Swedish Certification Body for IT Security

Certification Report

Symantec Security Analytics S500

Issue: 1.0, 2018-Sept-28

Table of Contents

1 Executive Summary

The Target of Evaluation, TOE, is a network device intended for traffic monitoring and security analysis. The TOE is part of the Symantec Security Platform's Incident Response and Forensics solutions. The TOE is a hardware and software solution that is comprised of Security Analytics software version 7.2.4 build 45794 installed on the following hardware:

- SA-S500-10-CM
- SA-S500-20-FA
- SA-S500-30-FA
- SA-S500-40-FA

The TOE is intended to operate in a networked environment. The appliances can be deployed anywhere in a network assigned with task to capture, index and classify all network traffic in real time, as well as analyzing the data in the traffic flow.

The TOE is delivered as a turnkey, pre-configured appliance with the Security Analytics software preinstalled. In order to use the TOE in the certified mode it requires that a remote/local management workstation, certificate authority, syslog server and CRL server is be present in the environment.

The ST claims conformance to Collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015. The NIT technical decisions that have been applied to the Network Device Collaborative Protection Profile can be found in the ST.

There are six assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the nine threats and comply with the one organisational security policy (OSP) in the ST. The assumptions, the threat and the OSP are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by Combitech AB and EWA-Canada Ltd. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. The evaluation was performed at the evaluation assurance level EAL 1, augmented by ASE_SPD.1 Security Problem Definition.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation. EWA-Canada Ltd. operates as a Foreign location for Combitech AB within scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 1 + ASE_SPD.1 and in accordance with the NDcPP v1.0 Evaluation Activities.

The certification results only apply to the versions of the products indicated in the certificate, and on the condition that all the stipulations in the Security Target [ST] are met.
This certificate is not an endorsement of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification

Certification ID	CSEC2017006
Name and version of the certified IT product	Symantec Corporation Security Analytics S500 Appliances consisting of: Security Analytics software version 7.2.4 build 45794 - SA-S500-10-CM - SA-S500-20-FA - SA-S500-30-FA -SA-S500-40-FA
Security Target	Symantec Corporation Security Analytics S500 Appliances Security Target
Assurance level	EAL 1 + ASE_SPD.1 and NDcPP v1.0
Sponsor	Symantec Corporation
Developer	Symantec Corporation
ITSEF	Combitech AB and EWA-Canada Ltd.
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
Certification date	2018-09-28

3 Security Policy

The TOE provides the following security services:

- Security Audit
- Cryptography Support
- Identification & Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channel

3.1 Security Audit

The Network Appliances provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event.

The TOE is configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using TLS.

The logs for all the appliances can be viewed via the remote GUI interface or through the CLI. The records include the date/time the event occurred, the event/type of event, the user ID associated with the event, and additional information of the event and its success and/or failure.

3.2 Cryptographic Support

The TOE provides cryptographic support for the following features,

- TLSv1.1, TLSv1.2 and HTTPS connectivity with the following entities:
  - Management Web Browser,
  - Audit Server.
- SSH connectivity with the following entities:
  - Management SSH Client.
- Secure software update

3.3 Identification and Authentication

The TOE provides authentication services for administrative users to connect to the TOE's administrator interfaces (local CLI, remote CLI, and remote GUI). The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. In the Common Criteria evaluated configuration, the TOE is configured to require a minimum password length of 15 characters. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on any TOE administrative.

3.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. Management can take place over the following interfaces:

- Local console command line administration;

- Remote CLI administration via SSH;
- Remote GUI administration via HTTPS/TLS.

The TOE provides the ability to securely manage the below listed functions;

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE;
- Update to the TOE.

3.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Administrators. The TOE prevents reading of cryptographic keys and passwords

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE’s clock manually. Finally, the TOE performs testing to verify correct operation of the security appliances themselves. The TOE verifies all software updates via digital signature (4096-bits/SHA-512) and requires administrative intervention prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

3.6 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE displays an Authorized Administrator specified banner on both the CLI and GUI management interfaces prior to allowing any administrative access to the TOE.

3.7 Trusted Path/Channels

The TOE supports several types of secure communications, including,

- Trusted paths with remote administrators over SSH,
- Trusted paths with remote administrators over TLS/HTTPS,
- Trusted channels with remote IT environment audit servers over TLS.

4 Assumptions and Clarifications of Scope

4.1 Usage Assumptions

The Security Target [ST] makes five assumptions on the usage of the TOE.

A.LIMITED_FUNCTIONALITY

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).

