National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Corelight Sensors with BroLin v28

Report Number: CCEVS-VR-VID11489-2025
Dated: January 16, 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

Linda Morrison
Clare Parran
Lisa Mitchell
The MITRE Corporation

Anne Gugel
The Johns Hopkins University Applied Physics Laboratory

Common Criteria Testing Laboratory

John Messiha
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary 1
2 Identification 2
3 Architectural Information 3
3.1 TOE Description 3
3.2 TOE Evaluated Platforms 3
3.3 TOE Architecture 4
3.4 Physical Boundaries 4
4 Security Policy 6
4.1 Security audit 6
4.2 Cryptographic support 6
4.3 Identification and authentication 6
4.4 Security management 6
4.5 Protection of the TSF 7
4.6 TOE access 7
4.7 Trusted path/channels 7
5 Assumptions & Clarification of Scope 8
6 Documentation 9
7 IT Product Testing 10
7.1 Developer Testing 10
7.2 Evaluation Team Independent Testing 10
8 Evaluated Configuration 11
9 Results of the Evaluation 13
9.1 Evaluation of the Security Target (ASE) 13
9.2 Evaluation of the Development (ADV) 13
9.3 Evaluation of the Guidance Documents (AGD) 13
9.4 Evaluation of the Life Cycle Support Activities (ALC) 14
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 14
9.6 Vulnerability Assessment Activity (VAN) 14
9.7 Summary of Evaluation Results 15
10 Validator Comments/Recommendations 16
11 Annexes 17
12 Security Target 18
13 Glossary 19
14 Bibliography 20

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Corelight Sensors with BroLin v28 solution provided by Corelight, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report 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 January 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 *collaborative Protection Profile for Network Devices*, version 2.2e, 23 March 2020 (NDcPP22e).

The TOE is the Corelight Sensors with BroLin v28. The 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 evaluation technical report 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 evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Corelight Sensors with BroLin v28 Security Target, Version 0.6, December 20, 2024 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.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Corelight Sensors with BroLin v28 (Specific models identified in Section 8)
Protection Profile	*collaborative Protection Profile for Network Devices*, version 2.2e, 23 March 2020
ST	Corelight Sensors with BroLin v28 Security Target, Version 0.6, December 20, 2024
Evaluation Technical Report	Evaluation Technical Report for Corelight Sensors with BroLin v28, Version 0.3, December 20, 2024
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	Corelight, Inc.
Developer	Corelight, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Lisa Mitchell, Anne Gugel, Clare Parran, Linda Morrison

3 Architectural Information

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

The Target of Evaluation (TOE) is Corelight's Sensors. Simple to deploy and integrate with existing analysis tools, the Corelight Sensor Appliances transform high-volume network traffic into high-fidelity data for incident response, intrusion detection, forensics and more. The Sensor parses dozens of network protocols and generates rich, actionable data streams designed for security professionals.

