AMOSSYS

NOZOMI NETWORKS

CSPN Security Target

Product Guardian on NSG-M version 21.3.0

Category « Security administration and supervision »

Reference: CSPN-ST-Guardian on NSG-M-1.05

Date: 11/08/2021

Internal code: NZN001

EVOLUTION OF THE DOCUMENT

Revision	Date	Description	Editor(s)
1.00	13/12/2019	Document creation	Nathan CASTETS (AMOSSYS)
1.01	09/03/2020	Document revision (removal of perimeter of the Remote Collector)	Julie LEMETEYER (AMOSSYS)
1.02	12/03/2020	Document validation	Natalino PICONE (NOZOMI)
1.03	12/05/2020	Document revision after comments from ANSSI	Marion VOGT (AMOSSYS)
1.04	10/05/2021	Document revision (ToE version change)	Natalino PICONE (NOZOMI)
1.05	11/08/2021	Document revision (ToE version change)	Florian BILLON (AMOSSYS)

TABLE OF CONTENTS

1. INTRODUCTION

1.1. DOCUMENT SUBJECT

This document is written as part of the evaluation, following the ANSSI CSPN scheme, of the product« Guardian on NSG-M » developed by **Nozomi Networks**.

The TOE[1] is Guardian on NSG-M **version** 21.3.0.

This document is subject to technical and quality controls by **AMOSSYS** and validation by **Nozomi Networks**. Updates of this document are carried out by the **AMOSSYS** project team.

1.2. PRODUCT IDENTIFICATION

Vendor	**Nozomi Networks** Global HQ 575 Market Street, Suite 3650 San Francisco, CA 94105 European HQ Via Laveggio 6, CH-6850 Mendrisio, Switzerland
Link to the organization	www.nozominetworks.com
Product name	Guardian on NSG-M
Evaluated version	21.3.0
Product category	Security administration and supervision

1.3. REFERENCES

In order to establish this security target, the following documents have been consulted:

- N2OS-UserManual-21.3.0.pdf;
- N2OS-UserManual-SDK-21.3.0.pdf;
- www.nozominetwork.com/products/solution-overview/.

[1] *Target Of Evaluation*

2. PRODUCT DESCRIPTION

2.1. GENERAL DESCRIPTION

Nozomi Networks Solution is a bundle that provides network security management and intrusion detection through different entities. It is comprised of five components:

- The "Guardian", the main entity in charge of processing all the data;
- The "Remote Collector", a minimalist (optional) component that gathers data for the "Guardian";
- The "Central Management Console", a unifying management interface for architectures with several "Guardian" entities;
- "Threat Intelligence", an optional service to enhance malware and anomaly detection;
- "Smart Polling", an enhanced data extraction strategy.