A.NO_THRU_TRAFFIC_PROTECTION

A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g, firewall).

A.TRUSTED_ADMINISTRATOR

The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.

A.REGULAR_UPDATES

The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.ADMIN_CREDENTIALS_SECURE

The administrator’s credentials (private key) used to access the network device are protected by the platform on which they reside.

4.2 Environmental Assumptions

One assumption on the environment is made in the Security Target.

A.PHYSICAL_PROTECTION

The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device’s physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.

4.3 Organizational Security Policies

The Security Target [ST] places one Organizational Security Policy on the TOE.

P.ACCESS_BANNER

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4.4 Clarification of Scope

The Security Target [ST] contains nine threats, which have been considered during the evaluation.

T.UNATHORIZED_ADMINISTRATOR_ACCESS

Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

T.WEAK_CRYPTOGRAPHY

Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

T.UNTRUSTED_COMMUNICATION_CHANNELS

Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

T.WEAK_AUTHENTICATION_ENDPOINTS

Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.

T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

T.UNDETECTED_ACTIVITY

Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.

T.SECURITY_FUNCTIONALITY_COMPROMISE

Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.

T.PASSWORD_CRACKING

Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.

T.SECURITY_FUNCTIONALITY_FAILURE

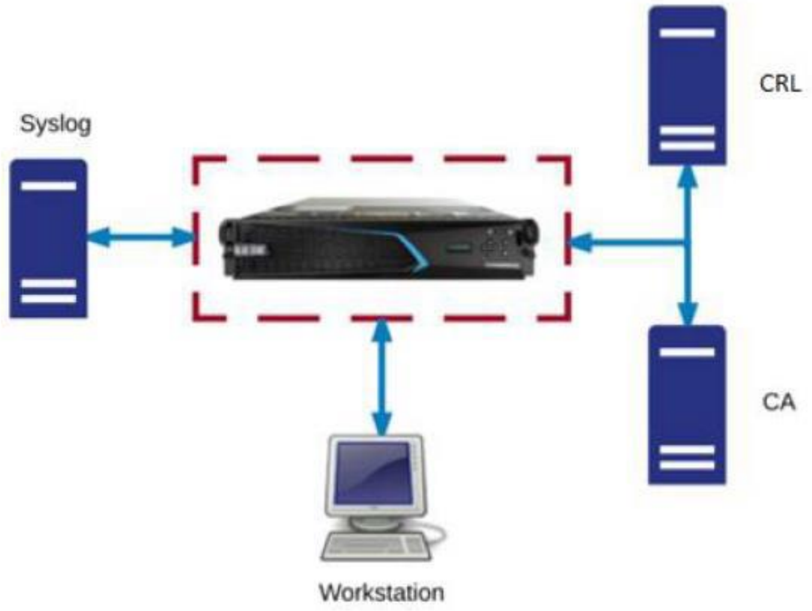
A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

5 Architectural Information

The TOE is a hardware and software solution that is comprised of the network device. The network security analytic appliance can be deployed anywhere in a network to provide a clear view of the installed network. The TOE supports mutual authentication with an audit server as a TLS client. In addition, the TOE can rest in different areas of the network, such as on the perimeter, in the core, in a backbone or at a remote link to deliver clear, actionable intelligence. The TOE also provides real-time, policy-based artifact extraction, and is not limited to any specific operating system.

The IPv4 network on which the TOE resides is considered part of the environment.

The figure below depicts the evaluated configuration. The red rectangle represents the physical boundary of the TOE. In addition, as part of the evaluation, the TOE IT environment includes the use of a Certificate Authority (CA), Syslog Server, and Certificate Revocation List (CRL) service. This is shown in the figure.



6 Documentation

For proper configuration of the TOE into the evaluated configuration, the following guidance documents are available:

- Symantec Corporation Security Analytics S500 Appliances Common Criteria Administrative Guidance Document
- Security Analytics 7.2.3 Administration and Central Manager Guide
- Security Analytics 7.2.3 Reference Guide

7 IT Product Testing

The evaluator testing was executed on Symantec Corporation Security Analytics S500 Appliances. The used TOE software version was 7.2.4 build 45710. The appliances used for testing were SA-S500-10-CM and SA-S500-40-FA. The test environment was located at EWA-Canada’s test lab, Ottawa, Canada, and was managed from Combitech’s test lab, Sundbyberg, Sweden, over a secure VPN and Windows Remote Desktop setup. Some assistance from local test resources in Ottawa were required, e.g. to physically reset devices. Cryptographic algorithm testing was performed at the developer's site in Mountain View, USA.

