National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

NIKSUN NetOmni, and NetDetector/NetVCR/LogWave running Everest Software v5.1.6.3

Report Number: CCEVS-VR-11204-2022

Dated: January 19, 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 George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Jenn Dotson
Sheldon Durrant
Lisa Mitchell
Clare Parran
The MITRE Corporation

Common Criteria Testing Laboratory

Kevin Zhang
Shaunak Shah
Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) Validation team assessment of the evaluation of the NIKSUN NetOmni, and NetDetector/ NetVCR/LogWave running Everest Software v5.1.6.3 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation was completed by the Acumen Security Common Criteria Testing Laboratory (CCTL) Rockville, MD, United States of America, and was completed in January 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements defined in the *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 [NDcPP22e].

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 documented in the ETR and the Assurance Activities Report (AAR). 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). Based on these findings, 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 *NIKSUN NetOmni, and NetDetector/NetVCR/LogWave running Everest Software v5.1.6.3 Security Target*, Version 0.8, January 06, 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 (PP) 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	NIKSUN NetOmni, and NetDetector/NetVCR/LogWave running Everest software v5.1.6.3
Protection Profile	*collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 [NDcPP22e]
Security Target	*NIKSUN NetOmni, and NetDetector/NetVCR/LogWave running Everest Software v5.1.6.3 Security Target,* Version 0.8, January 06, 2022
Evaluation Technical Report	*NIKSUN NetOmni, and NetDetector/NetVCR/LogWave running Everest Software v5.1.6.3 Evaluation Technical Report*, ETR Version 1.1, January 03, 2022
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	NIKSUN, Inc.
Developer	NIKSUN, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Paul Bicknell, Jenn Dotson, Sheldon Durrant, Lisa Mitchell, Clare Parran

3 Architectural Information

The TOE includes the NIKSUN NetOmni, and NetDetector/NetVCR/LogWave appliances, running the software Everest version 5.1.6.3. NIKSUN NetOmni, and NIKSUN NetDetector/NetVCR/LogWave independently represent a TOE. Each of the appliances are running the exact same Everest software and the functionality is distinguished based on the licenses that are activated on the appliance.

NetOmni's primary functionality is to provide an overview of critical operations of the monitored network. The overview includes monitoring business service disruptions, performance issues, and security incidents. NetOmni accomplishes this by providing performance monitoring, traffic analysis, and reporting systems for a network[1]. NetOmni communicates to one or more NetDetector/NetVCR/LogWave appliances to collect data from distributed point solutions. The data is aggregated from many sources based on user-defined criteria so that it can be viewed as one flow. NetOmni generates reports based on the data collected that covers network-wide services, applications, and performance. Finally, NetOmni provides real-time network-wide analysis, forensics, and event alerting.

NetDetector primary functionality is to provide security monitoring of network traffic using IDS methods and statistical anomaly detection in order to safeguard networks against cyber-attacks. The anomaly detection uses user-defined and threshold-based anomalies[2]. Users of NetDetector are notified of security breaches as soon as they occur. NetVCR is a solution for full packet capture with stream-to-disk recording, real-time indexing and application analytics for network/application performance. LogWave is an advanced log and event analytics engine that provides real-time analysis of security alerts generated by applications or services.

NetOmni, and NetDetector/NetVCR/LogWave appliances running Everest software individually represent the TOE. They are identical in terms for security and management features and independently meet all the mandatory security requirements of the Protection Profile. The TOE allows Security Administrators to access the TOE through a local CLI, remote CLI via SSH, and a web GUI via TLS/HTTPS.

3.1 Evaluated Configuration

Appliance	Model Number	Processor
NetOmni	9080	Xeon Gold 6140 (Skylake)
	9180	Xeon Gold 6140 (Skylake)
NetDetector/NetVCR/LogWave	12100	Xeon Gold 6140 (Skylake)
	12500	Xeon Gold 6152 (Skylake)

[1] Note: NetOmni's performance monitoring, traffic analysis, forensics, event alerting and reporting features are not evaluated as part of the CC evaluation.

[2] Note: NetDetector/NetVCR/LogWave traffic monitoring, IDS, anomaly detection, application analytics, and event analytics features are not evaluated as part of the CC evaluation.

The TOE evaluated configuration consists of one of the NIKSUN appliances listed above, including all the hardware and software. The TOE also requires the following environmental components to operate in the evaluated configuration:

Components	Description
NIKSUN appliance	Another instance of the TOE
LDAP Server	Remote authentication
SCP Server	Firmware updates via an SCP server
SMTP Server	Email server
Syslog Server	External storage for audit logs
Workstation	Local or remote management

3.2 Excluded Functionality

The following product functionality is not included in the CC evaluation:

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

4 Security Policy

The TOE provides the following security functions:

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 has 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.

Cryptographic Support

The TOE relies on its NIKOS FIPS Object Module and NIKOS Java Object Module to implement cryptographic methods and trusted channels. The TOE uses 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 SMTP 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 the communication 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.

