KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

CyberSecurity MALAYSIA
An agency under MOSTI

# C093 Certification Report

## DNSVault Intelligent Threat Protection version 5.0

File name: ISCB-5-RPT-C093-CR-v1
Version: v1
Date of document: 23 March 2018
Document classification: PUBLIC


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



CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999
www.cybersecurity.my

# C093 Certification Report

## DNSVault Intelligent Threat Protection version 5.0

23 March 2018

ISCB Department

**CyberSecurity Malaysia**

Level 5, Sapura@Mines,
No 7 Jalan Tasik,The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 Fax: +603 8992 6841
http://www.cybersecurity.my

# Document Authorisation

| | |
|---|---|
| ***DOCUMENT TITLE:*** | C093 Certification Report |
| ***DOCUMENT REFERENCE:*** | ISCB-5-RPT-C093-CR-v1 |
| ***ISSUE:*** | v1 |
| ***DATE:*** | 23 March 2018 |

| | |
|---|---|
| ***DISTRIBUTION:*** | UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION |

# Copyright and Confidentiality Statement



Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – 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 23 March 2018 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 associated certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (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 | 12 March 2018 | All | Initial draft of certification report |
| v1 | 16 March 2018 | All | 1st Revision of certification report |
| v1 | 23 march 2018 | All | Final version of certification report |

# Executive Summary

The Target of Evaluation (TOE) is DNSVault Intelligent Threat Protection version 5.0.

The TOE is a web application that has the ability to perform DNSVault Node management, DNS management, DNS Statistics and logs monitoring. By integrating DNSVault Analytic into the platform, the TOE able to revolutionize the way Admin view the raw data of the DNS statistics and logs providing advanced threat Intelligent protections such as malware detection and web filtering. It's also automatically monitor DNS and related service health and status and can predictively adjust capacity based on needs.

With DNSVault Intelligent Threat Protection, Administrators have a holistic and unified platform that empowers admins to control, secure and analyse every aspect of the DNS performance, security, agility and availability whether it is on premises, in data centres, or even in the cloud. Thus, by automating essential processes, eradicating solution silos and integrating into your existing ecosystem, mitigating risk proactively, every aspect of DNS is in context and leveraging DNS data for a truly intelligent threat protection.

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 (Ref [4]).

The evaluation was performed by Securelytics SEF (Security Evaluation Facility) and completed on 2 March 2018.

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 DNSVault Intelligent Threat Protection version 5.0 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

**Document Authorisation** ..... ii

**Copyright and Confidentiality Statement** ..... iii

**Foreword** ..... iv

**Disclaimer** ..... v

**Document Change Log** ..... vi

**Executive Summary** ..... vii

**Table of Contents** ..... viii

**Index of Tables** ..... ix

**Index of Figures** ..... ix

**1 Target of Evaluation** ..... 1

1.1 TOE Description ..... 1
1.2 TOE Identification ..... 1
1.3 Security Policy ..... 2
1.4 TOE Architecture ..... 2
1.4.1 Logical Boundaries ..... 3
1.5 Clarification of Scope ..... 4
1.6 Assumptions ..... 4
1.7 Evaluated Configuration ..... 4
1.8 Delivery Procedures ..... 5
1.9 Documentation ..... 5

**2 Evaluation** ..... 6

2.1 Evaluation Analysis Activities ..... 6
2.1.1 Life-cycle support ..... 6
2.1.2 Development ..... 7
2.1.3 Guidance documents ..... 8
2.1.4 IT Product Testing ..... 8

**3 Result of the Evaluation** ..... 12

3.1 Assurance Level Information ..... 12
3.2 Recommendation ..... 12

**Annex A References ..... 13**

A.1 References ..... 13
A.2 Terminology ..... 13
A.2.1 Acronyms ..... 13
A.2.2 Glossary of Terms ..... 14

# Index of Tables

Table 1: TOE identification ..... 1
Table 2: List of Acronyms ..... 13
Table 3: Glossary of Terms ..... 14

# Index of Figures

Figure 1: TOE Physical Boundaries ..... 3

# 1 Target of Evaluation

## 1.1 TOE Description

1 The TOE is a web application that has the ability to perform DNSVault Node management, DNS management, DNS Statistics and logs monitoring. By integrating DNSVault Analytic into the platform, the TOE able to revolutionize the way Admin view the raw data of the DNS statistics and logs providing advanced threat Intelligent protections such as malware detection and web filtering. It's also automatically monitor DNS and related service health and status and can predictively adjust capacity based on needs.