3.1 TOE Description

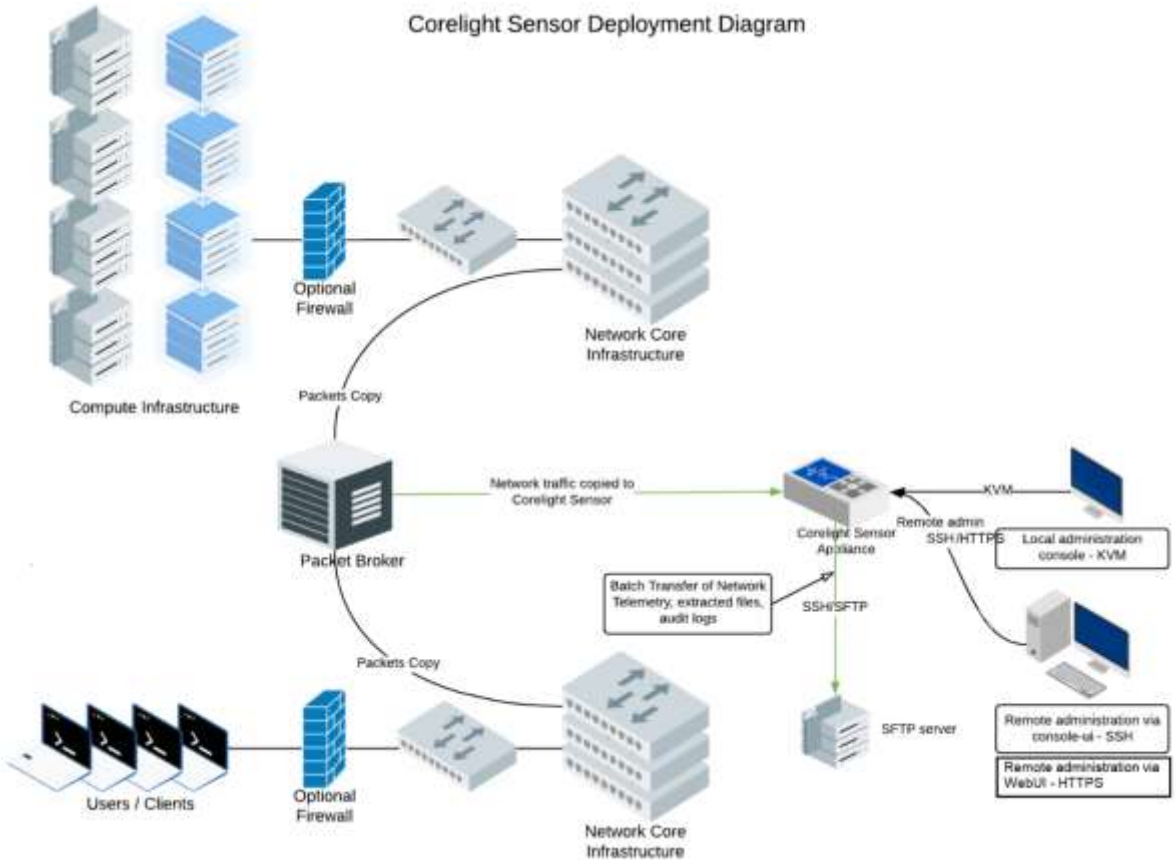
The TOE is a network device which is composed of hardware and software that offers a scalable solution to the end users. It satisfies all the criteria to meet the *collaborative Protection Profile for Network Devices*, Version 2.2e [NDcPP22e]. The TOE operating system is BroLin v28. The TOE boundary is the hardware appliance, which comprises hardware and software components. The SSHv2 client and web browser (running on the administrator's workstation) as well as the remote SFTP audit server lie in the TOE's Operational Environment.

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

3.3 TOE Architecture

The TOE operates within a network environment as diagrammed below.



TOE and TOE Operational Environment

An administrator uses an SSHv2 client or a web browser (each running on the administrator's workstation) to administer the TOE. The TOE does not have distributed components. Instead, the TOE implements all functionality within each model (physical appliance). Because the TOE independently satisfies all SFRs in the NDcPP22e without the Management Component, the NDcPP22e prescribes that the TOE be certified (by itself) according to the NDcPP22e and without the Management Component. "Figure 4: Non-distributed TOE use case" in the NDcPP22e depicts the TOE and its dedicated provisioning applications.

As a result, the TOE boundary includes only the TOE itself. The SSHv2 client and web browser (running on the administrator's workstation) as well as the remote SFTP audit server lie in the TOE's Operational Environment.

3.4 Physical Boundaries

The TOE boundary is the hardware appliance which consists of hardware and software components. It is deployed in an environment which contains the various IT components as depicted in the Figure above.

The TOE is shipped with the software pre-installed on it. Software updates are available for download from Corelight.

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 generates audit events for all start-up and shut-down functions, and all auditable events. Audit events are also generated for management actions specified in FAU_GEN.1. The TOE can store audit events locally and export them to an external audit server (via SFTP using SSH v2). Each audit record contains the date and time of event, type of event, subject identity, and the relevant data of the event.