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 is 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 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).

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 VCR 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.

The NDcPP22e'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 in order to match the terminology used by Common Criteria.

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 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. Power-on self-tests are executed automatically when the cryptographic module is loaded into memory. It verifies its own integrity using an HMAC-SHA-256 digest computed at build time and tests all algorithms for integrity. The TOE also performs self-tests on the CPU, RAM, and disk components. The TOE's DRBG also performs its own health tests.

The version of the TOE is verified via the CLI or web GUI. The TOE is updated by the VCR 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.

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.

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 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

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

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

6 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e and applicable Technical Decisions 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 *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.
- 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.

7 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- *NIKSUN NetOmni, and NetDetector/NetVCR/LogWave running Everest Software v5.1.6.3 Security Target*, Version 0.8, January 06, 2022
- *NIKSUN NetOmni, NetDetector/NetVCR/LogWave running Everest software v5.1.6.3 Common Criteria Guidance Addendum*, Version 1.2, January 13, 2022 [AGD]

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR and Detailed Test Reports (DTR) for NIKSUN NetOmni, and NetDetector/NetVCR/LogWave running Everest Software v5.1.6.3, which are not publicly available. The Assurance Activities Report (AAR) provides an overview of testing and the prescribed assurance activities.

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 NDcPP22e including the tests associated with optional requirements. Test activities were conducted at the Acumen test facility in Rockville, MD between November 2020 and April 2021 with Regression testing and reruns between May 2021 and January 2022.

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 DTR and ETR documents. The reader of this document can assume that 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 NIKSUN NetOmni, and NetDetector/NetVCR/LogWave running Everest Software v5.1.6.3 to be Part 2 extended, and to meet the SARs contained in the NDcPP22e.

9.1 Evaluation of Security Target

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/NetVCR/LogWave running Everest Software v5.1.6.3 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 Development Documentation

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 document. Additionally, the Evaluation team 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 Guidance Documents

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 guidance 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 Life Cycle Support Activities

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 Test Documentation and the Test Activity

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

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *Vulnerability Assessment for NIKSUN NetOmni and NetDetector*, Version 0.2, January 5, 2022. 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 Evaluation team performed a public search for vulnerabilities on November 22, 2021 and again on January 3, 2022 and did not discover any public issues with the TOE. The keywords used for the search were as follows:

- NIKSUN
- Xeon Gold 6140
- Bouncy Castle FIPS 1.0.2
- OpenSSL 1.0.2u-fips
- OpenSSH 7.5p1
- Postfix 3.5.9
- Apache Tomcat 9.0.44
- Apache 2.4.46
- Syslog-ng 3.31.2
- Openldap-client 2.4.58
- FreeBSD 11.4_15
- PostgreSQL 9.5.25

The following resources were used for the searches:

- https://nvd.nist.gov/view/vuln/search
- http://cve.mitre.org/cve
- https://www.cvedetails.com/vulnerability-search.php
- https://www.kb.cert.org/vuls/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
- https://www.niksun.com

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 suggest 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.

Consumers administering the TOE should also note that the session termination timeout for the GUI (the Web UI) and the CLI are implemented differently by the TOE. For a CLI connection, the session timeout will occur immediately when the timeout threshold is reached, whereas a Web UI connection could take up to an additional minute to time out after the timeout threshold is reached. The AGD should be consulted for additional information.

11 Annexes

Not applicable.

12 Security Target

NIKSUN NetOmni, and NetDetector/NetVCR/LogWave running Everest Software v5.1.6.3 Security Target, Version 0.8, January 6, 2022

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 requirements*, Version 3.1 Revision 5, April 2017.
3. *Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements*, Version 3.1 Revision 5, April 2017.
4. *Common Evaluation Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 5, April 2017.
5. *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 202
6. *NIKSUN NetOmni, and NetDetector/NetVCR/LogWave running Everest Software v5.1.6.3 Security Target*, Version 0.8, January 6, 2022 [ST]
7. *Assurance Activity Report for NIKSUN NetOmni and NetDetector Appliances*, Version 1.2, 01/13/2022 [AAR]
8. *NIKSUN NetOmni, and NetDetector/NetVCR/LogWave running Everest Software v5.1.6.3 Evaluation Technical Report*, ETR Version 1.1, January 03, 2022 [ETR]
9. *NIKSUN NetOmni, and NetDetector/NetVCR/LogWave running Everest software v5.1.6.3 Common Criteria Guidance Addendum*, Version 1.2, January 13, 2022 [AGD]
10. *Vulnerability Assessment for NIKSUN NetOmni and NetDetector*, Version 0.2, January 05, 2022
11. *Test Plan for NIKSUN NetOmni*, Version 1.1, 1/6/2022 [DTR]
12. *Test Plan for NIKSUN NetDetector*, Version 1.2, 1/12/2022 [DTR]