2 With DNSVault Intelligent Threat Protection, Administrators have a holistic and unified platform that empowers admins to control, secure and analyse every aspect of the DNS performance, security, agility and availability whether it is on premises, in data centres, or even in the cloud. Thus, by automating essential processes, eradicating solution silos and integrating into your existing ecosystem, mitigating risk proactively, every aspect of DNS is in context and leveraging DNS data for a truly intelligent threat protection.

3 The functionality defined in the Security Target (Ref [6]) that was subsequently evaluated is as follows:

- Security Audit
- Identification & Authentication
- Security Management
- Secure Communication

## 1.2 TOE Identification

4 The details of the TOE are identified in

5 Table 1 below.

Table 1: TOE identification

| | |
|---|---|
| **Evaluation Scheme** | Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme |
| **Project Identifier** | C093 |
| **TOE Name** | DNSVault Intelligent Threat Protection |
| **TOE Version** | version 5.0 |
| **Security Target Title** | DNSVault Intelligent Threat Protection Security Target |
| **Security Target Version** | Version 1.0 |
| **Security Target Date** | 15 February 2018 |
| **Assurance Level** | Evaluation Assurance Level 2 (EAL2) |

| | |
|---|---|
| **Criteria** | Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [2]) |
| **Methodology** | Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [3]) |
| **Protection Profile Conformance** | None |
| **Common Criteria Conformance** | CC Part 2 Conformant<br>CC Part 3 Conformant |
| **Sponsor** | DNSVAULT Sdn Bhd<br>No.29-2, Tingkat 2, Jalan Tukul N15/N,<br>Seksyen 15, 40200 Shah Alam, Selangor,<br>Malaysia |
| **Developer** | DNSVAULT Sdn Bhd<br>No.29-2, Tingkat 2, Jalan Tukul N15/N,<br>Seksyen 15, 40200 Shah Alam, Selangor,<br>Malaysia |
| **Evaluation Facility** | Securelytics SEF (Security Evaluation Facility)<br>A-19-06, Tower A, ATRIA SOFO SUITES, Jalan SS 22/23<br>47400 Damansara Jaya, , Petaling Jaya, Malaysia |

## 1.3 Security Policy

6 There are no organisational security policies that have been defined regarding the use of the TOE.

## 1.4 TOE Architecture

7 The TOE includes both logical and physical boundaries as described in Section 1.5.1 and 1.5.2 of the Security Target (Ref [6]).

8 The TOE architecture consists of the following components:

1) TOE:

   The Target of Evaluation (TOE) is DNSVault Intelligent Threat Protection version 5.0. The TOE is a web application that has the ability to perform DNSVault Node management, DNS management, DNS Statistics and logs monitoring.

2) TOE Users:

   There are two types of TOE users; Admin and Normal User. Refer to Section 5.2.4, Table 1 in Security Target (Ref [6]) for detail explanations on user's operation.

3) Web Browser:

A web browser is a software program that allows a user to locate, access, and display web pages. TOE Users (Admin and Normal User) interact with the TOE via a supported web browser stated in Section 1.4.3 of Security Target (Ref [6]).

4) Database:

A database is an electronic system that allows data to be easily accessed, manipulated and updated. a database is used as a method of storing, managing and retrieving data.

5) Operating System

Operating System is a software program that enables the computer hardware to communicate and operate with the computer software. The TOE requires an operating system to function. Refer to Section 1.4.3 of Security Target (Ref [6]) for minimum system requirement for operating system.