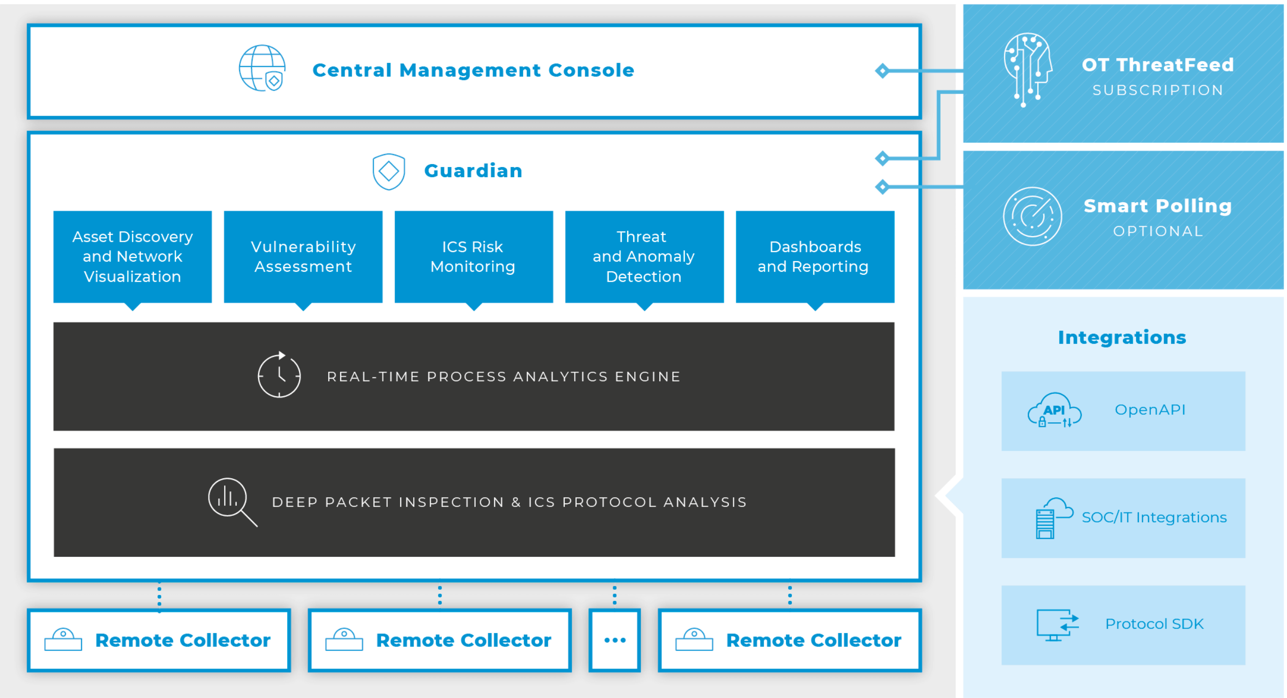


Figure 1 - Nozomi Networks Solution Architecture

The main component is the "Guardian", the processing core. It analyses, learns from network traffic in real-time and reports anomalies. It is able to deeply inspect packets through its knowledge of protocols. To gather data, the "Guardian" captures the traffic using a passive monitoring approach and optionally receives data from several "Remote Collector" which helps data analysis from remote and offsite locations.

These "Remote Collectors", if deployed, are located in the different isolated areas that need to be monitored. A "Remote Collector" is a minimalist appliance connected to a "Guardian" and acts as a remote interface that merely forwards traffic to the "Guardian", hence broadening its capture capability.

For this evaluation, "Remote Collector" are not deployed.

The results are available through a user-friendly GUI (Graphical User Interface) accessible from a web browser. The "Guardian" gathers the collected data and provides graphics and charts. The interface exposes a general view of the network, processes, alerts, reports and vulnerabilities detected in real-time. It is possible to control the access to this interface with an Active Directory database and to enable Single Sign-On functionalities with the SAML protocol.

The "Central Management Console" component is designed to easily monitor an architecture with several "Guardians" and to unify all the data.

Smart Polling is an enhanced data extraction feature, allowing the "Guardian" to contact nodes in order to gather information or to improve the already existing ones.

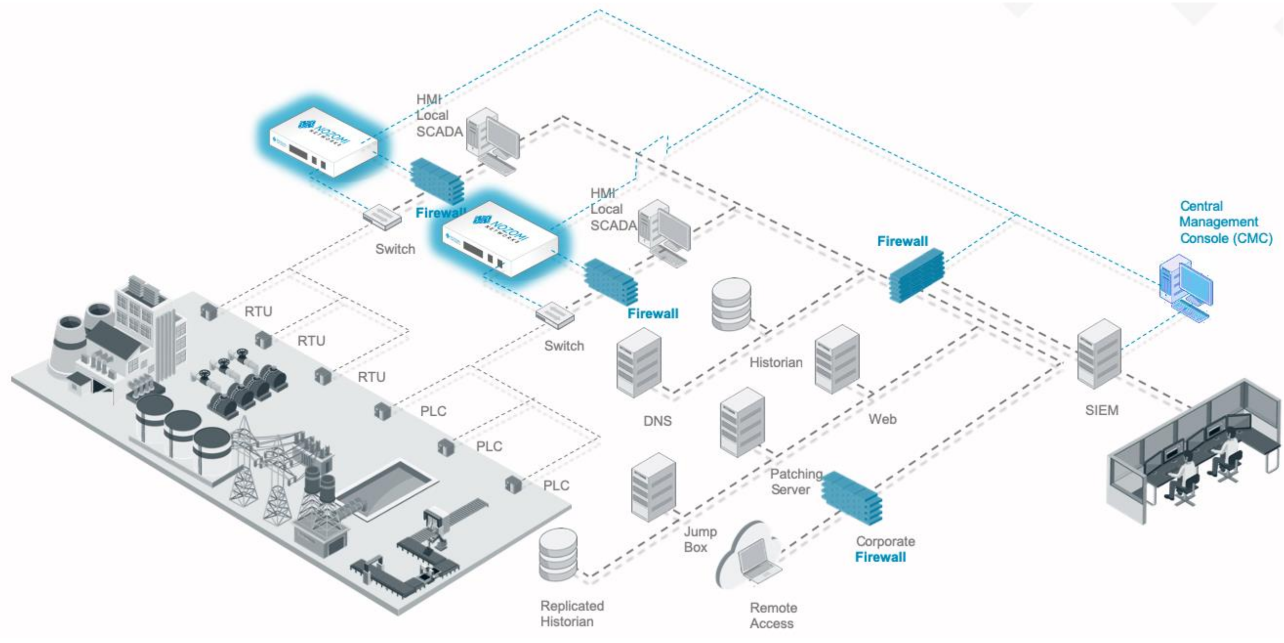
Nozomi Networks offer an optional service with subscription: Threat Intelligence. It is an online database to provide more accurate information about malwares and anomalies. The "Guardian" uses these signatures to improve intrusion detection.

