CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

C023 Certification Report
AssetCentral 4.0.0

File name: ISCB-5-RPT-C023-CR-v1a
Version: v1a
Date of document: 16 January 2012
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 8, Block A
Mines Waterfront Business Park
No 3 Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
T +603 8946 0999
F +603 8946 0888
www.cybersecurity.my

Securing Our Cyberspace

C023 Certification Report

AssetCentral 4.0.0

16 January 2012

ISCB Department

CyberSecurity Malaysia

Level 8, Block A, Mines Waterfront Business Park,

No 3 Jalan Tasik, The Mines Resort City

43300 Seri Kembangan, Selangor, Malaysia

Tel: +603 8946 0999 Fax: +603 8946 0888

http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C023 Certification Report - AssetCentral 4.0.0
DOCUMENT REFERENCE:	ISCB-5-RPT-C023-CR-v1a
ISSUE:	v1a
DATE:	16 January 2012

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 8, Block A,

Mines Waterfront Business Park,

No 3 JalanTasik, The Mines Resort City,

43300 Seri Kembangan

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 January 2012, 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 at www.commoncriteriaportal.org).

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 (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 3 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 3 (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
v1	6 January 2012	All	Final released.
v1a	16 January 2012	Page iv	Add the date of the certificate.

Executive Summary

AssetCentral 4.0.0 (hereafter referred as AssetCentral) from Authentic Venture Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

The TOE is an automated asset management system. AssetCentral automates the protection of managed systems against unauthorized software or hardware installations and removal and having unlicensed software-related vulnerabilities. The TOE allows users to monitor compliance throughout an organization for their IT asset.

AssetCentral comprises a server component and agents, known as AssetXplorer agents, which are deployed on computers throughout the enterprise. AssetXplorer agents send information about each computer to AssetCentral Server. AssetCentral Server consolidates all the information and allows administrators and custom-role users to view them through a web interface. AssetXplorer is part of the TOE.

The security features within the scope of the evaluation includes:

- **Auditing** – AssetCentral provides auditing capabilities.
- **Identification and Authentication** – AssetCentral provides identification and authentication of human users of the TOE. It also provides identification of AssetXplorer that are installed in managed devices.
- **Security Management** - AssetCentral provides security management through the use of the Web Administration Interface. Through the enforcement of the AssetCentral Access Control Policy, the ability to manage various security attributes is controlled.
- **User Data Protection** - AssetCentral provides its own access control between subjects and objects covered by the AssetCentral Access Control Policy.
- **Secure Communications** - AssetCentral is able to protect the user data from disclosure and modification when the scanned data is sent from AssetXplorer to AssetCentral Server.

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

This report describes the findings of the IT security evaluation of AssetCentral, to the Common Criteria (CC) evaluation assurance level of EAL 1 and that the evaluation was conducted in accordance with relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme. The evaluation was performed by the STRATSEC.NET SDN BHD (stratsec) Security Evaluation Facility (STRATSEF) and was completed on 24 November 2011.

Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the AssetCentral evaluation meets all the conditions of the Arrangement

on the Recognition of Common Criteria Certificates and that the product will be listed on the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement at www.commoncriteriaportal.org).

It is the responsibility of the user to ensure that the AssetCentral meets their requirement and security needs. It is recommended that prospective users of the AssetCentral refer to the ST (Ref [6]), and read this Certification Report prior to deciding whether to purchase and deploy the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), AssetCentral 4.0.0 (hereafter referred as AssetCentral) is an automated asset management system. AssetCentral automates the protection of managed systems against unauthorised software or hardware installations and removal, and having unlicensed software-related vulnerabilities. The TOE allows users to monitor compliance throughout an organisation for their IT asset.

2 AssetCentral comprises a server component (AssetCentral Server version 4.0) and agents, known as AssetXplorer agents (version 5.0), which are deployed on computers throughout the enterprise. AssetXplorer agents send information about each computer to AssetCentral Server. AssetCentral Server consolidates all the information and allows administrators and custom-role users to view them through a web interface. AssetXplorer is part of the TOE.

3 The security functionality that is within the scope of the evaluation includes:

a) **Auditing:** The TOE provides auditing capabilities for identification and authentication of users, when the scanning of the managed devices is done, when a new managed device is added or deleted.

b) **User data protection:** The TOE provides its own access control between subjects and objects covered by the AssetCentral Access Control Policy. Different roles will have different privileges as enforced by the Access Control Policy.

c) **Identification and Authentication:** The TOE provides identification and authentication of users before allowing any TOE security function mediated actions.

d) **Security Management:** The TOE provides security management through the use of the Web Interface. Through the enforcement of the AssetCentral Access Control Policy, the ability to manage various security attributes is controlled.

e) **Secure Communication:** The TOE provides a secure communication channel between AssetXplorer and AssetCentral Server when scanned data is sent from the AssetXplorer.

