National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

AlienVault USM for Government v4.12 and RT Logic CyberC4:Alert v4.12

Report Number: CCEVS-VR-VID10548
Dated: October 29, 2015
Version: 1.0 Draft

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Patrick W. Mallett

Paul A. Bicknell

Bradford O'Neill

Common Criteria Testing Laboratory

Iain Holness

Nithya Rachamadugu

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the AlienVault USM for Government v4.12 Security Target.

Table of Contents

1. Executive Summary 5

2. Identification 6

3. The Scope of Evaluation 7

3.1. Physical Boundary 7

3.2. Logical Boundary 7

3.2.1. Security Audit 7

3.2.2. Cryptographic Support 7

3.2.3. User Data Protection 8

3.2.4. Identification and Authentication Functions 8

3.2.5. Security Management Functions 8

3.2.6. Protection of Security Functions 8

3.2.7. TOE Access 9

3.2.8. Trusted Path/Channels 9

3.3. Excluded Functionality 9

3.4. Secure Usage Assumptions 10

4. Architectural Information 11

5. Documentation 13

5.1. User Documentation 13

6. IT Product Testing 14

6.1. Developer Testing 14

6.2. Evaluator Independent Testing 14

7. Results of Evaluation 15

8. Validators Comments/Recommendations 16

9. Glossary 17

9.1. Acronyms 17

9.2. Terminology 17

10. Bibliography 22

List of Figures

Figure 1: TOE Boundary 11

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product *AlienVault USM for Government v4.12 and RT Logic CyberC4:Alert v4.12* as defined in the *AlienVault USM for Government, Version 4.12 and RT Logic CyberC4:Alert v4.12 Security Target v2.2*. It presents the evaluation results, their justifications, and the conformance results. The validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either express or implied.

CyberC4:Alert is an OEM version of USM for Government. The products are identical in terms of hardware, code, functionality. There are no differences between the two. CyberC4:Alert is simply rebranded under RT Logic's product offerings using the same documentation for as USM for Government v4.12.

The Target of Evaluation (TOE) is a network device as defined by the *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1: "*A network device is a device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise".* The TOE claims exact compliance to this protection profile.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL) and was completed in October 2015. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The TOE has been evaluated using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the Protection Profile for Network Devices (NDPP) with Errata #3 and all applicable Technical Decisions.

This Validation Report applies only to the specific version of the TOE operating in the specific evaluated configuration. The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on the web site www.niap-ccevs.org.

2. Identification

Target of Evaluation:	AlienVault USM for Government v4.12 and RT Logic CyberC4:Alert v4.12
Evaluated Platforms:	AlienVault USM for Government v4.12
ST Title:	AlienVault USM for Government, Version 4.12 and RT Logic CyberC4:Alert v4.12 Security Target
Developer:	AlienVault
CCTL:	CygnaCom Solutions 7925 Jones Branch Dr, Suite 5400 McLean, VA 22102-3321
Evaluators:	Iain Holness Nithya Rachamadugu
Validation Scheme:	National Information Assurance Partnership CCEVS
Validators:	Patrick W. Mallett Paul A. Bicknell Bradford O’Neill
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1 R4, September 2012
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 R4, September 2012
PP Identification:	US Government Protection Profile for Network Devices, Version 1.1, 8 June 2012 with Errata 3

3. The Scope of Evaluation

3.1. *Physical Boundary*

The physical boundary of the TOE is the hardware appliance. The TOE’s hardware is based on an Intel Quad-Core Xeon E5 blade server running Debian “Wheezy” 7.8 based on a Linux 3.4 kernel.

3.2. *Logical Boundary*

The logical scope of the TOE is defined by implemented security functions. These security functions are as follows:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

3.2.1. Security Audit

The TOE generates audit records related to cryptographic functionality, identification and authentication, and management actions. For each security relevant event, the TOE records the date and time, the type of event, the subject identity, and the outcome of the event logged. Auditing is enable by default. The TOE also implements timestamps to ensure that reliable audit information is available. The logs can be accessed through the appropriate menu of the Web Interface. The TOE can be configured to duplicate audit messages to an external Syslog Server.

3.2.2. Cryptographic Support

The TOE implements a cryptographic module that performs the following cryptographic operations:

- Secure channel with the following parameters:
    - TLS 1.0 protocol
    - TLS_RSA_WITH_AES_128_CBC_SHA
      TLS_RSA_WITH_AES_256_CBC_SHA
- Random Bit Generation using CTR_DRBG (AES-256)

The TOE uses the cryptographic module to manage session-based plaintext secrets stored in the volatile memory. After the session termination when the secrets are no longer needed, a function call overwrites contents with zeros. The TOE requires a separate, administrator-initiated procedure to clear long-term plaintext secrets from the non-volatile memory.