7.1 Independent Evaluator Testing

The test configuration and the test cases follows the test requirements for each SFR placed in NDcPP. The test cases provide coverage for the TOE interfaces and SFRs.

The results of all test cases were consistent with the expected test results, and all tests were judged to pass.

7.2 Evaluator Penetration Testing

The following types of penetration tests were performed:

- Port scan
- Vulnerability scanning
- Protocol fuzzing

Port scans were run after installation and configuration had been done according to the guidance documentation. The purpose was to check that no unexpected ports were opened unfiltered and no unexpected services available. The Nmap (www.nmap.org) port scan tool was used. Four different modes were used: TCP Connect, TCP SYN, UDP, and IP protocol scans. All possible 65535 ports were scanned for TCP/UDP.

Nexpose (www.rapid7.com) vulnerability scans were run. No issues concerning the evaluated configuration were found.

The ICMP and TCP protocols were fuzzed with 256 strings using scapy (http://www.secdev.org/projects/scapy).

All penetration testing had negative outcome, i.e. no vulnerabilities were found.

8 Evaluated Configuration

The TOE evaluated configuration is comprised of at least one of the following: SA-S500-10-CM, SA-S500-20-FA, SA-S500-30-FA, or SA-S500-40-FA. The evaluated configuration also requires the following external IT entities;

Remote Management Workstation (GUI).
This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration through HTTPS and TLS protected channels.

Remote Management Workstation (CLI).
This includes any IT Environment Management workstation with an SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels.

Local Management Workstation (CLI).
This includes any IT Environment Management workstation with a local CLI support that is used by the TOE administrator to support TOE administration through a direct connection.

Certificate Authority
The CA is used in support of certificate validation operations.

Syslog Server
The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE.

CRL Server
The CRL server is used to in support of certificate revocation testing.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators' overall verdict is PASS.

The verdicts for the respective assurance classes and components are summarised in the following table:

Assurance Class/Family	*Short name*	*Verdict*
Development	ADV	PASS
Basic functional specification	ADV_FSP.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
Labeling of the TOE	ALC_CMC.1	PASS
TOE CM coverage	ALC_CMS.1	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives for the Operational Environment	ASE_OBJ.1	PASS
Extended Components Definition	ASE_ECD.1	PASS
Stated Security Requirements	ASE_REQ.1	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Independent Testing - conformance	ATE_IND.1	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability survey	AVA_VAN.1	PASS

10 Evaluator Comments and Recommendations

The evaluators do not have any comments or recommendations concerning the product nor regarding its usage.

11 Glossary

CA	Certificate Authority
CC	Common Critera
CLI	Command Line Interface
CRL	Certificate Revocation List
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IP	Internet Protocol
IPv4	Internet Protocol version 4
NDcPP	Network Device Collaborative Protection Profile
OS	Operating System
PP	Protection Profile
SA	Security Analytics
SHA	Secure HashAlgorithm
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
UDP	User Datagram Protocol

12 Bibliography

ST	Symantec Corporation Security Analytics S500 Appliances Security Target, Symantec Corporation, 2018-08-27, document version 0.9
CCADM	Symantec Corporation Security Analytics S500 Appliances Common Criteria Administrative Guidance Document, Symantec Corporation, 2018-05-03, document version 0.6
ADM	Security Analytics 7.2.3 Administration and Central Manager Guide, Symantec Corporation, 2017-02-24
REF	Security Analytics 7.2.3 Reference Guide, Symantec Corporation, 2017-02-24
NDCPP	Collaborative Protection Profile for Network Devices, 27 February 2015, version 1.0
NDSD	Evaluation Activities for Network Device cPP, 27 February 2015, version 1.0
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003
CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2018-04-24, document version 29.0
SP-188	SP-188 Scheme Crypto Policy, CSEC, 2017-04-04, document version 7.0

Appendix A - QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received 2017-05-08:

QMS 1.20.3	valid from 2017-04-24
QMS 1.20.4	valid from 2017-05-11
QMS 1.20.5	valid from 2017-06-28
QMS 1.21	valid from 2017-11-15
QMS 1.21.1	valid from 2018-03-09
QMS 1.21.2	valid from 2018-03-09 SIC!
QMS 1.21.3	valid from 2018-05-24
QMS 1.21.4	valid from 2018-09-13

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 1.21.4”.

The certifier concluded that, from QMS 1.20.3 to the current QMS 1.21.4, there are no changes with impact on the result of the certification.