NOZOMI NETWORKS

DATA SHEET

Threat Intelligence

Detect Emerging OT and IoT Threats and Vulnerabilities

Nozomi Networks **Threat Intelligence**™ continuously updates **Guardian**™ appliances with rich data and analysis so you can detect and respond to emerging threats faster.

Guardian correlates Threat Intelligence information with broader environmental behavior to deliver maximum security and operational insight.

See

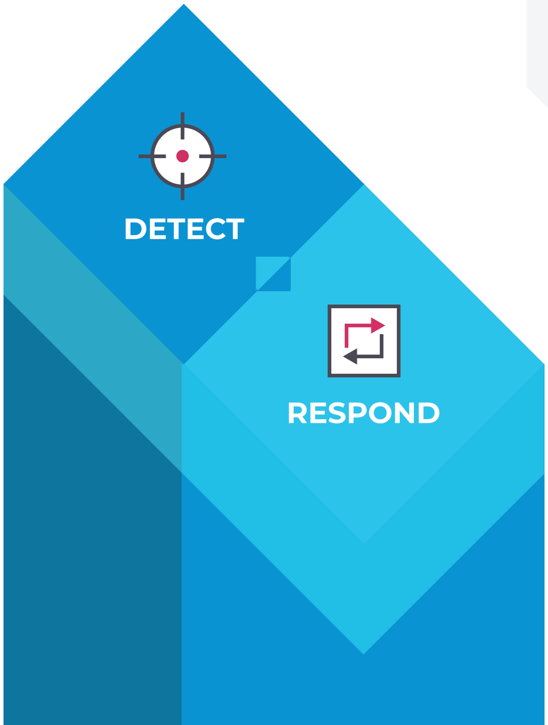
What's on your network and how it's behaving

Detect

Cyber threats, risks and anomalies for faster response

Unify

Security, visibility and monitoring across all your assets



Detect

Intelligence that Reduces the Mean-Time-to-Detection (MTTD)

Rapidly Detect Threats and Identify Vulnerabilities

Up-to-Date Threat Intelligence

Delivers continuously updated OT and IoT threat and vulnerability intelligence

Detects early stage and late stage advanced threats and cyber risks

Identifies assets at risk of attack with OT and IoT vulnerability assessment

Extensive Threat Indicators

Provides detailed threat information:

- Yara rules
- Packet rules
- STIX indicators
- Threat definitions
- Threat knowledgebase
- Vulnerability signatures

Significantly Strengthen Your Security Posture

OT and IoT Threat Insights

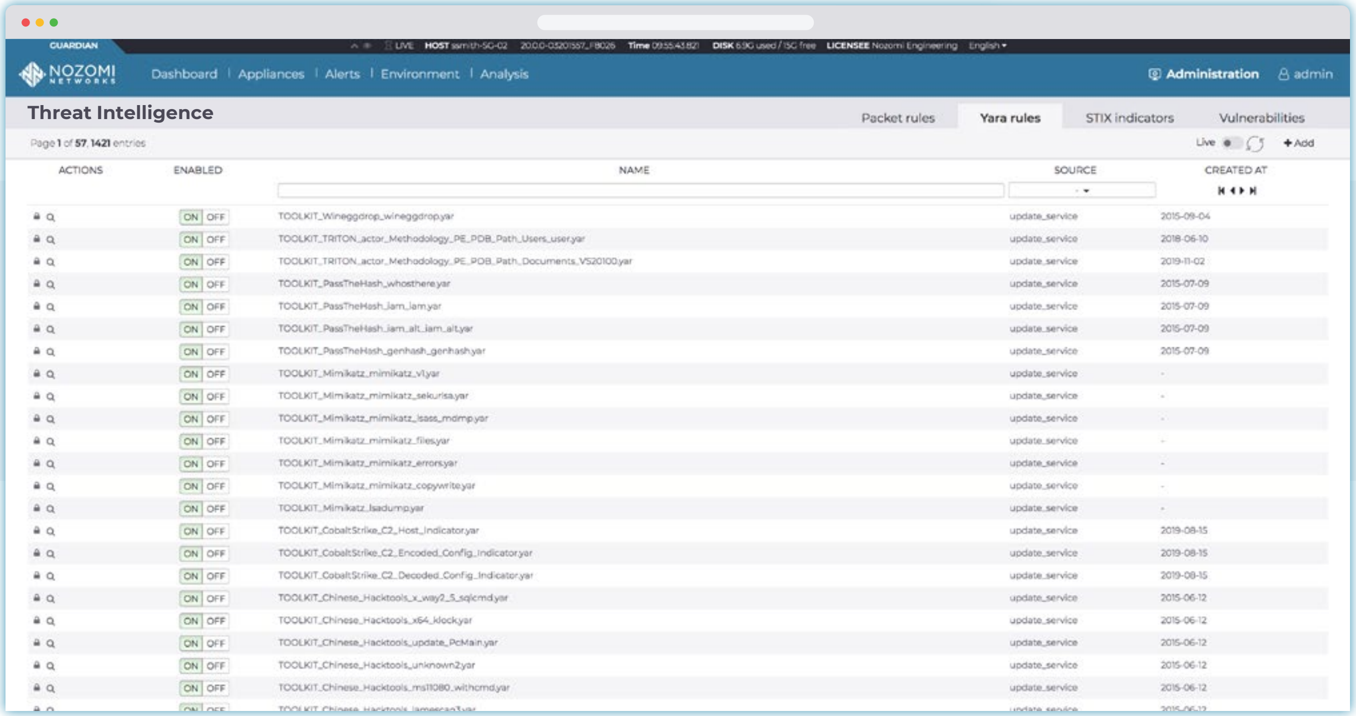
Provides an accurate assessment of your security posture through full network visibility with integrated threat intelligence