9 The TOE components can essentially be portrait as below:

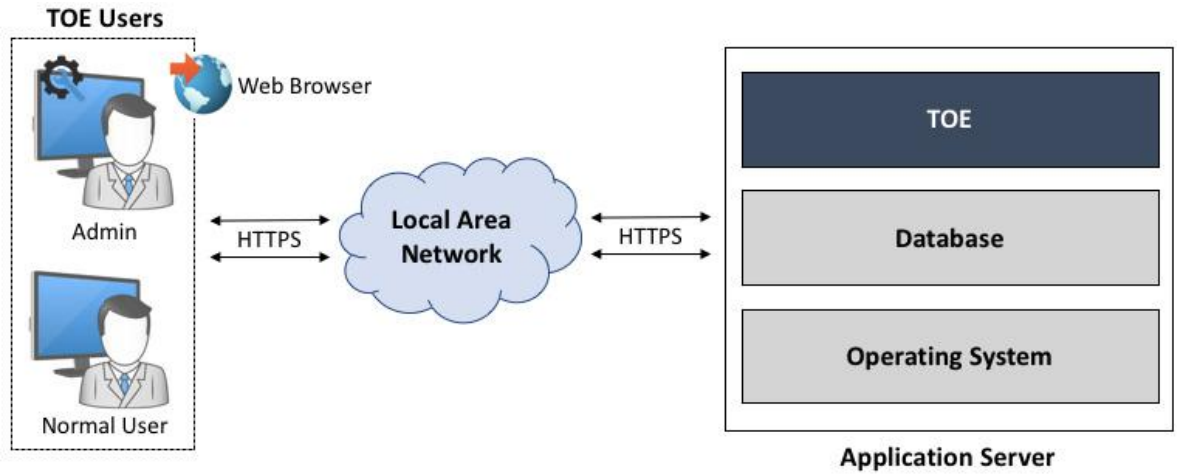


Figure 1: TOE Physical Boundaries

### 1.4.1 Logical Boundaries

10 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:

11 **Security Audit:** The TOE generates audit records for security events. The Admin has the ability to view/export the audit logs. Types of audit logs are:

- User/Admin login
- User/Admin logout
- Data modification by User/Admin

Only Admin has the capability to review these audit records via the web interface.

12 **Identification and Authentication:** All users are required to be identified and authenticated before any information flows are permitted. The TOE checks the credentials presented by the user at the login page against the authentication information stored in the database.

13 **Security Management:** The TOE contains various management functions to ensure efficient and secure management of the TOE. The TOE maintains role-based access control mechanisms to ensure that functions are restricted to those who have the privilege to access them. The system admin has the ability to create users' roles, who have privileged access to specific functions. The functions above are restricted based on this role.

14 **Secure Communication:** The TOE provides a secure SSL channel between the end-user and the TOE.

## 1.5 Clarification of Scope

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

16 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]).

17 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 requirement for using functions and services outside of the evaluated configuration.

## 1.6 Assumptions

18 This section summarises the assumptions regarding the operational environment and the intended usage of the TOE, as described in the Security Target (Ref [6]):

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

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

c) 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.

d) The platforms on which the TOE operate shall be able to provide reliable time stamps.

e) It is assumed that the appliance hosting the operating system and database are in a secure operating facility with restricted physical access and non-shared hardware.

## 1.7 Evaluated Configuration

19 As stated in the ST (Ref [6]), there are five (5) main components of the TOE that make up the evaluated configuration, namely the TOE itself, TOE Users, Web Browser, Database and Operating System.

20 The TOE components are deployed as configured in Figure 1.

21 The TOE also includes the components as the supporting hardware, software and/or firmware mentioned in section 1.4.3 of Security Target (Ref [6]).

## 1.8 Delivery Procedures

22 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.

23 The delivery procedures should consider, if applicable, issues such as:

- ensuring that the TOE received by the consumer corresponds precisely to the evaluated version of the TOE;
- avoiding or detecting any tampering with the actual version of the TOE;
- preventing submission of a false version of the TOE;
- avoiding unwanted knowledge of distribution of the TOE to the consumer: there might be cases where potential attackers should not know when and how it is delivered;
- avoiding or detecting the TOE being intercepted during delivery; and
- avoiding the TOE being delayed or stopped during distribution.

24 The TOE is delivered by an authorized representative to the customer. It is sealed in a box (along with the user manuals) using a packaging tape. Before the server is delivered, the following steps are performed by an Authorized Representative are as follows:

- 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 DNSVault's representative.
- Upon completion of installation and configuration of the TOE, customer needs to complete the Application Installation Acceptance & Sign-off.

25 All delivery process details are described in Section 2.3 of the Life Cycle documentation.

## 1.9 Documentation

26 It is important that the TOE is used in accordance with the guidance documentation in order to ensure secure usage of the product.

