configuration and monitoring.

d) Security Management

The TOE maintains role-based access control mechanisms to ensure the functions are restricted to those who have the privilege to access them.

e) Secure Communication

The TOE can protect the user data from disclosure and modification by using HTTPS (TLS v1.2) and SSH as a secure communication.

1.4.2 Physical Boundaries

15 The TOE implements an advanced cyber threat defence mechanism.

16 It is designed to be installed in line between an Internet router and main network switch or firewall.

17 Network packets are inspected in real-time as they pass through the platform in both (inbound and outbound protection).

18 The TOE is divided into two (2) sections:

i) One section performs the security operations on the network packets.
ii) Other section handles the management and configuration of the platform.

19 The section that handles the security operations for the protected network is implemented without the use of a traditional operation system. Instead it is implemented using a technology that allows for direct ownership of the hardware of the server.

20 The section that handles management and configuration is implemented using a Linux kernel and a limited set of support functions.

21 The platforms presence on the network is transparent to another IT equipment in the protected network.

22 No IP addresses or MAC addresses are required or exposed on the Ethernet ports used for network protection.

23 Network packets travel through the platform in stealth mode and the security operations are performed on the packets as they reside temporarily in memory buffers in the platform.

24 There are no TCP/IP stacks being used and there is no operating system involved in the security operations.

25 The configuration and management are handled through a separate dedicated management Ethernet port only accessible from inside the protected network.

26 The platforms are configured and managed through a web GIU application accessed from this management Ethernet connection.

27 One part of this GUI web application handles device configuration and the second part allows for monitoring the device.

28 This communication goes over HTTPS through the use of a standard web browser inside the platform.

29 An external cloud located server is used to transfer up-to-date Cyber Threat Intelligence (CTI) to the TOE containing lists of malicious IP addresses, domain names, URL's, SSL certificates, TOR exit nodes, DGA domain names and DPI rules.

30 The TOE uses this intelligence to make decisions about what network packets to allow into the protected network and which ones to block and drop.

31 The TOE performs automatic hourly updates of this CTI over an SSH or HTTPS connection.

32 In addition to CTI updates the TOE also pull software updates from this server. The TOE support remote monitoring through either a third-party monitoring tool or by Invisiron's own developed remote monitoring tool called Threat Commander SIEM.

33 The TOE sends security events over an SSH to an external server running the remote monitoring software.

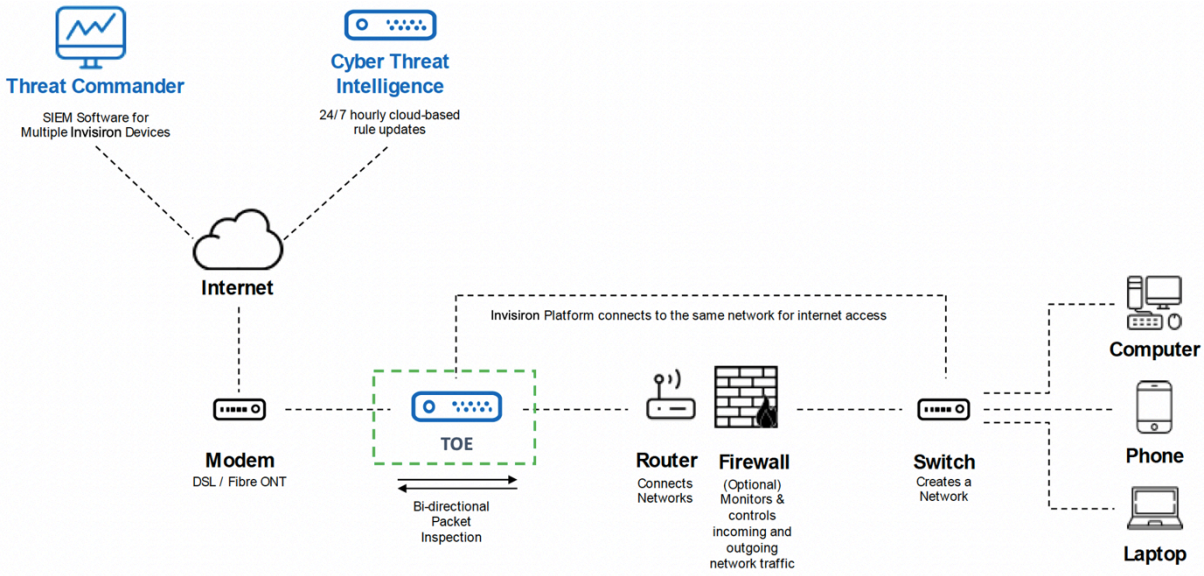


Figure 1: TOE physical boundary

1.5 Clarification of Scope

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

35 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]).