1.2 TOE Identification

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

Table 1: TOE Identification

Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C023

TOE Name	AssetCentral
TOE Version	AssetCentral 4.0.0 consist of • AssetXplorer (version 5.0) • AssetCentral Server (version 4.0)
Security Target Title	Authentic Venture AssetCentral Security Target
Security Target Version	1.1
Security Target Date	14 November 2011
Assurance Level	Evaluation Assurance Level 1 (EAL1)
Criteria	Common Criteria July 2009, Version 3.1, Revision 3
Methodology	Common Methodology for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL1
Sponsor and Developer	Authentic Venture Sdn Bhd Block U, UPM-MTDC, Incubation Center One, University Putra Malaysia, 43400 Serdang, Selangor MALAYSIA
Evaluation Facility	STRATSEC.NET SDN BHD known as STRATSEF

1.3 Security Policy

5 In order to provide user data protection, the TOE enforces an access control policy on protected scan data of the managed devices. Only authorised users have permission to perform the requested actions on the scan data after they identify and authenticate to the TOE.

6 Through the web based interface of the AssetCentral Server, Administrator can configure user access control policy, mapping of users to roles, groups as well as modifying the user accounts. By default, no policy is set or member computers are assigned when a group is created.

7 The detail of the access control policy is described in Section 4 and Section 5 of the Security Target (Ref [6]).

1.4 TOE Architecture

8 The Security Target defines clearly both logical and physical boundaries of the TOE.

9 Figure 1 below provides the major architectural components that comprise the entire implementation of the AssetCentral and identifies all the major supporting elements that combine to deliver the system. The TOE comprises the AssetCentral Server (version 4.0) and AssetXplorer Agents (version 5.0).

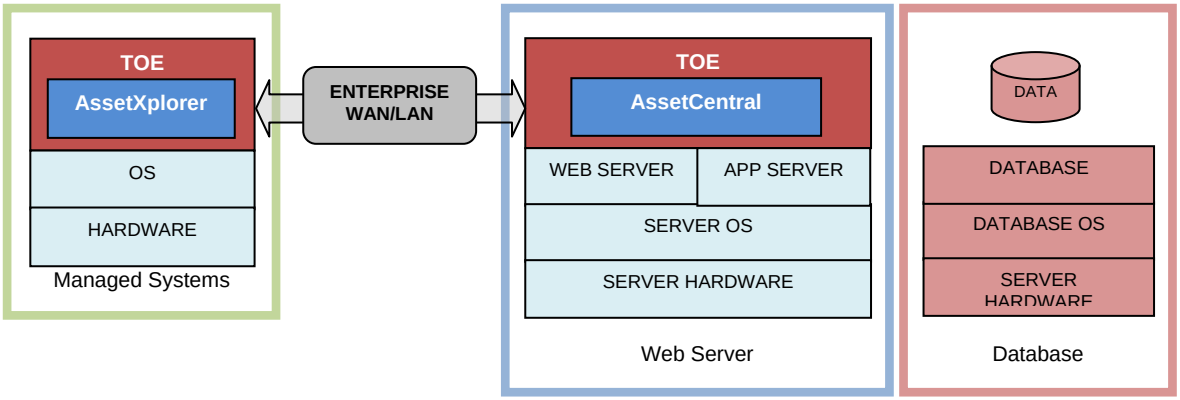

Figure 1: AssetCentral Architecture

10 AssetCentral Server is a collection of web components on a web server. All computer inventory retrieved from AssetXplorer Agents is sent to AssetCentral Server and stored in the third party database. The web interface of AssetCentral Server ties all these components together to provide a system-wide view of all the computers on the network.

11 Through the web interface of the AssetCentral Server, the Administrators can customise user account creation and modify role-based policy. The web interface of the AssetCentral Server also allows an authorised user to view information about the managed devices assigned to them.

12 AssetXplorer Agents are installed on every computer that is to be managed under AssetCentral Server. AssetXplorer scans the local host computer and compiles a full computer inventory; both hardware and software. The information is sent from the agent to AssetCentral Server through a secure channel.