The guidance documentation provided by the developer to the end user act as guidance to ensure secure delivery, installation and operation of the product.

# 2 Evaluation

27 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [4]).

## 2.1 Evaluation Analysis Activities

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

- The evaluators' testing consisted of independent testing efforts, which comprise both functional and penetration test cases to address testing requirements for ATE_IND.2 and AVA_VAN.2 evaluation components.
- For functional testing, the focus was on testing the claimed security functionality (SFRs within the ST) through the interfaces specified in the functional specification (TSFI). For the penetration testing, the effort was limited to attacks that are commensurate to an attacker with equal or less than Basic attack potential. The testing approach for both testing commensurate with the respective assurance components (ATE_IND.2 and AVA_VAN.2).

### 2.1.1 Life-cycle support

#### 2.1.1.1 Configuration Management Capability

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

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

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

32 The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the CM documentation.

#### 2.1.1.2 Configuration Management Scope

33 The evaluators confirmed that the configuration list includes the following set of items:

- the TOE itself;
- the parts that comprise the TOE; and
- the evaluation evidence required by the SARs in the ST.

34 The evaluators confirmed that the configuration list uniquely identifies each configuration item.

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

#### 2.1.1.3 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.

### 2.1.2 Development

#### 2.1.2.1 Architecture

37 The evaluators examined the security architecture description and determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

38 The security architecture description describes the security domains maintained by the TSF.

39 The initialisation process described in the security architecture description preserves security.

40 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

#### 2.1.2.2 Functional Specification

41 The evaluators examined the functional specification and determined that:

- the TSF is fully represented,
- it states the purpose of each TSF Interface (TSFI),
- the method of use for each TSFI is given,

42 The evaluators also examined the presentation of the TSFI and determined that:

- it completely identifies all parameters associated with every TSFI,
- it completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI,

43 The evaluators also confirmed that the developer supplied tracing that links the SFRs to the corresponding TSFIs.

#### 2.1.2.3 TOE Design Specification

44 The evaluators examined the TOE design and determined that the structure of the entire TOE is described in terms of subsystems. The evaluators also determined that all subsystems of the TSF are identified. The evaluators determined that interactions between the subsystems of the TSF were described.

45 The evaluators examined the TOE and determined that each SFR supporting or SFR-non-interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is not SFR-enforcing.

46 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

47 The evaluators examined the TOE design and determined that it provides a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

48 The evaluators determined that 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.

49 The evaluators determined that all SFRs were covered by the TOE design, and concluded that the TOE design was an accurate instantiation of all SFRs.

### 2.1.3 Guidance documents

#### 2.1.3.1 Operational Guidance

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. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

51 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

52 The evaluators examined the operational user guidance (in conjunction with other evaluation evidence and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

53 The evaluators determined that the operational user guidance 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.

54 The evaluators found that the operational user guidance is clear and reasonable.

#### 2.1.3.2 Preparation Guidance

55 The evaluators examined the provided delivery acceptance documentation and determined that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

56 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.

57 The evaluators performed all user procedures necessary to prepare the TOE during testing and determined that the TOE and its operational environment can be prepared securely using only the supplied preparative user guidance.

### 2.1.4 IT Product Testing

58 Testing at EAL2 consists of assessing developer tests, performing independent functional tests, and conducting penetration tests. The TOE testing was conducted by the evaluators of

Securelytics SEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

#### 2.1.4.1 Assessment of Developer Tests

59 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, 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).

#### 2.1.4.2 Independent Functional Testing

60 At EAL2, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan and creating test cases that are independent of the developer's tests.

