National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform

Report Number: **CCEVS-VR-VID11467-2025**
Dated: **February 25, 2025**
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
Sheldon Durrant
Clare Parran
Lori Sarem
The MITRE Corporation

Common Criteria Testing Laboratory

Julia Miller
Cody Cummins
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform solution provided by Ciena Corporation. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) 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 Febraury 2025. 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 Conformant, and meets the assurance requirements of the PP-Configuration for Network Devices and MACsec Ethernet Encryption, Version 1.0, 29 March 2023 (CFG_NDcPP-MACsec_v1.0) which includes the Base PP: *collaborative Protection Profile for Network Devices,* Version 2.2e, 23 March 2020 (NDcPP22e) with the *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 (MACSEC10).

The TOE is the Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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 VR 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 (CCEVS) 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 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 *Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform Security Target*, version 1.1, February 17, 2025 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 Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (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.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform
Protection Profile	PP-Configuration for Network Devices and MACsec Ethernet Encryption, Version 1.0, 29 March 2023 (CFG_NDcPP-MACsec_v1.0) which includes the Base PP: *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e) with the *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 (MACSEC10)
ST	*Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform Security Target*, version 1.1, February 17, 2025
Evaluation Technical Report	*Evaluation Technical Report for Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform*, version 1.1, February 17, 2025
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Ciena Corporation
Developer	Ciena Corporation
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Clare Parran, Lori Sarem

3 Architectural Information

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

The TOE is the Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform. The TOE is a non-distributed, non-virtual network device which implements routing and switching functionalities for enterprise, mobility, and converged network architectures. In these architectures, the TOE can be deployed in the access, aggregation, or core of the network. The TOE uses a Linux based container architecture for its SAOS Network Operating System and includes the Ciena SAOS R10.9.1 operating system executed on the 3926 with Large NFV Compute Server Service Aggregation Platform.

3.1 TOE Description

The TOE implements the general functionality of a router/switch consistent with the collaborative Protection Profile for Network Devices v2.2E with MACsec Module v1.0. The TOE implements controlled connectivity between two subnetworks and a management interface. All network traffic between the connected subnetworks is controlled by the TOE and the authorized administrators may manage the TOE using the management interface.

The management interface is a Command Line Interface (CLI) which may be accessed locally or remotely. Local access is via a console port which is a Serial EIA-561 (RJ-45) or a USB-C port. It allows management of the TOE from a workstation physically connected to the TOE. Remote management is over Secure Shell (SSH). SSH implements a secure remote login over a network connection and allows protected CLI and Network Configuration Protocol (NETCONF) access to the TOE.

All administrators are identified and authenticated using a username and password or based on SSH public key authentication. Access is only granted, and the user assigned to the role administrator upon successful authentication. Authentication is implemented locally. Authentication of TLS peers is done using X.509 Public Key Certificates. The validity of the X.509 public key certificates is verified using the Online Certificate Status Protocol (OCSP). TLS may also be used for forwarding audit records to an external audit server. MACsec is used for protected communication among MACsec peers.

3.2 TOE Evaluated Platforms

The TOE is composed of the following components:

- TOE software is Ciena SAOS R10.9.1
- TOE hardware is the Ciena 3926-905 with Large NFV Compute Server Service Aggregation Platform

3.3 TOE Architecture

The TOE is the Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform. The platform is a single instance with the following physical characteristics:

- 3926-905
  - Processor - ARM Cortex A53, 4CORE
  - ASIC –Broadcom BCM82759 MACsec
- Large NFV Compute Server
  - Processor - Intel XEON D1548, 8CORE

3.4 Physical Boundaries

The TOE is deployed in an environment that includes the IT components illustrated in Figure 1. The TOE itself is delivered as an appliance or an FRU with the software installed.

The physical boundary of the TOE is also illustrated in Figure 1. The TOE implements a TLS Client and SSH Server for secure connectivity to the components of the environment. Each component of the environment is required to implement the corresponding client and/or server. The remote management workstation is required to implement a SSH Client for accessing the TOE.