Nozomi Networks also provide an SDK in order to add protocol support by the user. The language used to write a scriptable protocol is Lua.

2.2. MODE OF OPERATION

Nozomi Networks solution usually is deployed as passive detection appliance which receives all the network traffic on his dedicated network interfaces.

« Guardian » advanced technology automatically maps and visualizes the entire industrial network, including assets, connections, and protocols. Guardian monitors network communications and behavior for risks that threaten the reliability of your systems and provides the information you need to respond quickly.



The « Guardian » exposes a web interface on which users log to access the analysis information. Authentication is required for all users and it is managed through a local database of users (login/password) or via Active Directory/LDAP/SAML authentication. Once a user is logged in, it can access the *environment*, which provides a synthetic view in real-time of the state of the network. The interface also provides access to the alerts and vulnerabilities reported on the network. An alert is an event of interest observed on the network and a vulnerability is a weakness which allows an attacker to reduce the system's information insurance. Anomalies are reported as well and traces are provided to users to provide more details. The actors communicating on the network can be referred to as assets or nodes.

Administrators manage user access rights through the same interface. They can also define groups to manage access and rights more easily. A SAML module can be added to each "Guardian" to provide a SSO (Single Sign-On) feature for users. It is also possible to use the "Central Management Console" to have a more centralized view of several deployed "Guardians" (**not included** in the perimeter).

All the data observed by users either come directly from the "Guardian" sniffing the traffic on his local network (or from a "Remote Collector" whose sole task is to forward traffic to the "Guardian"). It is also possible to aggregate data from both sources.

An administrator can use the web GUI to change the main configuration parameters. Complete system configuration and customization can be performed via SSH, web CLI (Command Line Interface) or open API.

2.3. DEPENDENCIES DESCRIPTION

No specific dependencies are required by the TOE apart from the requirements detailed in section §2.4.1.

2.4. ENVIRONMENT DESCRIPTION

2.4.1. Compatible hardware and software

The Guardian is executed on the Nozomi custom OS named N2OS. It can be deployed on physical and virtual architectures. It can be purchased as a physical appliance:

- NSG-L, NSG-M, NSG-H or NSG-HS Series
- Portable P550
- NSG-R Series

It can also be purchased like as a software to be installed on a virtual machine or containers. N2OS officially supports these hypervisors/container engine:

- VMware ESXi 5.5 or newer;
- HyperV 2012 or newer;
- XEN 4.4 or newer;
- KVM 1.2 or newer;
- Docker container engine.

For this evaluation, the Guardian will be deployed on an **NSG-M appliance**.

The minimum requirements for a "Guardian" on a virtual machine are:

- 4 vCPU running at 2 GHz;
- 4 GB of RAM;
- 10 GB of minimum disk space;
- 2 or more NICs.

These specifications may be insufficient depending on the number of nodes.[2]

As "Remote Collector" and "Central Management Console" are additional/optional products of the Nozomi Networks solutions they are not part of this deployment and evaluation.

2.4.2. Operating system

N2OS is based upon a hardened FreeBSD 12.2 operating system customized to deliver a secure environment to the customers.

The system is treated as a closed system, and any unauthorized changes violate the Nozomi Networks End User License Agreement and may void the warranty and related support.

2.5. EVALUATION SCOPE

2.5.1. Perimeter

This evaluation perimeter is the "Guardian" deployed on an NSG-M appliance. The COTS and N2OS are part of the perimeter.

"Remote Collectors" are **not included** in the perimeter. The "Central Management Console" is **not included** in the perimeter because it is mainly an overlay unifying multiple "Guardian" instances. Moreover, the features Threat Intelligence and Smart Polling are **not included** in the perimeter as well.

Secondary servers like Active Directory and the SAML (SSO) protocol will not be considered for the evaluation.

2.5.2. Evaluated platform

The evaluated platform is the physical appliance NSG-M, provided by Nozomi Networks.