61 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

| Test ID | Description | SFRs |
|---|---|---|
| F001 - Identification and Authentication Security Management ADMIN Interface USER Interface | • To test that each user to be successfully authenticated and identified before allowing any other TSF-mediated actions on behalf of that user.<br>• To test that the TOE maintains the roles Admin and Normal User.<br>• 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, Users Account to Admin.<br>• To test that the TOE maintains the following list of security attributes belonging to individual users; Username, Password, User role, User Account<br>• To test that the TOE enforce access control SFP to provide permissive default values for security attributes that are used to enforce the SFP.<br>• To test that the TOE performs the following management functions: Refer to objects listed in Section 5.2.13 of the ST (Ref [6])<br>• To test that the TOE restricts the ability to modify the User Accounts to Admin<br>• To test that the TOE enforces the access control SFP on objects listed in Section 5.2.4 of the ST (Ref [6])<br>• To test that If the Admin and Normal User are successfully authenticated accordingly, then | FIA_ATD.1<br>FIA_UID.2<br>FIA_UAU.2<br>FMT_MSA.1<br>FMT_MSA.3<br>FMT_MTD.1<br>FMT_MOF.1<br>FMT_SMF.1<br>FMT_SMR.1<br>FDP_ACC.1<br>FDP_ACF.1 |

| Test ID | Description | SFRs |
|---|---|---|
| | access is granted based on privilege allocated and If the Admin and Normal User are not authenticated successfully, therefore, access permission is denied<br>• To test that the TOE restricts the ability to disable, enable and modify the behaviour of the functions of TOE Configurations to Administrators | |
| F002 – Trusted Path SSL_API | • 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<br>• To test that the TOE permits remote users to initiate communication via the trusted path<br>• To test that the TOE requires the use of the trusted path for initial user authentication and all further communication after authentication | FTP_TRP.1 |
| F003 – Security Audit ADMIN Interface | • To test that the TOE able to generate audit record of the following auditable events:<br>a. Event date<br>b. Event associated with the user<br>c. Activity type<br>d. Existing data and;<br>e. Change data<br>• To test that the TOE record within each audit record at least the following information:<br>a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and<br>b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST (none).<br>• 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 | FAU_GEN.1<br>FAU_SAR.1 |

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

#### 2.1.4.3 Penetration Testing

63 The evaluators performed 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, and TOE design and security architecture description.

64 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 (elapsed time);

b) Specialist technical expertise required (specialist 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.

65 The penetration tests focused on:

a) SQL Injection

b) Cross Site Scripting

c) Cross-site Request Forgery (CSRF)

d) Security misconfiguration

e) Failure to restrict URL Access

f) Information Disclosure

g) Directory Traversal

66 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]).

#### 2.1.4.4 Testing Results

67 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target (Ref [6]) and its functional specification. In addition, the documentation supplied as evidence for the EAL2 with Common Criteria evaluation of the TOE was analysed to identify possible vulnerabilities.

# 3 Result of the Evaluation

68 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 DNSVault Intelligent Threat Protection version 5.0 performed by Securelytics SEF.

69 Securelytics SEF found that DNSVault Intelligent Threat Protection version 5.0 upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2).

70 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

71 EAL 2 provides assurance by a full Security Target and analysis of the SFRs in that Security Target (Ref [6]), using functional and interface specifications, guidance documentation and a basic description of the design and architecture of the TOE, to understand the security behaviours of the TOE.

72 The analysis is supported by an 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.

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

## 3.2 Recommendation

74 The following recommendations are made:

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

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

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

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

# Annex A References

## A.1 References

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

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] ISCB Product Certification Schemes Policy (Product_SP), v1a, CyberSecurity Malaysia, June 2017.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v1, June 2017.

[6] DNSVault Intelligent Threat Protection Security Target, Version 1.0, 15 February 2018

[7] T1709-4-ETR 1.0, Evaluation Technical Report – DNSVault Intelligent Threat Protection, Version 1.0, 2 March 2018

## A.2 Terminology

### A.2.1 Acronyms

Table 2: 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 |

| Acronym | Expanded Term |
|---|---|
| TOE | Target of Evaluation |
| EAL | Evaluation Assurance Level |
| SEF | Security Evaluation Facility |
| MyCB | Malaysia Certification Body |
| ST | Security Target |
| SFRs | Security Functional Requirements |
| TSF | TOE Security Function |
| TOE | Target of Evaluation |

### A.2.2 Glossary of Terms

Table 3: 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**. |

| Term | Definition and Source |
|---|---|
| Certifier | The certifier responsible for managing a specific certification task. |
| Evaluator | The evaluator responsible for managing the technical aspects of a specific evaluation task. |
| Maintenance Certificate | The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme. |
| National Interpretation | An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only. |
| Security Evaluation Facility | An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy |
| Sponsor | The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer. |

--- END OF DOCUMENT ---