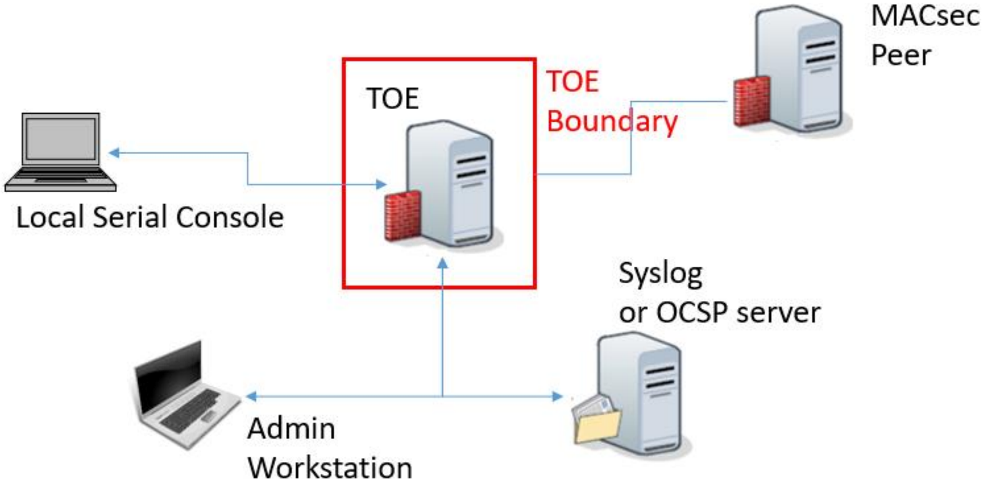

Figure 1: TOE boundary and environment

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

The TOE is able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and also to send the logs to a designated log server using TLS to protect the logs while in transit on the network. Each audit record contains the date and time of event, type of event, subject identity, and any other event-related relevant data.

4.2 Cryptographic support

The TOE contains a CAVP-tested cryptographic module that provides key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher-level cryptographic protocols including MACsec, SSH and TLS.

4.3 Identification and authentication

The TOE authenticates all users connecting to the management interfaces of the TOE. Authentication may take place over the console for local access or over SSH for remote access. Only upon successful authentication, given that the user is authorized for the role, is a user assigned to the role administrator and granted access to the management functions of the TOE. Local users authenticate to the TOE using a username and password. Remote users may also use SSH public-key authentication.

Users may change their own passwords, but the TOE enforces minimum quality criteria for the passwords. The TOE also maintains a counter for consecutive, failed authentication attempts for each user. If the counter value reaches an administrator-defined threshold, the TOE triggers protective measures to prevent password guessing attacks.

The TOE uses X.509v3 certificates for peer entity authentication of TLS peers. The TSF determines the validity of the certificates by confirming the validity of the certificate chain and verifying that the certificate chain ends in a trusted Certificate Authority (CA). The TOE connects to an Online Certificate Status Protocol (OCSP) server to confirm the revocation status of the certificates.

4.4 Security management

The TOE allows local and remote management of its security functions. Local management is from a management workstation connected to the console or USB port of the TOE. Remote management is from a workstation connected to the TOE over SSHv2.

All management functions are implemented using the CLI and are only made available to authorized administrators upon successful identification and authentication. The TOE also supports a NETCONF interface which is also protected with SSH. The administrator can use the NETCONF interface to perform the same functions as the CLI.

4.5 Protection of the TSF

The TOE protects all passwords, pre-shared keys, symmetric keys, and private keys from unauthorized disclosure. Pre-shared keys, symmetric keys, and private keys are stored encrypted. An exception is the SSH host keys which are required by the SSH Daemon when the SSH starts. The SSH Daemon is executed with root privileges and the SSH host keys are only accessible with root privileges. No user of the TOE is granted root privileges. Passwords are stored as non-reversible hash values computed using SHA-512 using the shadow utility functions. The TOE maintains system time via its local hardware clock which is manually set by an administrator.

The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. An administrator can install software updates to the TOE and verify the authenticity of all updates prior to the installation.

4.6 TOE access

Prior to establishing an administration session with the TOE, an access banner is displayed to the user. The banner messaging is customizable but is typically used to warn the users of the consequences of attempted unauthorized access. The TOE will terminate an interactive session after a configurable time of session inactivity. A user may terminate his/her local and remote administrative sessions on will.

4.7 Trusted path/channels

The TOE implements trusted paths and trusted channels. The trusted path is a SSH connection between the TOE and the remote management workstation. The SSH client of the remote management workstation connects to the SSH server implemented by the TOE. Upon successful connection establishment and authentication of the user, the remote administrator uses the CLI or NETCONF over SSH to manage the TOE.