1.5 Clarification of Scope

13 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, personnel and communication security in accordance with administrator guidance that is supplied with the product. 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) **Auditing.** The TOE provides auditing capabilities on:

   i) the success or failure of the identification and authentication of users,

   ii) added or removed of a managed device to the system, and

iii) when the scanned data is sent from the AssetXplorer to the TOE.

The TOE relies on the underlying operation system for reliable time stamps. It is able to associate each event to the user or managed devices.

The TOE also provides the capabilities for administrators and authorised custom-role users to view the audit records on the web interface. Only administrator can enable or disable the auditing function.

b) **User data protection.** The TOE enforces an access control policy on the features, functions and pages to the scan data of the managed devices. After a user identifies and authenticates to the TOE, the TOE will permit the user to access the features, functions and pages if the user role and group has permission to perform the requested action on the scan data.

There are 2 types of user for the TOE: administrator and custom-role user. Each type of user has different access rights and privileges to features, functions and pages on the scan data of the managed devices.

c) **Identification and Authentication.** The TOE requires all users to identify and authenticate themselves before performing any TOE security function mediated actions on behalf of the user. During login, the TOE will check the credentials presented by the user through the web interface against the authentication information in the database. After a successful identification and authentication, they are assigned a role which has been defined by the AssetCentral administrator.

d) **Security Management.** The TOE contains various management functions to ensure efficient and secure management of the TOE as follows:

i) user management – administrator and custom-role (given admin function) are responsible to modify the access control list, mapping of users to roles, groups as well as modifying the user accounts. Administrator and custom-role users are 2 roles within the TOE to ensure that the functions are restricted to only those users that need to have access to privileged functions. The administrator is responsible to create and set the privileges of the custom-role users.

ii) permission management to scan data – the TOE allows administrator and custom-role (given admin function) users to change the default value of the TOE security function (TSF) data and security attributes of the TOE.

e) **Secure Communication.** Communication between AssetXplorer and AssetCentral Server is always initiated by the AssetXplorer. The TOE provides a secure communication channel between AssetXplorer and AssetCentral Server when scanned data is sent from the AssetXplorer to protect the data from disclosure and modification. The communication session is secured (encrypt and decrypt) using a passkey with a unique Authentic Venture's developed algorithm that is auto generated by the TOE.

14 Potential consumers of the TOE are advised that some functions and services may not have been evaluated as part of the evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

15 Functions and services which are not included in the scope of the evaluation, but these IT environment are required to ensure that the TOE perform in its intended operations, are as follows:

a) Web server – Windows Server 2003 with Microsoft IIS

b) Database – Microsoft SQL Server 2005

c) Microsoft .NET Framework Version 2.0

d) Client browsers

16 The secure installation of the operational environment is an important element in ensuring that the TOE is initialised correctly and protection from tampering.

1.6 Assumptions

17 This evaluation was performed at EAL1. Therefore, no assumptions for the TOE were defined in the Security Target (Ref [6]).

1.7 Evaluated Configuration

18 This section describes the configurations of the TOE that is included within the scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented preparative and operational user guidance, and only by trustworthy staff.

19 The TOE is a configured based on secure installation guidance as following:

a) Authentic Venture AssetCentral EAL1 Evaluation Guidance Documents (Ref [9])

b) SYSTEM MANUAL – PJ017 – ONLINE IT ASSET MANAGEMENT SYSTEM (AssetXplorer) (Ref [10])

c) SYSTEM MANUAL – PJ017 – ONLINE IT ASSET MANAGEMENT SYSTEM (AssetCentral) (Ref [11])

1.8 Delivery Procedures

20 This section aims to provide direction on the methods used to deliver the TOE to consumers or users of the product.

21 AssetCentral Server, which is a web portal for administrators and users to manage the system, resides at Authentic Venture Sdn. Bhd. In this case, the user can access AssetCentral Server via http://www.assetcentral.com.my/sys/login.aspx. The version of AssetCentral Server can be determined at the bottom of the web portal at the login page.

22 AssetXplorer Agent, which will be installed in the managed device, can be downloaded from AssetCentral web portal after successful authentication and presenting the company ID. The version of AssetXplorer can be determined during the installation where it will be displayed at the installation screen.

23 However, for this EAL1 evaluation, TOE Delivery (ALC_DEL) is not included in the scope of the evaluation. Thus, developer did not provide any documentation on TOE delivery and the evaluators did not verify any TOE delivery process.

