National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Palo Alto Networks Cortex XSOAR Engine 6.6

Report Number: CCEVS-VR-11325-2022
Dated: October 5, 2022
Version: 1.0

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

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson
Linda Morrison
Clare Parran
Lori Sarem
Chris Thorpe
The MITRE Corporation

Common Criteria Testing Laboratory

Tammy Compton
John Messiha
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Palo Alto Networks Cortex XSOAR 6.6 Engine solution provided by Palo Alto Networks, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in October 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended, and meets the assurance requirements of the Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14) with the Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11).

The Target of Evaluation (TOE) is the Palo Alto Networks Cortex XSOAR Engine 6.6. The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the Palo Alto Networks Cortex XSOAR Engine 6.6 Security Target, Version 1.1, September 30, 2022 and analysis performed by the Validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Palo Alto Networks Cortex XSOAR Engine 6.6
Protection Profile	Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14) with the Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11)
ST	Palo Alto Networks Cortex XSOAR Engine 6.6 Security Target, Version 1.1, September 30, 2022
Evaluation Technical Report	Evaluation Technical Report for Palo Alto Networks Cortex XSOAR Engine 6.6, version 0.3, September 30, 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Rev 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
Sponsor	Palo Alto Networks, Inc.
Developer	Palo Alto Networks, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jenn Dotson, Linda Morrison, Clare Parran, Lori Sarem, Chris Thorpe

Table 1: Evaluation Identifiers

3 Assumptions & Clarification of Scope

Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14)
- Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11)

That information has not been reproduced here and the ASPP14/PKGTLS11 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the ASPP14/PKGTLS11 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Application Software Protection Profile with the TLS Package and performed by the Evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Software Application models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the ASPP14/PKGTLS11 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is the Palo Alto Networks Cortex[1] XSOAR Engine. Cortex XSOAR combines security orchestration, incident management, and interactive investigation into a seamless experience. The orchestration component is designed to automate security product tasks and weave in human analyst tasks and workflows. The Server (in the operational environment) provides UI functionality and playbook detection/response functionality, while Engine (as known as the TOE) is used to efficiently share the workload (e.g., load-balancing), thereby speeding up execution time. In essence, the TOE is like an extension of the Server used to offload tasks to it.

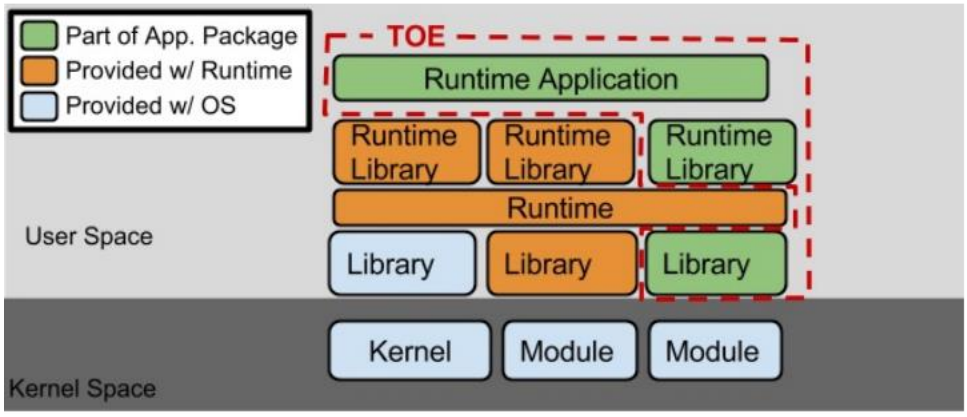
The Server (in the operational environment) provides security management functions and interface via web UI protected by HTTPS (out of scope) and communicates with the TOE through TLSv1.2 protected channels. The Server implements TLS server functionality while the TOE implements TLS client functionality.

4.1 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 7 below.

4.2 TOE Architecture

The following diagram depicts the software architecture of the TOE.



4.3 Physical Boundaries

The physical boundary of the TOE is the Cortex Engine application installed and running on a supported platform (i.e., Linux operating systems).

[1] Cortex was formerly known as Demisto.

5 Security Policy

This section summaries the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Identification and authentication
4. Security management
5. Privacy
6. Protection of the TSF
7. Trusted path/channels

5.1 Cryptographic support

The TOE implements CAVP validated cryptographic algorithms that provide key management, random bit generation, encryption/decryption, digital signature and cryptographic hashing and keyed-hash message authentication features in support of cryptographic protocols such as TLS.