Provides the information you need to effectively manage OT and IoT risks

High Performance for Fast MTTD

Conducts analysis on local Guardian physical and virtual appliances for accelerated threat detection

Delivers immediate, accurate alerts grouped into incidents for fast response



Threat Intelligence

Page 1 of 57, 1421 entries

ACTIONS	ENABLED	NAME	SOURCE	CREATED AT
🔒 🔍	ON OFF	TOOLKIT_Wineggdrop_wineggdrop.yar	update_service	2015-09-04
🔒 🔍	ON OFF	TOOLKIT_TRITON_actor_Methodology_PE_PDB_Path_Users_user.yar	update_service	2018-06-10
🔒 🔍	ON OFF	TOOLKIT_TRITON_actor_Methodology_PE_PDB_Path_Documents_VS20100.yar	update_service	2019-11-02
🔒 🔍	ON OFF	TOOLKIT_PassTheHash_whosthere.yar	update_service	2015-07-09
🔒 🔍	ON OFF	TOOLKIT_PassTheHash_iam_iam.yar	update_service	2015-07-09
🔒 🔍	ON OFF	TOOLKIT_PassTheHash_iam_alt_iam_alt.yar	update_service	2015-07-09
🔒 🔍	ON OFF	TOOLKIT_PassTheHash_genhash_genhash.yar	update_service	2015-07-09
🔒 🔍	ON OFF	TOOLKIT_Mimikatz_mimikatz_v1.yar	update_service	-
🔒 🔍	ON OFF	TOOLKIT_Mimikatz_mimikatz_sekurlsa.yar	update_service	-
🔒 🔍	ON OFF	TOOLKIT_Mimikatz_mimikatz_lsass_mdmp.yar	update_service	-
🔒 🔍	ON OFF	TOOLKIT_Mimikatz_mimikatz_files.yar	update_service	-
🔒 🔍	ON OFF	TOOLKIT_Mimikatz_mimikatz_errors.yar	update_service	-
🔒 🔍	ON OFF	TOOLKIT_Mimikatz_mimikatz_copywrite.yar	update_service	-
🔒 🔍	ON OFF	TOOLKIT_Mimikatz_lsadump.yar	update_service	-
🔒 🔍	ON OFF	TOOLKIT_CobaltStrike_C2_Host_Indicator.yar	update_service	2019-08-15
🔒 🔍	ON OFF	TOOLKIT_CobaltStrike_C2_Encoded_Config_Indicator.yar	update_service	2019-08-15
🔒 🔍	ON OFF	TOOLKIT_CobaltStrike_C2_Decoded_Config_Indicator.yar	update_service	2019-08-15
🔒 🔍	ON OFF	TOOLKIT_Chinese_Hacktools_x_way2_5_sqlcmd.yar	update_service	2015-06-12
🔒 🔍	ON OFF	TOOLKIT_Chinese_Hacktools_x64_klock.yar	update_service	2015-06-12
🔒 🔍	ON OFF	TOOLKIT_Chinese_Hacktools_update_PcMain.yar	update_service	2015-06-12
🔒 🔍	ON OFF	TOOLKIT_Chinese_Hacktools_unknown2.yar	update_service	2015-06-12
🔒 🔍	ON OFF	TOOLKIT_Chinese_Hacktools_ms11080_withcmd.yar	update_service	2015-06-12
🔒 🔍	ON OFF	TOOLKIT_Chinese_Hacktools_lamescan3.yar	update_service	2015-06-12

Threat Intelligence provides continuously updated and detailed threat information.