4.2 Cryptographic support

The TOE provides cryptographic support for the secure administration access and audit export via SSH, for secure administration access via SFTP (FTP over SSH v2). Secure administration may also be performed using HTTPS/TLS (remote WebUI). The operating system is BroLin v28 which is based upon Linux Kernel version 5.4. The TOE leverages the SafeLogic's OpenSSL 3.0 and FIPS provider module for its cryptographic functionality. Functions include Key generation, key establishment, key distribution, key destruction, and cryptographic operations.

4.3 Identification and authentication

The TOE provides authentication services for administrative users to connect to the TOE's secure CLI administrator interface and to its WebUI. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE supports SSH password-based authentication and public key-based authentication. The TOE's WebUI and local console support password-based authentication. The TOE's SSHv2 interface supports authentication of administrative clients using SSH public keys.

4.4 Security management

TOE administrators manage the security functions of the TOE through both an SSH CLI and through the TOE's HTTPS/TLS WebUI. The TOE also provides the ability to configure the session activity timeout of an administrator and to configure the TOE's access banner.

4.5 Protection of the TSF

The TOE protects all passwords, pre-shared keys, symmetric keys and private keys from unauthorized disclosure. Passwords are stored on the file system in encrypted format. Passwords are stored as SHA-512 salted hash value as per standard Linux approach. 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. The TOE internally maintains the date and time.

4.6 TOE access

Prior to establishing an administration session with the TOE, a banner is displayed to the user. The banner messaging is customizable. The TOE will terminate an interactive session after 60 minutes of session inactivity. A user can terminate their local CLI session and remote CLI session by entering exit at the prompt.

4.7 Trusted path/channels

The TOE supports SSH v2 for secure communication to the following IT entities: Audit server via SFTP. The TOE supports SSH v2 (remote CLI) and HTTPS/TLS (remote WebUI) for secure remote administration.

5 Assumptions & Clarification of Scope

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)

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

Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e 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.

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 collaborative Protection Profile for Network Devices 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 Network device 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 NDcPP22e 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:

- Corelight Sensor AP 200, AP 520, AP 1001, AP 1100, AP 1200, AP 3000, AP 3100, AP 3200, AP 5000, AP 5002 & AP 5200 Common Criteria Guidance Document, Version 0.2, December 20, 2024 (Admin Guide)

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 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 Corelight Sensors with BroLin v28*, Version 0.3, December 20, 2024 (DTR), as summarized in the evaluation Assurance Activity Report (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 including the tests associated with optional requirements. AAR Section 3.4.1 provides a diagram of the test environment while Section 1.2 provides the equivalency argument for those models not tested.

8 Evaluated Configuration

The TOE includes several models as shown below:

Model	CPU	Form Factor	Monitoring Interface	Management Interface	Power
AP 200	Intel Xeon Scalable Silver 4110 Skylake-SP	1U half-depth rackmount	Four 1G SFP interfaces	One 10/100/1000 copper Ethernet port	120/240 VAC 50/60 Hz single PSUs.
AP 520	Intel Xeon Scalable Gold 5317 Sunny Cove/Icelake-SP	1U rackmount	Four 1G SFP interfaces	One 10/100/1000 copper Ethernet port	120/240 VAC 50/60 Hz single PSUs.
AP 1001	Intel Xeon Scalable Silver 4116 Skylake-SP	1U rackmount	Four 1G/10G SFP/SFP+ interfaces	One 10/100/1000 copper ethernet port and up to 2 10G Ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.
AP 1100	Intel Xeon Scalable Silver 4314 Sunny Cove/Icelake-SP	1U rackmount	Four 1G/10G SFP/SFP+ interfaces	2 1G Ethernet ports and 4 10G Ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.
AP 1200	AMD EPYC 9254 Genoa/Zen 4	1U rackmount	Four 1G/10G SFP/SFP+ interfaces	2 1G Ethernet ports and 4 10/25G Ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.
AP 3000	Intel Xeon Scalable Gold 6238 Skylake/Cascade Lake-SP	1U rackmount	Four 1G/10G SFP/SFP+ interfaces OR 10G QSF28 OR two 40G QSFP28 OR eight 10G QSFP28 interfaces	2 1G Ethernet ports and 4 10G Ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.
AP 3100	Intel Xeon Scalable Gold 5318Y Sunny Cove/Icelake-SP	1U rackmount	Four 1G/10G SFP/SFP+ interfaces OR 10G QSF28 OR two 40G	2 1G Ethernet ports and 4 10G Ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.