3.2.3. User Data Protection

The TOE implements a residual information clearing mechanism as part of network packet processing. Ingress packets are stored in the managed buffer that allocates dedicated memory space to each packet. Once the packet has been processed, the memory used for that packet is returned back to the pool for reuse. As a result, residual data is never transmitted from the TOE.

3.2.4. Identification and Authentication Functions

The TOE uses a Role-Based Access Control (RBAC) structure for restricting system access. Before any other action, each user is identified with a login name and authenticated with a password. Each authorized user is associated with an assigned role and specific permissions that determine their access to TOE features.

User role profiles are defined to provide two axes of permissions:

- Functions that a role can access within the system
- Assets that are accessible for each type of function

The default roles for the TOE are as follows:

- **“Administrator” Role**: this role is used to manage the secure configuration and operation of the TOE
- **“Operator” Role**: this role can view and manipulate data, but cannot access or alter the security functionality of the TOE.

3.2.5. Security Management Functions

The TOE allows administrative remote access using a Web Interface. To support remote administration, a management workstation with a web browser that is capable of supporting HTTPS and the TLS protocol must be used. Security management commands are accessible only by authorized administrators with sufficient permissions.

3.2.6. Protection of Security Functions

The TOE protects against tampering and unauthorized data disclosure by using dedicated communication channels protected by cryptographic means and access control methods. The TOE enforces user access controls and restricts access to the system and data to identified and authorized users. The TOE performs self-tests designed to detect when its core functionality is failing or the TOE has been tampered with. The TOE is designed to periodically check for updates, but updates are applied manually. All updates are protected from tampering by the use of published hash. The TOE also ensures that reliable time information is available for both log accountability and synchronization with the operating environment.

3.2.7. TOE Access

Access to TOE management functions is restricted to identified, authenticated and authorized users. The TOE implements a message of the day banner displayed during each management session. The TOE enforces a configurable inactivity timer after which a management session is automatically terminated by the TOE. Once a session (local or remote) has been terminated, the TOE requires the user to re-authenticate.

3.2.8. Trusted Path/Channels

The TOE ensures integrity and disclosure protection of remote administrative sessions by implementing HTTPS /TLS. The TOE protects communication with various optional operational environment components, such as a Syslog Server using TLS connection. If the negotiation of a secure session with the TOE fails, a connection will not be established.

3.3. Excluded Functionality

The TOE supports a number of features that are not part of the core functionality. These features are *not* included in the scope of the evaluation:

- Any integration and/or communication with authentication servers such as Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access-Control Systems (TACACS) is excluded from the evaluated configuration.
- Remote management using console interface (SSHv2) is excluded and disabled by default.
- Use of the SNMP functionality is excluded and it is disabled by default. The use of SNMPv3 is not restricted; however, it is an excluded functionality in NDPP evaluations.
- Use of the SMTP for sending out automated alerts is outside the scope of NDPP evaluation and as a result is not evaluated.

3.4. Secure Usage Assumptions

The ST identifies the following assumptions about the use of the product:

The ST identifies the following assumptions about the use of the product:

1. It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
2. Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
3. TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4. Architectural Information

The underlying architecture of the TOE consists of computer hardware that supports a hardened Linux-based OS that manages the disk, memory, and network resources and provides all necessary support to run the embedded modular software. A dedicated cryptographic module provides cryptographic functionality that implements secure communications and protects critical security parameters.

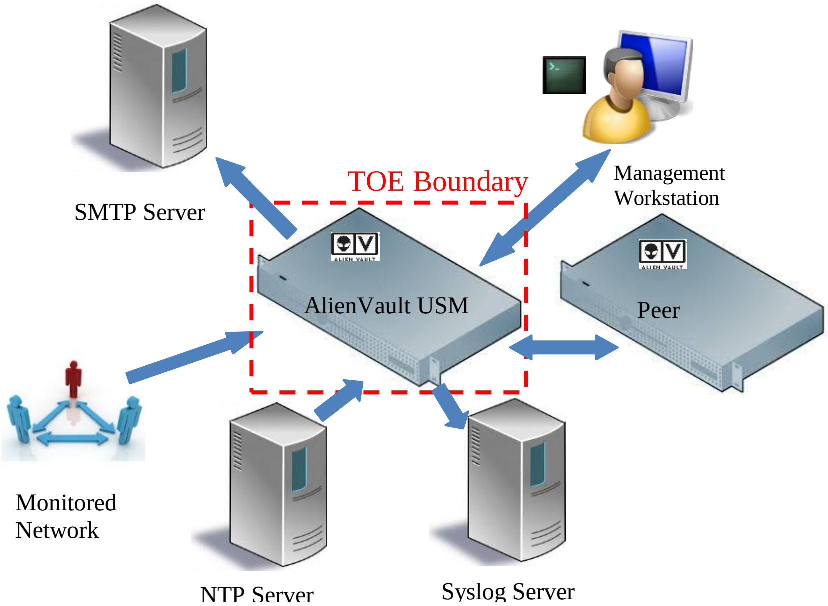

Figure 1: TOE Boundary

The TOE can be subdivided into the following profiles:

- *Sensor*
- *Server*
- *Logger*

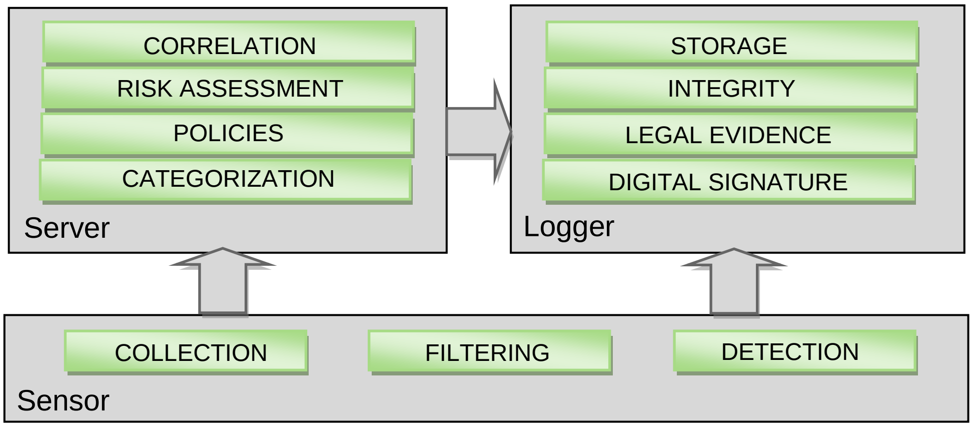

Figure 2: TOE Architecture

The TOE relies upon the Operational Environment for the following Security functionality:

- Audit storage
- Reliable time stamps from a Network Time Protocol (NTP) server

5. Documentation

The following documents were available for the evaluation. These documents are developed and maintained by AlienVault:

5.1. *User Documentation*

Identifier	Edition	Reference Title
AVUG-00001	13	Configuration for Common Criteria
AVUG-00107	01	User Management Guide
AVUG-00116	01	Proxy Configuration
AVUG-00127	01	HIDS Deployment on Windows
AVUG-00131	01	Lifecycle of a Log
AVUG-00133	01	Active Directory Integration
AVUG-00135	01	USM Intrusion Detection
AVUG-00153	01	Send Emails Triggered by Events
AVUG-00160	01	Policy Management Fundamentals
AVUG-00161	01	HIDS File Integrity Monitoring
AVUG-00163	01	Correlation Reference Guide
AVUG-00164	01	Customizing Correlation Directives or Cross Correlation Rules
AVUG-00185	01	Netflow Collection

The most up-to-date versions of the documentation can be accessed on the AlienVault website: www.alienvault.com/documentation

6. IT Product Testing

This section describes the testing efforts of the Evaluation Team. The information is derived from the *Evaluator Test Report for AlienVault USM for Government v4.12* document. The purpose of this activity was to confirm that the TOE behaves in accordance with security functional requirements specified in the ST.

6.1. Developer Testing

Standard-PP evaluations do not require additional developer testing evidence for assurance activities. However, the AlienVault provided access to their QA and Development system and submitted a descriptive report of their CM system allowing the evaluation team to determine industry best practices are followed.

6.2. Evaluator Independent Testing

A test plan was developed in accordance with the Testing Assurance Activities specified in the NDPPv1.1

Testing was conducted August 17 to September 4 2015 at the 1000 Innovation Drive, Kanata facility in a dedicated testing space.

The Evaluator successfully performed the following activities during independent testing:

- Placed the TOE into evaluated configuration by executing the preparative procedures
- Successfully executed the PP Assurance-defined tests, including the optional TLS tests
- Planned and executed a series of vulnerability/penetration tests

It was determined after examining the Test Report and full set of test results provided by the evaluators, that the testing requirements for NDPP v1.1 are fulfilled.

7. Results of Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 3.1 R4 of the CC and the CEM. Additionally the evaluators performed the assurance activities specified in the Protection Profile U.S. Government Standard Protection Profile for Network Devices, 08 June 2012, Version 1.1 with Errata 3.