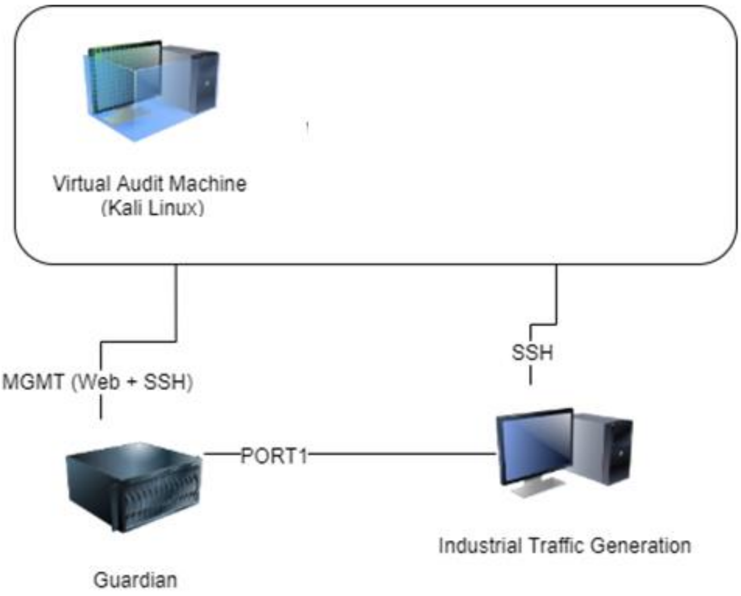


Figure 2 - Evaluation platform

[2] Technical references can be found on this webpage : https://www.nozominetworks.com/products/technical-specifications/#guardian

3. SECURITY THREAT

3.1. TYPICAL USERS DESCRIPTION

The following roles have to be considered during the security evaluation:

- **Users** of the TOE. Through the web interface, they access the different security reports and process the alerts;
- **Administrator** of the network. He is in charge of deploying the "Guardian" entities in a secure environment.
- **Administrator** of the TOE. He is in charge of configuring the "Guardian" entities. He also manages the user access and authentication rights. Finally, he has access to the logs.

3.2. CRITICAL ASSETS DESCRIPTION

Critical assets are data (or functions) rated as valuable for the TOE. The value is estimated by security criterion: availability, integrity, confidentiality and authenticity.

Critical assets to protect are as follows:

- **A1.GENERATED DATA**

  The data generated by the "Guardian" like alerts and vulnerabilities. It must not be altered.

  Security needs: Availability, integrity and confidentiality.

- **A2.CONFIGURATION DATA**

  Configuration files contain critical data on the policies to detect vulnerabilities and intrusions, and must not be altered.

  Security needs: Availability, integrity and confidentiality.

- **A3.USER DATA**

  Users credentials are stored locally on the TOE.

  Security needs: Integrity, confidentiality and authenticity.

- **A4.LOGS**

  The TOE logs its anomalies in general.

  Security need: Integrity.

- **A5.DATA ANALYSIS MECHANISMS**

  The TOE needs to run continuously on the network in order to provide relevant reports.

  Security need: Availability.

- **A6.CRYPTOGRAPHIC MATERIAL**

  Critical functions such as establishing secure communications rely on cryptographic material that must be protected.

  Security need: Integrity, Confidentiality.

3.3. ENVIRONMENT HYPOTHESIS DESCRIPTION

The following hypotheses on the environment of the TOE have to be taken into account:

- **H1.ADMINISTRATORS**

  The administrators of the TOE are trusted and well-formed to the configuration and usage of the product.

- **H2.REMOTE COLLECTORS**

  As Remote collectors consist in additional products they are not included in the perimeter of the evaluation. This implies that the integrity and availability of the data collected by these entities have to be trusted. However, the communications between "Remote Collectors" and "Guardians" use a mutually authenticated secure channel.

- **H3.PHYSICAL ENVIRONMENT**

  Physical access to the TOE is protected.

3.4. THREATS DESCRIPTION

The agents to take into account for this security evaluation are the following:

- **Forbidden entity**: a remote attacker interacting with the TOE but without legal access to the TOE;
- **Allowed entity**: a human attacker with limited access to the TOE.

Administrators (local users) are not considered as attackers.

The threats on the TOE critical assets are the following:

- **T1.COMPROMISSION OF GENERATED DATA**

  An attacker manages to corrupt the generated data by the "Guardian", altering the resulting security reports.

- **T2.COMPROMISSION OF CONFIGURATION DATA**

  An attacker manages to corrupt the configuration files located on the "Guardian".

