National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

NIKSUN NetOmni, and NetDetector/NetVCR/LogWave running Everest software v6.0.1.0

Report Number: CCEVS-VR-VID11524-2025
Dated: May 2, 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

Daniel P Faigin
Patrick W Mallett
Mike Quintos
The Aerospace Corporation

Common Criteria Testing Laboratory

Eugene Polulyakh
Diana Polulyakh
Valeriy Polulyakh, Ph.D.
Joseph R. Maixner
Advanced Data Security, LLC

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of NIKSUN NetOmni, and NetDetector/NetVCR/LogWave appliances, running the software Everest version 6.0.1.0. 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 Advanced Data Security, LLC (ADSec) Common Criteria Testing Laboratory (CCTL) in San Jose, CA, United States of America, and was completed in April 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Advanced Data Security, LLC. 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 (NDcPP2.2e).

The Target of Evaluation (TOE) is NIKSUN NetOmni, and NetDetector/NetVCR/LogWave appliances, running the software Everest version 6.0.1.0

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 evaluation was completed in May 2025.

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 NIKSUN NetOmni, and NetDetector/NetVCR/ LogWave appliances, running Everest Software v6.0.1.0 Security Target, Version 1.8, May 1, 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 Product Compliant 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

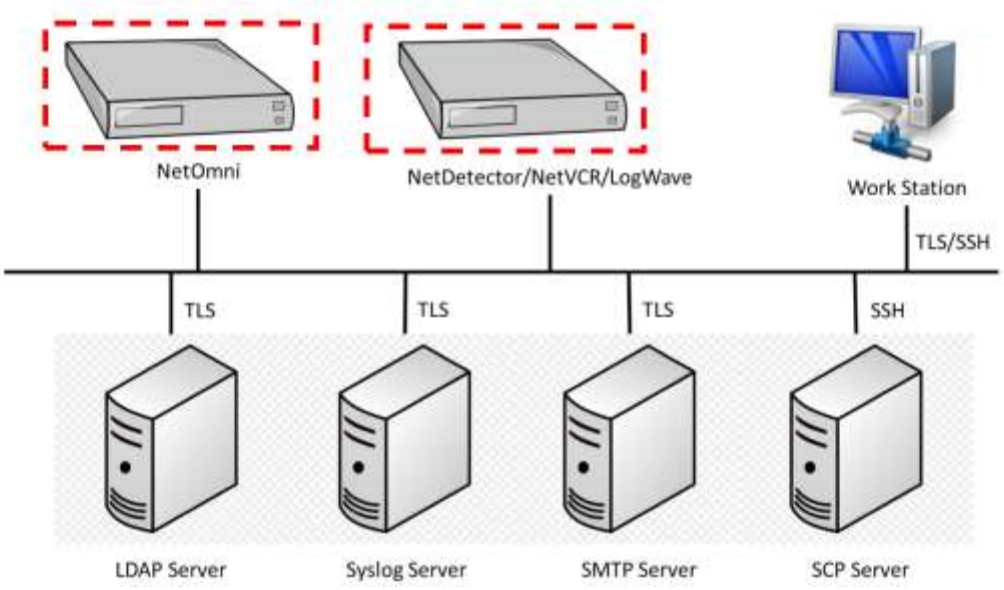
Name	Description
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	NIKSUN NetOmni, and NetDetector/NetVCR/LogWave appliances, running the software Everest version 6.0.1.0
Protection Profile	collaborative Protection Profile for Network Devices Version 2.2e, 23 March 2020
ST	NIKSUN NetOmni, and NetDetector/NetVCR/ LogWave appliances, running Everest Software v6.0.1.0 Security Target, Version 1.8, May 1, 2025
Evaluation Technical Report	Evaluation Technical Report for NIKSUN NetOmni, and NetDetector/NetVCR/ LogWave appliances, running Everest Software v6.0.1.0, Version 1.3, May 1, 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	NIKSUN, Inc.
Developer	NIKSUN, Inc.
Common Criteria Testing Lab (CCTL)	Advanced Data Security, LLC
CCEVS Validators	Daniel P Faigin, Patrick W Mallett, Mike Quintos

3. ARCHITECTURAL INFORMATION

The TOE includes the NIKSUN NetOmni, and NetDetector/NetVCR/LogWave appliances, running the software Everest version 6.0.1.0. NIKSUN NetOmni, and NetDetector/NetVCR/LogWave independently represents a TOE. Each of the appliances is running the exact same Everest software and the functionality is distinguished based on the licenses that are activated on the appliance.

The TOE consists of the physical appliance including all the hardware and the software. The TOE appliance model numbers and corresponding processor are shown in table and figure below.

Appliance	Model #	Processor	CPU Microarchitecture	OS
NetOmni	B1000	AMD EPYC 7252	AMD Zen-2	NIKOS-Max 12
NetDetector/NetVCR/LogWave	C3010	Intel Xeon Gold 6238	Intel Cascade Lake	NIKOS-Max 12



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 provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates an audit record for each auditable event. The TOE keeps local and remote audit records of security relevant events. The TOE internally maintains the date and time, which can be set manually. Each security relevant audit event includes the date, timestamp, event description, and subject identity. The TOE provides the administrator with a circular audit trail. The TOE can be configured to transmit its audit messages to an external syslog server over an encrypted channel using TLS.