1.9 Documentation

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

25 The following guidance document is provided by the developer to the end user as guidance to ensure secure usage and operation of the product:

a) USER MANUAL – ASSETCENTRAL FOR E-IT ASSET VERSION 2.0 (Ref [8])

b) Authentic Venture AssetCentral EAL1 Evaluation Guidance Documents (Ref [9])

26 The following guidance document are provided to the administrator as guidance for secure installation of the product:

a) Authentic Venture AssetCentral EAL1 Evaluation Guidance Documents (Ref [9])

b) SYSTEM MANUAL – PJ017 – ONLINE IT ASSET MANAGEMENT SYSTEM (AssetXplorer) (Ref [10])

c) SYSTEM MANUAL – PJ017 – ONLINE IT ASSET MANAGEMENT SYSTEM (AssetCentral) (Ref [11])

2 Evaluation

27 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 1 (EAL1). The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

29 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators confirmed that the configuration list which includes the TOE and the evaluation evidence were clearly and uniquely labelled.

2.1.2 Development

30 The evaluators analysed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces (TSFIs), and how the TSF implements the security functional requirements (SFRs).

2.1.3 Guidance documents

31 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it's sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

2.1.4 IT Product Testing

32 Testing at EAL1 consists of performing independent function test, and performing penetration tests. The formal testing was conducted by STRATSEF at stratsec lab in Plaza Sentral, Kuala Lumpur where it was subjected to an independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Independent Functional Testing

33 At EAL1, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining functional and guidance documentation, and creating test cases to verify the behaviour of the TOE.

34 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The result of the independent tests developed and performed by the evaluators to verify the TOE functionality are as follows:

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
To verify the auditable events are recorded with reliable time stamps.	FAU_GEN.1 Audit data generation	Web interface. AssetXplorer Interface. Storage Database Interface.	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE is able to associate each auditable event with identity of the user caused the event.	FAU_GEN.2 User identity association	Web interface. AssetXplorer Interface. Storage Database Interface.	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE is able to read all audit information records using administrator and authorized custom user role.	FAU_SAR.1 Audit Review	Web interface. Storage Database Interface. Authentication Database Interface.	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE shall restrict all users read access to audit records, except those users that have been granted explicit read-access.	FAU_SAR.2 Restricted Audit Review	Web interface. Storage Database Interface. Authentication Database Interface.	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE shall control the access of reading scan reports of individual managed devices using administrator and custom (role defined by AssetCentral administrator)	FDP_ACC.1 Subset access control	Web interface. Storage Database Interface. Authentication Database Interface.	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE shall control the access right	FDP_ACF.1 Security attribute based	Web interface.	**PASS**. The result shows

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
for device scan reports based on assigned group and managed devices.	access control	Storage Database Interface. Authentication Database Interface.	that the TOE functions as per claims.
To test that the TOE shall maintain the security attributes associate with individual user such as user identity, roles, assigned access rights, assigned group and assigned managed devices.	FIA_ATD.1 User attribute definition	Web Interface	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE require user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.	FIA_UAU.2 User authentication before any action	Web interface. Authentication Database Interface.	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE require user to be identified before allowing any other TSF-mediated actions on behalf of that user.	FIA_UID.2 User identification before any action	Web interface. Authentication Database Interface.	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE shall restrict the ability to determine the behaviour of, disable, enable, and modify the behaviour of the audit functions based on authorize administrator or custom user and user group.	FMT_MOF.1 Management of security function behaviour	Web Interface.	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE shall Enforce Access Control to restrict the ability to query, modify, delete and create the security attributes using Authorized administrator and custom (role defined by AssetCentral	FMT_MSA.1 Management of security attributes	Web Interface.	**PASS**. The result shows that the TOE functions as per claims.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
administrator).			
To test that the TOE shall enforce the Access Control that provides restrictive default values for security attributes. The administrator and authorized custom user role shall specify alternative initial values to override the default values when an object or information is created.	FMT_MSA.3 Static attribute initialisation	Web Interface.	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE shall capable of performing the management functions.	FMT_SMF.1 Specification of management functions	Web interface. Authentication Database Interface.	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE shall capable of performing the following management functions.	FMT_SMR.1 Security roles	Web interface. Authentication Database Interface.	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE shall protect data when it is transmitted between separate AssetXplorer and AssetCentral Server.	FPT_ITT.1 Basic internal TSF data transfer protection	AssetXplorer Interface.	**PASS**. The result shows that the TOE functions as per claims.

35 All tests performed by the evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.2 Penetration Testing

36 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, and functional specification.