Respond

Detailed Alerts and Forensic Tools for Fast Response

Quickly Respond Using Detailed, Accurate Information

Accurate Threat Intelligence

Ensures valid threat insights based on the expertise of Nozomi Networks Labs, a team of specialized security researchers

Delivers accurate rules subjected to rigorous testing before release to minimize false positives

Detailed, Helpful Alerts

Provides detailed alerts that pinpoint what occurred

Groups alerts into incidents, providing security and operations staff with a simple, clear, consolidated view of what's happening on their network

Swiftly Analyze Incidents and Simplify IT/OT Processes

Simplified IT/OT Security Processes

Reduces costs with a single, comprehensive OT and IoT threat detection and vulnerability assessment

Integrates with IT security infrastructure for streamlined security processes, see: **nozominetworks.com/integrations**

Harmonizes security data across enterprise tools for cohesive response

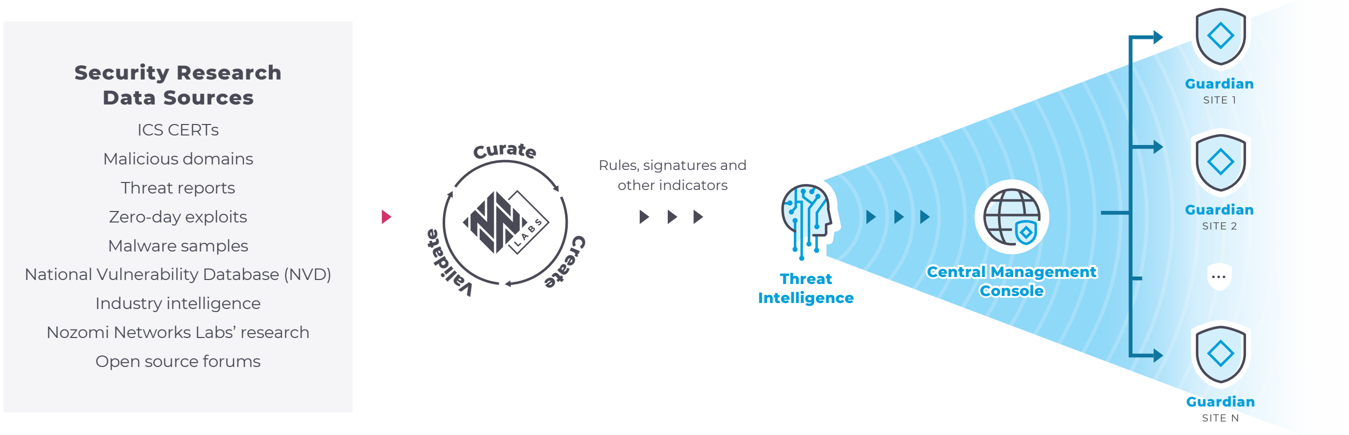
Fast Forensic Analysis

Focuses effort with Smart Incidents™ that:

- Correlate and consolidate alerts
- Provide operational and security context
- Supply automatic packet captures

Decodes incidents with Time Machine™ before and after system snapshots

Provides answers fast with a powerful ad hoc query tool



Continuous Threat Research reduces the time to detect active threats and vulnerabilities.

Products and Services

PRODUCT

Guardian provides industrial strength OT and IoT security and visibility. It combines asset discovery, network visualization, vulnerability assessment, risk monitoring and threat detection in a single solution. Guardian accelerates security and simplifies IT/OT convergence.

PRODUCT

The **Central Management Console** (CMC) consolidates OT and IoT risk monitoring and visibility across many distributed sites, at the edge or in the cloud. It integrates with IT security infrastructure for streamlined workflows and faster response to threats and anomalies.

SUBSCRIPTION

The **Threat Intelligence** service delivers ongoing OT and IoT threat and vulnerability intelligence. It helps you stay on top of the dynamic threat landscape and reduce your mean-time-to-detection (MTTD).

SUBSCRIPTION

The **Asset Intelligence** service delivers ongoing OT and IoT asset intelligence for faster and more accurate anomaly detection. It helps you focus efforts and reduce your mean-time-to-response (MTTR).

GUARDIAN ADD-ON

Smart Polling adds low-volume active polling to Guardian's passive asset discovery for enhanced asset tracking, vulnerability assessment and security monitoring.

GUARDIAN ADD-ON

Remote Collectors capture data in remote, distributed locations and send it to Guardian for analysis, improving visibility while reducing deployment costs.

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks is the leader in OT and IoT security and visibility. We accelerate digital transformation by unifying cybersecurity visibility for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation and other OT sites around the world. Our innovation and research make it possible to tackle escalating cyber risks through exceptional network visibility, threat detection and operational insight.

nozominetworks.com