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 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

Security Research Data Sources
ICS CERTs
Malicious domains
Threat reports
Zero-day exploits
Malware samples
National Vulnerability Database (NVD)
Industry intelligence
Nozomi Networks Labs’ research
Open source forums

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

**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.

**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).

**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).

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

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

**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.