The evaluation determined the TOE meets the SARs contained the PP.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL (proprietary) and Assurance Activity Report (AAR) which is public document.

Below lists the assurance requirements the TOE as specified by the PP. All assurance activities and work units received a passing verdict.

- ADV_FSP.1 Basic functional specification
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ALC_CMC.1 Labelling of the TOE
- ALC_CMS.1 TOE CM coverage
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.1 Security objectives
- ASE_REQ.1 Derived security requirements
- ASE_TSS.1 TOE summary specification
- ATE_IND.1 Independent testing – conformance
- AVA_VAN.1 Vulnerability survey

The evaluators concluded that the overall evaluation result for the target of evaluation is PASS. The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

the evidence and documentation of the work performed support the assigned rating.

8. Validators Comments/Recommendations

None.

9. Glossary

9.1. *Acronyms*

The following are product specific and CC specific acronyms. Not all of these acronyms are used in this document.

CC	Common Criteria [for IT Security Evaluation]
CIDR	Classless Inter Domain Routing
CM	Configuration Management
FIPS	Federal Information Processing Standards Publication
GB	Gigabyte
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure
ICMP	Internet Control Message Protocol
ID	Identifier
IT	Information Technology
NIST	National Institute of Standards and Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirements
SNMP	Simple Network Management Protocol
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UI	User Interface
URI	Uniform Resource Identifier

9.2. *Terminology*

This section defines the product-specific and CC-specific terms. Not all of these terms are used in this document.

Assignment The specification of an identified parameter in a component.

Assurance Grounds for confidence that an entity meets its security objectives.

Attack potential The perceived potential for success of an attack, should an attack be launched, expressed in terms of a threat agent’s expertise, resources and motivation.

Augmentation The addition of one or more assurance component(s) to a package.

Authentication data Information used to verify the claimed identity of a user.

Authorised user A user who may, in accordance with the SFR, perform an operation.

Class A grouping of families that share a common focus.

Component The smallest selectable set of elements on which requirements may be based.

Connectivity The property of the TOE that allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

Dependency A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package..

Element An indivisible security requirement.

Evaluation Assessment of a PP, an ST, or a TOE against defined criteria.

Evaluation authority A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted community.

Evaluation scheme The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

Extension The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

External entity Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.

Family A grouping of components that share security objectives but may differ in emphasis or rigor.

Formal Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Identity A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Informal Expressed in natural language.

Inter-TSF transfers Communicating data between the TOE and the security functions of other trusted IT products.

Internal communication channel A communication channel between separated parts of TOE.

Internal TOE transfer Communicating data between separated parts of the TOE.

Iteration The use of the same component to express two or more distinct requirements.

Object A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Organizational security policies A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organisation in the operational environment.

Package A named set of either functional or assurance requirements (e.g. EAL 3).

Protection Profile (PP) An implementation-independent statement of security needs for a TOE type.

Prove This term refers to a formal analysis in its mathematical sense. It is completely rigorous in all ways. Typically, “prove” is used when there is a desire to show correspondence between two TSF representations at a high level of rigor.

Refinement The addition of details to a component.

Role A predefined set of rules establishing the allowed interactions between a user and the TOE.

Secret Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.

Secure state A state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.

Security attribute A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.

Security Function Policy (SFP) A set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs.

Security objective A statement of intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions.

Security Target (ST) An implementation-dependent statement of security needs for a specific identified TOE.

Selection The specification of one or more items from a list in a component.

Semiformal Expressed in a restricted syntax language with defined semantics.

Subject An active entity in the TOE that performs operations on objects.

Target of Evaluation (TOE) A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE resource Anything useable or consumable in the TOE.

TOE Security Functions (TSF) A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

Transfers outside TSF TSF mediated communication of data to entities not under control of the TSF.

Trusted channel A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.

Trusted path a means by which a user and a TSF can communicate with necessary confidence.

TSF data Data created by and for the TOE that might affect the operation of the TOE.

TSF interface (TSFI) A means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the

TSF, receive data from the TSF and invoke services from the TSF.

User See **external entity**

User data Data created by and for the user that does not affect the operation of the TSF.

10. Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (https://www.niap-ccevs.org/).

[2] CygnaCom Solutions CCTL (http://www.cygnacom.com/cc).

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, September 2012 Version 3.1 Revision 4, CCMB-2012-09-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, September 2012 Version 3.1 Revision 4, CCMB-2012-09-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, September 2012, Version 3.1 Revision 4, CCMB-2012-09-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, September 2012, Version 3.1 Revision 4, CCMB-2012-09-004.