For trusted channels, the TOE implements a TLS client used by the TOE to connect to the peer entities. The peer entity is the syslog server. The TOE uses MACsec to protect communications with MACsec peers.

5 Assumptions & Clarification of Scope

5.1 Assumptions

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

- *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e)
- *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 (MACSEC10)

That information has not been reproduced here, and the NDcPP22e/MACSEC/10 should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/MACSEC10 as described for this TOE in the ST. 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.

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 NDcPP22e and the MACSEC10 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 MACsec Device models was not included in the scope of the evaluation and, therefore, should not 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 NDcPP22e/MACSEC10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- *Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform CC Guidance Supplement*, version 1.1, February 17, 2025

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 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 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 Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform*, version 1.1, February 17, 2025 (DTR), as summarized in the evaluation *Assurance Activity Report for Ciena SAOS R10.9.1 on the 3926 with large NFV Compute Server Service Aggregation Platform*, version 1.1, February 17, 2025 (AAR).

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e/MACsec10 including the tests associated with optional requirements. The AAR, in Section 3.4, lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The TOE is composed of the following components:

- TOE software is Ciena SAOS R10.9.1
- TOE hardware is the Ciena 3926-905 with Large NFV Compute Server Service Aggregation Platform

As described and illustrated in Section 3.4, the TOE is deployed in an environment that includes the IT components shown in Figure 1: TOE boundary and environment. The physical boundary of the TOE is also illustrated in that Figure. The non-TOE components are summarized below in Table 1: IT Environment Components and are required to operate the TOE in the evaluated configuration.

Component	Description
MACsec Peer	A peer server that supports MACsec to communicate with the TOE.
Audit (syslog) server (Mandatory)	The audit server supports syslog messages over TLS v1.2 to receive the audit files from the TOE. The audit data is stored in the remote audit server for redundancy purposes.
OCSP Server (Mandatory)	Validity of the certificates the TOE uses for asserting the authenticity of the TLS peers is verified using OCSP.
Admin Workstation (Mandatory)	A workstation used by an administrator to manage the TOE locally or remotely. The remote management station must include a SSH client.

Table 1: IT Environment Components

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 Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/MACsec10.

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 Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team 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 ST and Guidance document. Additionally, the Evaluation team performed the assurance activities specified in the NDcPP22e/MACSEC10 related to the examination of the information contained in the TSS.

The Validation team 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. The guide was assessed during the design and testing phases of the evaluation to ensure it was complete.

The Validation team 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 Validation team 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 NDcPP22e/MACSEC10 and recorded the results in a Test Report, summarized in the AAR.

The Validation team 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 contained in the DTR prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the following sites:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities)
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories)
- Offensive Security Exploit Database (https://www.exploit-db.com/)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)

The search was conducted on February 17, 2025, with the following search terms: “Ciena”, “Ciena SAOS”, “Ciena SAOS R10.9.1”, “Ciena 3926-905”, “3926”, “FRU”, “MACsec”, “Broadcom BCM82759”, “Broadcom BCM56271”, “ARM Cortex A53”, “Intel XEON D1548”, “Ciena Cryptographic Library”, “NFV Compute Server”.

The Validation team 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 *Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform CC Guidance Supplement* document. As noted in Section 6, consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated. No versions of the TOE and software, either earlier or later, were evaluated. Any additional customer documentation, not listed in Section 6, provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore, should not be relied upon to configure or operate the TOE as evaluated.

The Validation team suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness. For example, specifically, the Zero Touch Provisioning (ZTP), including the Secure ZTP, functionality was not part of the evaluated configuration and was not evaluated, as noted in the Guidance document.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform Security Target*, version 1.1, February 17, 2025.

13 Glossary

The following definitions are used throughout this document:

- **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.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e).

[5] *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 (MACSEC10).

[6] *Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform Security Target*, version 1.1, February 17, 2025 (ST).

[7] *Assurance Activity Report for Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform*, version 1.1, February 17, 2025 (AAR).

[8] *Detailed Test Report for Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform*, version 1.1, February 17, 2025 (DTR).

[9] *Evaluation Technical Report for Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform*, version 1.1, February 17, 2025 (ETR).