37 From the vulnerability analysis, the evaluators conducted penetration testing to determine whether potential vulnerabilities could be exploited in the intended operating environment of the TOE, to attack 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.

38 The penetration tests focused on :

a) Injection attacks;
b) Insecure Direct Object References;
c) Security misconfiguration;
d) Failure to restrict URL access;
e) Malicious file execution;
f) Information disclosure.

39 The results of the penetration testing note that there is no exploitable vulnerability and/or residual vulnerability found. However, it is important to ensure that the TOE environment have been correctly configured, patched and hardened.

2.1.4.3 Testing Results

40 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

41 Based on the results of penetration testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

3 Results of the Evaluation

42 After due consideration during the oversight of the evaluation execution by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of AssetCentral performed by the stratsec Security Evaluation Facility which known as STRATSEF.

43 STRATSEF found that AssetCentral upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level EAL1.

44 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 undiscovered in its claimed security functionality. This risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

45 EAL1 provides a basic level of assurance by a limited Security Target and an analysis of the security functions in that Security Target, using a functional and interface specification and guidance documentation, to understand the security behaviour.

46 The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TOE security functions.

47 EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

48 This EAL provides a meaningful increase in assurance over unevaluated IT.

3.2 Recommendation

49 In addition to ensure secure usage of the product, below are additional recommendations for AssetCentral users:

a) Those responsible for the AssetCentral Server and AssetXplorer must install, configured and set up in accordance with the preparative and operational guidance, and only by trustworthy staff. They must ensure that those parts of AssetCentral and its platform that are critical to security policy are protected from any physical attack.

b) Those responsible for AssetCentral must ensure that no untrusted software shall be installed on the machines the AssetCentral is installed on.

c) Those responsible for administrating the AssetCentral Server shall ensure that the databases in the environment have been correctly configured according to the principle of least privilege.

d) Those responsible for the AssetCentral Server must ensure that the IT environment provides the AssetCentral Server with appropriate physical security.

e) Those responsible for administrating the AssetCentral Server must ensure that the administrator who manages the server is not hostile and is competent and that all management of the server is performed through the management interfaces of the server and not through the underlying environment.

f) Those responsible for AssetCentral should periodically perform testing to confirm that all vulnerabilities have been suitably addressed.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[4] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1, December 2009.

[6] Authentic Venture AssetCentral EAL1 Security Target, v1.1, 14 November 2011.

[7] Evaluation Technical Report EAL1 Evaluation of AssetCentral, version 1.1, 24 November 2011.

[8] USER MANUAL – ASSETCENTRAL FOR E-IT ASSET VERSION 2.0, v 2.0.0 Draft 2, 8 June 2009.

[9] Authentic Venture AssetCentral EAL1 Evaluation Guidance Documents, v0.4, 14 November 2011.

[10] SYSTEM MANUAL – PJ017 – ONLINE IT ASSET MANAGEMENT SYSTEM (AssetXplorer), v 4.0.0, 11 August 2009.

[11] SYSTEM MANUAL – PJ017 – ONLINE IT ASSET MANAGEMENT SYSTEM (AssetCentral), v 3.0.0, 11 August 2010.

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology (ISO/IEC 18045)
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body

Acronym	Expanded Term
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
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
Administrator	The system administrator with privileged system access. This role can control the deployment and operation of the AssetCentral capability within an organisation.
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.

Term	Definition and Source
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.
Certifier	The certifier responsible for managing a specific certification task.
Custom Role	The Administrator can define one or more additional controlling roles with varying levels of privilege and access to the system.
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.
Managed Device	Any device or system that has the AssetXplorer agent installed and operating on it.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Scan Data	Data collected by AssetXplorer related to the configuration of the managed device on which the agent is installed.
Scan Report	A human readable output of the scan data presented for the Administrator to view the results and current status of managed devices.
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.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE
Unauthorized users	Unauthorized users can mean a legitimate user with access rights to certain web resource, an external entity that has no rights to any protected web resource/data.
Users	It means any entity (human user or external IT entity) outside the TOE that interacts with the TOE. In this case, there are end users (Administrator, Supervisor and Employee, Super Administrator) of the TOE access the TOE through a web browser as well as Super Administrators who are also developers of PHP modules that use the TOE underlying functions.

Term	Definition and Source
User data	Data created by and for the user, that does not affect the operation of the TSF
TSP	TOE Security Policy, a set of rules that regulate how assets are managed, protected and distributed.

--- END OF DOCUMENT ---