5.2 User data protection

The TOE accesses the network connectivity of its' platform to communicate with Server. The TOE does not access any sensitive information repositories.

5.3 Identification and authentication

The TOE authenticates using X509v3 certificate-based method.

5.4 Security management

The TOE provides access to the security management functions via configuration files. Identification and authentication are required by the operating system before accessing the files. In addition, the operating system can provide some configuration options for TOE. In that case, the operating system I&A method and privileges will be used and enforced.

5.5 Privacy

The TOE does not transmit PII over the network.

5.6 Protection of the TSF

The TOE implements a number of functions to ensure that it is protected against tampering and corruption. These mechanisms include utilizing platform APIs, memory mapping, and stack-based buffer overflow protection. Palo Alto Networks provides customers with a means of updating their TOE using trusted updates. These trusted updates (signed RPM package) are securely delivered over HTTPS website and verified using approved digital signature methods. All of these updates are properly signed using RSA 2048 with SHA-256 and is verified by the operating system mechanism. In addition, the TOE image is protected

with FIPS Software integrity test at power-up (e.g., when the application is started or is reloaded).

5.7 Trusted path/channels

The TOE protects communication with Server, in the operational environment, using TLS to ensure both integrity and disclosure protection.

6 Documentation

The following documents were available with the TOE for evaluation:

- Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) Cortex XSOAR Server and Engine 6.6, September 16, 2022

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 Evaluated Configuration

The evaluated configuration is the Cortex XSOAR Engine 6.6. The TOE runs on an operating system that includes RHEL 8, RHEL 7, Ubuntu (18.04, 20.04), Oracle Linux 7, or Amazon Linux 2. The TOE was tested on RedHat Enterprise Linux v8.4.

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for Palo Alto Networks Cortex XSOAR Engine 6.6, Version 0.3, September 27, 2022 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the ASPP14/PKGTLS11 including the tests associated with optional requirements. The AAR, in section 1 provides a summary of the test methods including the tested platform.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

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 CC version 3.1 Rev 5 and CEM version 3.1 Rev 5. The evaluation determined the Palo Alto Networks Cortex XSOAR Engine TOE to be Part 2 extended, and to meet the SARs contained in the ASPP14/PKGTLS11.

9.1 Evaluation of the Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Palo Alto Networks Cortex XSOAR 6.6 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally the Evaluators performed the assurance activities specified in the ASPP14/PKGTLS11 related to the examination of the information contained in the TSS.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was

conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was identified.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the ASPP14/PKGTLS11 and recorded the results in a Test Report, summarized in the AAR.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the Evaluators. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The Evaluators searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 9/27/2022 with the following search terms: "Palo Alto Networks", "Cortex XSOAR", "Cortex XSOAR Server", "Cortex XSOAR Engine", "RedHat Enterprise Linux v8.4", "Golang 1.16", "BoringCrypto".

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.7 Summary of Evaluation Results

The Evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team’s testing also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the Evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) Cortex XSOAR Server and Engine 6.6, September 16, 2022. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Palo Alto Networks Cortex XSOAR Engine 6.6 Security Target, Version 1.1, September 30, 2022*.

13 Glossary

The following definitions are used throughout this document:

Term	Definition
Common Criteria Testing Laboratory (CCTL)	An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
Evaluation	The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
Evaluation Evidence	Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
Feature	Part of a product that is either included with the product or can be ordered separately.
Target of Evaluation (TOE)	A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
Validation	The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
Validation Body	A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

Table 2: Glossary

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, September 2012.

[4] Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14)

[5] Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11).

[6] Palo Alto Networks Cortex XSOAR Engine 6.6 Security Target, Version 1.1, September 30, 2022 (ST).

[7] Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) Cortex XSOAR Server and Engine 6.6, September 16, 2022.

[8] Assurance Activity Report for Palo Alto Networks Cortex XSOAR Engine 6.6, Version 0.3, September 30, 2022 (AAR).

[9] Detailed Test Report for Palo Alto Networks Cortex XSOAR 6.6, Version 0.3, September 27, 2022 (DTR).

[10] Evaluation Technical Report for Palo Alto Networks Cortex XSOAR Engine 6.6, Version 0.3, September 30, 2022 (ETR)