4.2 CRYPTOGRAPHIC SUPPORT

The TOE relies on its NIKOS-Max FIPS Object Module and NIKOS-Max BC-FJA (Bouncy Castle FIPS Java API) to implement cryptographic methods and trusted channels. The TOE uses non-mutually authenticated TLS to secure the automatic transfer of syslog audit files and VAR logs to the Syslog Server. The TOE uses TLS to secure the connection to the LDAP/AD Server for remote authentication. When a user utilizes the "Forgot Username/Password" feature on the login screen, the TOE will send an email to the SMTPS Server over a protected TLS channel. TOE communicates with another NIKSUN appliance over TLS. X.509v3 certificates are used to support authentication mechanisms. SSH is used to secure the remote CLI interface for remote management of the TOE. SSH is also used to secure communications with the SCP Server when the TOE receives software image updates. TLS/HTTPS is used to secure the connection for remote management of the TOE via the web GUI as well as connections to other devices. The TOE will deny any connections for disallowed protocols and invalid X.509v3 certificates.

4.3 IDENTIFICATION AND AUTHENTICATION

The TOE verifies the identity of users connecting to the TOE. All users must be identified and authenticated before being allowed to perform actions on the TOE. This is true of users accessing the TOE via the local console, or through protected paths using the remote CLI via SSH or the web GUI via TLS 1.2. Users can authenticate to the TOE using a username and password. In addition, when authenticating by the remote CLI, users can instead use SSH public-key authentication. LDAP can be configured to provide external authentication. Passwords can consist of upper-case letters, lower-case letters, numbers, and a set of selected special characters. Password information is never revealed during the authentication process, including during login failures. Before a user authenticates to the device, a customizable warning banner can be configured to be displayed. In addition, via the web GUI only, the user has the option to use a "Forgot Username/Password" feature prior to authenticating.

The TOE uses X.509v3 certificates to perform non-mutual authentication for the Syslog Server. 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 TSF connects with a CRL distribution point through HTTP to confirm certificate validity and to access certificate revocation lists (CRL).

4.4 SECURITY MANAGEMENT

The TOE has a role-based authentication system where roles (permissions) are assigned to groups for the web GUI. Authorized actions for a particular user are dependent on which group they are assigned to. There are 4 initial groups: Administrator, Account Administrator, Advanced Users, and Users. Only users assigned to the Administrator group are capable of performing SFR related management functions via the web GUI and thus, are Security Administrators in the context of the evaluation. The root user is the Security Administrator user for the remote and local CLI and is able to update the TOE's software and verify it via published-hash validation.

The NDcPP's definition of "role" is synonymous with NIKSUN's definition of "permissions". NIKSUN's terminology fits into the Protection Profiles by using the term "user roles" in place of "user permissions". For the remainder of this document, "user permissions" is used to match the terminology used by Common Criteria.

4.5 PROTECTION OF THE TSF

The TOE stores passwords in a variety of locations depending on their use and encryption. They cannot be viewed by any user regardless of the user's role. The vcr and root user passwords are stored in the OS hashed by SHA-512. Web GUI passwords are stored in the PostgreSQL Database hashed with SHA-256. Pre-shared keys, symmetric keys, and private keys cannot be accessed in plaintext form by any user. There is an underlying hardware clock that is used for accurate timekeeping and is set by the Security Administrator. The TOE performs integrity checks during initial start-up (power-on) to ensure the firmware integrity. After successful integrity checks, the TOE then further performs all cryptographic algorithm self-tests for its OpenSSL and Bouncy Castle cryptographic providers. The TOE also performs self-tests on the CPU, RAM, and disk components. The TOE's DRBGs also perform their own health tests.

The version of the TOE is verified via the CLI or web GUI. The TOE is updated by the root user via the CLI. Updated software images are downloaded to the SCP Server and are transferred to the TOE via the SCP using SSH. The administrator is also capable of copying the image to a CD and manually loading it to the TOE. The TOE conducts a hash verification on the system image using SHA-256 against the known hash to ensure the integrity of the update.

4.6 TOE ACCESS

Before any user authenticates to the TOE, the TOE displays a configurable Security Administrator banner for the web GUI. The local and remote CLI interfaces display the default security banner prior to authentication that is also configurable. The TOE can terminate local CLI, remote CLI, and web GUI sessions after a specified time period of inactivity. Administrative users have the capability to terminate their own sessions.

4.7 TRUSTED PATH/CHANNELS

The TOE connects and sends data to IT entities that reside in the Operational Environment via trusted channels. In the evaluated configuration, the TOE connects to Syslog Server via TLS to send audit data for remote storage. The TLS connection to the Syslog server is over non-mutually authenticated TLS channel. TLS is used to connect to an SMTP email server for secure credentials reset. TLS is also used for the TOE's connection with the LDAP/AD Server for its remote authentication store. TLS is used for the transfer of data between the NIKSUN appliances. SSH is used for the connection to the SCP Server when the TOE receives software image updates.