Model	CPU	Form Factor	Monitoring Interface	Management Interface	Power
			QSFP28 OR eight 10G QSFP28 interfaces		
AP 3200	AMD EPYC 9354 Genoa/Zen4	1U rackmount	Four 1G/10G SFP/SFP+ interfaces OR 10G QSF28 OR two 40G QSFP28 OR eight 10G QSFP28 interfaces	2 1G Ethernet ports and 4 10/25G Ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.
AP 5000	AMD EPYC 7742 Rome/Zen2	1U rackmount	Two QSFP28 bays, capable of supporting eight 10G OR two 40G 8 OR two 100G interfaces in a powerful, specialized NIC.	One 10/100/1000 copper ethernet port and up to 4 10G ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.
AP 5002	AMD EPYC 7713 Milan/Zen3	1U rackmount	2 x QSFP56 bays capable of supporting eight 10G, two 40G or two 100G interfaces.	One 10/100/1000 copper ethernet port and up to 4 10G ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.
AP 5200	AMD EPYC 9754 Bergamo/Zen 4c	1U rackmount	2 x QSFP56 bays capable of supporting eight 10G, two 40G or two 100G interfaces	2 1G Ethernet ports and 4 10/25G Ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.

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 Sensors with BroLin v28 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e.

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 Corelight Sensors with BroLin v28 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 Security Target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP22e 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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were 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 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 in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on December 20, 2024 with the following search terms: “Corelight”, “Corelight Sensors”, “Corelight Sensors with BroLin v28”, “BroLin v28”, “AP 200”, “AP 5002”, “AP 520”, “AP 1001”, “AP 1100”, “AP 1200”, “AP 3000”, “AP 3100”, “AP 3200”, “AP 5200”, “Intel Xeon Scalable Silver 4110”, “Intel Xeon Scalable Gold 5317”, “Intel Xeon Scalable Silver 4116”, “Intel Xeon Scalable Silver 4314”, “AMD EPYC 9254”, “Intel Xeon Scalable Gold 6238”, “Intel Xeon Scalable Gold 5318Y”, “AMD EPYC 9534”, “AMD EPYC 7742”, “AMD EPYC 7713”, “AMD EPYC 9754”, “Linux Kernel version 5.4”, “Linux Kernel 5.4”, “SafeLogic”, “SafeLogic OpenSSL 3.0”, and “OpenSSL 3.0”.

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 Corelight Sensor AP 200, AP 520, AP 1001, AP 1100, AP 1200, AP 3000, AP 3100, AP 3200, AP 5000, AP 5002 & AP 5200 Common Criteria Guidance Document, Version 0.2, December 20, 2024. 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 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.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. Evaluation activities are strictly bound by the assurance activities described in the NDcPP22e and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: Corelight Sensors with BroLin v28 Security Target, Version 0.6, December 20, 2024.

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

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, 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.

[5] *Corelight Sensors with BroLin v28 Security Target*, Version 0.6, December 20, 2024 (ST).

[6] *Assurance Activity Report for Corelight Sensors with BroLin v28*, Version 0.3, December 20, 2024 (AAR).

[7] *Detailed Test Report for Corelight Sensors with BroLin v28*, Version 0.3, December 20, 2024 (DTR).

[8] *Evaluation Technical Report for Corelight Sensors with BroLin v28*, Version 0.3, December 20, 2024 (ETR).

[9] *Corelight Sensor AP 200, AP 520, AP 1001, AP 1100, AP 1200, AP 3000, AP 3100, AP 3200, AP 5000, AP 5002 & AP 5200 Common Criteria Guidance Document*, Version 0.2, December 20, 2024 (AGD).