36 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

37 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

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

a) A.NOEVIL

Authorized admins are non-hostile and follow all administrator guidance.

b) A.PHYSEC

The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

c) A.SINGEN

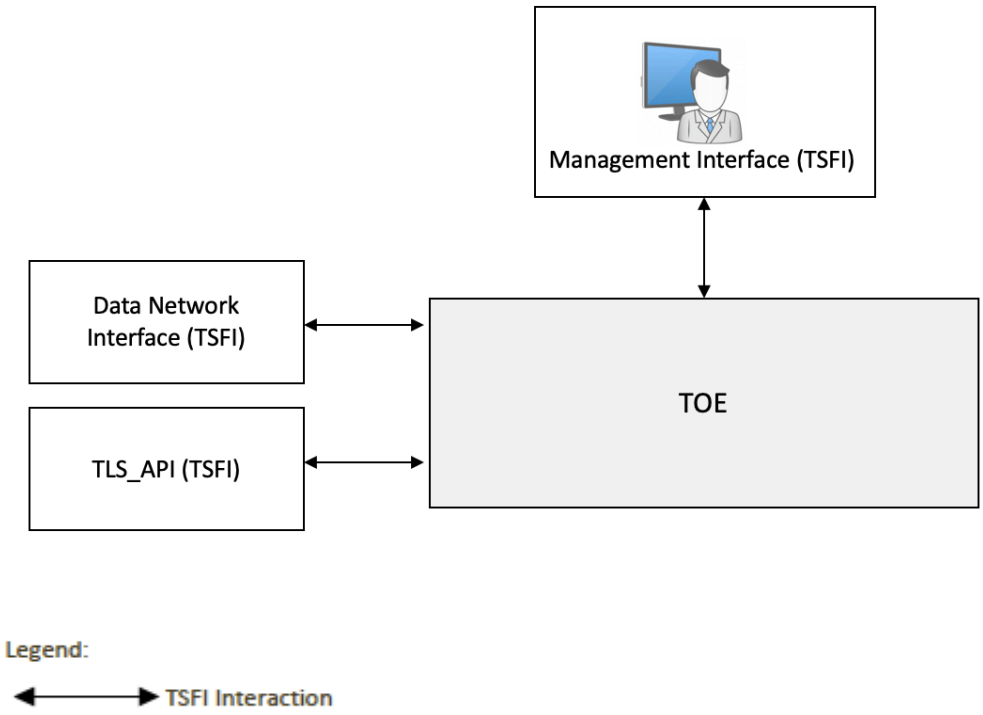
Information cannot flow among the internal and external networks unless it passes through the TOE.

1.7 Evaluated Configuration

39 The TOE is separated into various subsystems that provide the TOE Security Functions (TSFs).

40 The evaluated configuration of the TOE, shown in Figure 2 The TOE collects network traffic and subjects it to statistical and signature-based analysis, depending on configured security filters. If the analysis of collected network traffic indicates a potential intrusion attempt or the presence of malicious content in a packet, an action set associated with the detecting filter is triggered. The action set determines if the traffic is permitted or blocked. If traffic is permitted, an alert will be written to a TOE data log (specifically, the Event log). If traffic is blocked, an alert will also be written to the TOE Event log. Writing an alert to the TOE data log (specifically, the Event log) is always performed. In the evaluated configuration, action sets that block traffic always generate an alert. TOE users do not directly interact with this interface.

Figure 2 : Evaluated Deployment Configuration of the TOE



1.8 Delivery Procedures

41 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.

42 The TOE is delivered by Invisiron's authorized representative to the customer.

43 The TOE is wrapped in a plastic bag to provide resistance against moisture.

44 Each TOE is then enclosed in cardboard shipping boxes and sealed with tape that contain Invisiron logo.

45 A shipping label identifying the exact product (including the serial number for the included device) and the customer name is provided on the outside of the box.

46 Before TOE is delivered, the authorized representative from Invisiron will ensure that:

- 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 includes the TOE configuration, credentials configuration, IP address, zone upload and license generation.
- Default accounts and passwords are created by authorized representative from Invisiron

2 Evaluation

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

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

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

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

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

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

53 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

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

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

2.1.2 TOE Delivery

56 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.

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

2.1.3 Development

58 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.

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

60 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.

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

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

63 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

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

65 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.

66 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.

67 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.

68 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.

69 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

70 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.