TLS/HTTPS and SSH are used for remote administration of the TOE via the web GUI and remote CLI respectively.

5. ASSUMPTIONS & CLARIFICATION OF SCOPE

5.1 ASSUMPTIONS

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

- collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020

That information has not been reproduced here and the NDcPP2.2e 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 NDcPP2.2e 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.

5.2 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 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 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 NDcPP2.2e and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

The following services, capabilities, and functions, while included in the product, were not tested during the TOE's evaluation.

- Performance monitoring, service disruptions and forensics
- Traffic and network monitoring and analysis
- Event analytics, alerting, and reporting
- Security incidents, IDS, and anomaly detection

Furthermore, when operating the TOE in a manner compliant with this ST, the following features may not be used:

- NTP-based updates to TOE time
- IPv6

6. DOCUMENTATION

The following documents were available with the TOE for evaluation:

- NIKSUN NetOmni, NetDetector/NetVCR/LogWave running Everest Software v6.0.1.0 Common Criteria Guide, Version 1.4, May 1, 2025.

Only the Administrator Guide listed above, and the specific sections of the other documents referenced by that guide should be trusted for the installation, administration, and use of this product in its evaluated configuration.

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 Assurance Activity Report (NDcPP2.2e) for NIKSUN NetOmni, and NetDetector/NetVCR/ LogWave appliances, running Everest Software v6.0.1.0, Version 1.3, May 1, 2025.

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 the Common Criteria Certification document and ran the tests specified in the NDcPP2.2e including the tests associated with optional requirements. The specific test configurations and test tools utilized may be found in Section 5.5 of the AAR.

8. EVALUATED CONFIGURATION

The evaluated configuration consists of the hardware and software listed below when configured in accordance with the documentation specified in section 6.

Appliance	Model #	Processor	OS
NetOmni	B1000	AMD EPYC 7252	NIKOS-Max 12
NetDetector/NetVCR/LogWave	C3010	Intel Xeon Gold 6238	NIKOS-Max 12

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.

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.

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 NIKSUN NetOmni and NetDetector products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 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 NDcPP2.2e related to the examination of the information contained in the TSS.

The validator 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 units. 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 validator 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 validator 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 ran the set of tests specified by the assurance activities in the NDcPP2.2e and recorded the results in a Test Report, summarized in the AAR.

The validator 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 performed a public search for vulnerabilities at the following sites and did not discover any public issues with the TOE. The evaluator searched the following sources for vulnerabilities:

https://web.nvd.nist.gov/view/vuln/search

http://cve.mitre.org/cve/

https://www.cvedetails.com/vulnerability-search.php

http://www.kb.cert.org/vuls/html/search

www.exploitsearch.net

www.securiteam.com

http://nessus.org/plugins/index.php?view=search

http://www.zerodayinitiative.com/advisories

https://www.exploit-db.com/

https://www.rapid7.com/db/vulnerabilities

The terms used for the search on 4/7/2025 were as follows:

AMD EPYC 7252, Intel Xeon Gold 6238, AIDE 0.18.3, APT (Advanced Package Tool) 2.6.1, Apache 2.4.62-1,Bash 5.2.15, Firefox ESR 128.4.0, GRUB2 2.06, Linux 6.1.112, OpenJDK (JRE) 17.0.13, OpenLDAP 2.5.13, OpenSSH 9.2p1, OpenSSL 3.0.14, PAM [Pluggable Authentication Modules] 1.5.2, Perl 5.36.0, Postfix 3.7.11, PostgreSQL 15.8, Python 3.11.2, SNMP 5.9.3, Tomcat 10.1.6, auditd [Linux Audit Daemon] 3.0.9, cURL 7.88.1, syslog-ng 3.38.1, systemd 252.30, Spring [framework] 6.0.11, Spring security 6.2.3, Hibernate 6.1.7 and Bouncy Castle [FJA] 1.0.2.5.

The validator 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 Administrator Guide document listed in Section 6. No other 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. Other functionality provided by devices in the operational environment, such as the syslog server, 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: *NIKSUN NetOmni, and NetDetector/NetVCR/LogWave running Everest Software v6.0.1.0 Target, Version 1.8, May 1, 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.

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 (CPP_ND_V2.1),

[5] NIKSUN NetOmni, and NetDetector/NetVCR/ LogWave appliances, running Everest Software v6.0.1.0 Security Target, Version 1.8, May 1, 2025 (ST)

[6] Assurance Activity Report (NDcPP2.2e) for NIKSUN NetOmni, and NetDetector/NetVCR/ LogWave appliances, running Everest Software v6.0.1.0, Version 1.3, May 1, 2025 (AAR)

[7] Detailed Report (NDcPP2.2e) for NIKSUN NetOmni, and NetDetector/NetVCR/ LogWave appliances, running Everest Software v6.0.1.0, Version 1.8, May 1, 2025 (DTR)

[8] Evaluation Technical Report for NIKSUN NetOmni, and NetDetector/NetVCR/ LogWave appliances, running Everest Software v6.0.1.0, Version 1.3, May 1, 2025 (ETR)