- **T3.COMPROMISSION OF USER DATA**

  An attacker manages to corrupt user data stored locally on the "Guardian" or on an external database.

- **T4.USER IMPERSONATION**

  An attacker manages to impersonate an allowed user and access restricted data or perform illegal operations on the TOE.

- **T5.POLICY BYPASS**

  An attacker manages to bypass the configured policies in order to hide a suspicious action on the network. A policy bypass can also allow authenticated users to access restricted information on the TOE.

- **T6.LOG ALTERATION**

  An attacker manages to alter the logs in order to hide illicit activity on the TOE.

- **T7.DENIAL OF SERVICE**

  An attacker manages to suspend the activity of the TOE, hereby nullifying the analyses.

- **T8.COMPROMISSION OF CRYPTOGRAPHIC MATERIAL**

  An attacker manages to alter or steal cryptographic material.

- **T9.SOFTWARE CORRUPTION**

  An attacker manages to alter the software.

3.5. SECURITY FUNCTIONS DESCRIPTION

The necessary security functions of the TOE are the following:

- **F1.SECURE COMMUNICATIONS**

  Communications for TOE administration (Web and SSH) are encapsulated with secure protocols.

- **F2.SECURE AUTHENTICATION ON ADMINISTRATION INTERFACES**

  Authentication on the web administration interface and SSH access is based on robust mechanisms.

- **F3.SECURE UPDATES**

  The software update procedure relies on robust mechanisms to insure the authenticity of new releases.

- **F4.SECURE LOGGING**

  The TOE logs events and stores them in a secure manner.

- **F5.SECURE STORAGE OF SECRETS**

  The TOE provides secure storage sensitive data such as cryptographic material.

- **F6.CONFIGURATION CONFIDENTIALITY AND INTEGRITY**

  The access control prevents any unauthorized person to read or modify the configuration of the ToE.

- **F7.MALFORMED INPUT MANAGEMENT**

  The TOE has been developed in order to handle correctly malformed input, in particular malformed network traffic.

- **F8.ALERT MANAGEMENT**

  The TOE detects anomalous network behavior such as port scanning, mitm attacks, unencrypted communications, configuration downloads, bruteforce attacks on authentication interfaces, etc. For each security event, the TOE generates an alert stored in the postgresql database and shown on the web interface.

3.6. COVERAGE MATRIX

3.6.1. Threats and critical assets

The following matrix represents the critical assets coverage by the threats (letters “V”, “I”, “C” and “A” mean aVailability, Integrity, Confidentiality and Authenticity):

	A1.GENERATED DATA	A2.CONFIGURATION DATA	A3.USER DATA	A4.LOGS	A5.DATA ANALYSIS MECHANISMS	A6.CRYPTOGRAPHIC MATERIAL
T1.COMPROMISSION OF GENERATED DATA	**VIC**					
T2.COMPROMISSION OF CONFIGURATION DATA		**VI**			**V**	
T3.COMPROMISSION OF USER DATA			**ICA**			
T4.USER IMPERSONATION	**I**	**I**	**IC**			
T5.POLICY BYPASS	**I**		**IC**	**I**		
T6.LOG ALTERATION				**I**		
T7.DENIAL OF SERVICE					**V**	
T8.COMPROMISSION OF CRYPTOGRAPHIC MATERIAL						**IC**
T9.SOFTWARE CORRUPTION		**I**			**V**	**IC**

Table 1 critical assets coverage by threats

3.6.2. Threats and security functions

The following matrix represents the threats coverage by security functions:

	F1.SECURE COMMUNICATIONS	F2.SECURE AUTHENTICATION ON ADMINISTRATION INTERFACES	F3.SECURE UPDATES	F4.SECURE LOGING	F5.SECURE STORAGE OF SECRETS	F6.CONFIGURATION CONFIDENTIALITY AND INTEGRITY	F7.MALFORMED INPUT MANAGEMENT	F8.ALERT MANAGEMENT
T1.COMPROMISSION OF GENERATED DATA	√	√				√	√	√
T2.COMPROMISSION OF CONFIGURATION DATA		√				√		
T3.COMPROMISSION OF USER DATA		√				√		
T4.USER IMPERSONATION	√	√						
T5.POLICY BYPASS							√	√
T6.LOG ALTERATION				√				
T7.DENIAL OF SERVICE	√	√					√	√
T8.COMPROMISSION OF CRYPTOGRAPHIC MATERIAL					√			
T9.SOFTWARE CORRUPTION		√	√		√			

Table 2 – Threats coverage by security functions

End of the document