71 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.

72 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.

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

74 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.

75 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.

76 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

77 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

78 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

79 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.

80 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 Management 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 Authorised User 3. To test that the TOE enforces the access control SFP to restrict the ability to change default, modify and delete the security attributes Administrator Account, Device Configuration and Users Account to Administrators. 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 detects an admin configurable positive integer [2 to 5] unsuccessful authentication attempts and When the unsuccessful authentication attempts has been [met], the TOE shall block usage of the TOE 6. To test that the TOE provides a mechanism to verify that secrets meet number of characters equal to or greater than 6 and less than or equal to 30 and any combination of upper- and lower-case letters, numbers 7. To test that the TOE performs the following management functions: Refer to objects listed in Section 5.3.21 of the ST	FIA_UID.2 FIA_UAU.2 FMT_SMR.1 FIA_ATD.1 FIA_AFL.1 FIA_SOS.1 FMT_SMF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_MOF.1 FDP_ACC.1 FDP_ACF.1 FPT_STM.1	Pass

	8. To test that the TOE enforces the access control SFP to restrict the ability to change default, modify, delete the security attributes [Admin Account, TOE Configuration, Users Account] to Admin and Authorised User 9. To test that the TOE enforce access control SFP to provide permissive default values for security attributes that are used to enforce the SFP. 10. To test that the TOE restricts the ability to modify the User Accounts to Admin and Authorised User 11. To test that the TOE restricts the ability to disable, enable and modify the functions of TOE Configurations to Admin and Authorised User		
F002 – Intrusion and Packet Content Detection System Data Network Interface	1. To test that the TOE able to collect network traffic from targeted IT System resources. At a minimum, the TOE shall be able to collect and record the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) Network Packet, Protocol, source address, destination address 2. To test that the TOE performs the following functions on all IDS data received: a) Analyse packet filtering, statistical, signature b) Record date and time of the result, type of result, identification of data source; and data destination,	IDS_SDC_EXT.1 IDS_ANL_EXT.1 IDS_RCT_EXT.1 IDS_RDR_EXT.1 IDS_STG_EXT.1 IDS_STG_EXT.2	Pass

	protocol and severity 3. To test that the TOE sends an alarm to the IDS data log and the notification contacts (configured for the filter triggered by the network traffic) and take the action configured for the filter triggered by the network traffic (Block/Permit the network traffic) when an intrusion is detected. 4. To test that the TOE provides the authorised users and admin with the capability to read and interpret the list of IDS data in a suitable manner 5. To test that the TOE manages IDS data storage exhaustion, overwrite the oldest stored IDS data and send an alarm if the storage capacity has been reached. 6. The TSF shall protect the stored IDS data from unauthorized deletion and modification		
F003 – Trusted Path TLS_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 authentication and other services for which trusted path is required	FTP_TRP.1	Pass

F004 – Security Audit Management Interface	1. To test that the TOE able to generate audit record of the following auditable events: a. Start-up and shutdown of the audit functions b. Low severity security incidents c. Medium severity security incidents d. High severity security incidents 2. To test that the TOE records within each audit record at least the following information; Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and 3. To test that the TOE provides the Admin and Authorised User 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

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

2.1.5.3 Vulnerability Analysis

82 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.

83 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

84 The penetration tests focused on:

a) Web vulnerability scan

b) Cross Site Scripting

c) Cross-site Request Forgery (CSRF)

d) Security Misconfiguration and Session Implementation

e) Backup or Unreferenced Files

f) Information Disclosure – Sensitive information in the generated HTML, hardcoded and locally stored on browser

g) Running services and SSL misconfiguration/vulnerabilities

h) Failure to restrict URL Access

i) Information Disclosure - Version

85 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

86 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

87 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 Invisiron Cyber Defence Platform 3.1.0 which is performed by Securelytics SEF.

88 Securelytics SEF found that Invisiron Cyber Defence Platform 3.1.0 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2.

89 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

90 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.

91 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.

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

3.2 Recommendation

93 It is strongly recommended that:

a) The users should make themselves familiar with the developer guidance provided with
b) The users must maintain the confidentiality, integrity and availability of security relevant
c) System Auditor should review the audit trail generated and exported by the TOE periodically.

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

Annex A References

A.1 References

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

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

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

[4] ISCB Product Manual, v1, CyberSecurity Malaysia, Dec 2019.

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

[6] Invisiron Cyber Defence Platform Security Target, Version 1.0, 13 March 2020.

[7] Evaluation Technical Report Invisiron CDP, Version 1.0, 28 March 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 ---