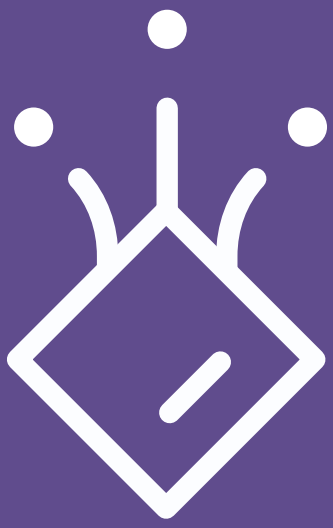
NOZOMI NETWORKS



PRODUCT OVERVIEW

Threat Intelligence

Actionable OT/IoT Threat and Vulnerability Information to Prevent Incidents from Becoming Outages

SOC teams charged with detecting, investigating and responding to OT and IoT threats typically lack the actionable threat intelligence needed to stay ahead of adversaries targeting their environments. With threat actors using AI to discover vulnerabilities and create malware faster than traditional defenses can respond, IT-centric threat intelligence services, signature-only OT/IoT threat intelligence and manual IoC updates don't suffice.

Defenders need to leverage both curated and AI-powered threat intelligence that helps them identify emerging threats earlier, reduce reliance on manual analysis and shorten the time between threat discovery and defense.

The Nozomi Threat Intelligence subscription provides continuous insights into the unique attack techniques and vulnerabilities specific to OT and IoT processes and devices. Curated by Nozomi Networks Labs, it sends detailed threat information in the form of YARA, packet and Sigma rules; STIX and vulnerability indicators; and threat definitions directly to Guardian network sensors, Arc endpoint sensors and the Vantage SaaS platform, so you can detect and respond more quickly.

AI-powered Threat Detection to Stop Emerging Threats

Nozomi Threat Intelligence features an AI-powered threat detection engine that enhances our curated threat intelligence by identifying emerging threats, malicious files, malware variants and evolving attack activity across converged OT/IT/IoT environments — before signatures or known indicators are available. The AI engine:

- **Analyzes suspicious file samples** collected through globally deployed Nozomi sensors
- **Alerts Nozomi platform users and subscribers** on novel, high-confidence malware detections
- **Prompts Nozomi Networks Labs researchers** to create signatures for confirmed new malware

Benefits

Accelerated detection and response with continuously updated OT/IoT-specific intelligence fed into the Nozomi platform

Improved SOC efficiency with seamless integration into SIEM and SOAR platforms

Clear visibility into cross-domain attack paths with integrated Mandiant Threat Intelligence

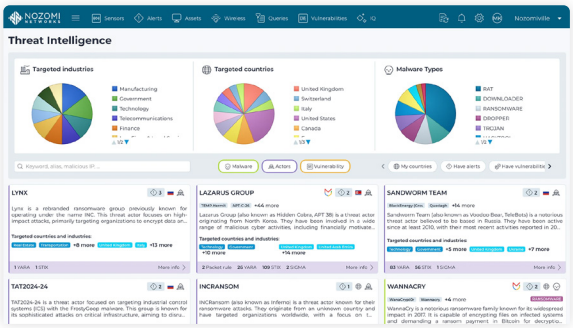
AI-powered detection of emerging threats before signatures or known indicators are available

Comprehensive Insights into OT & IoT Threat Actor Behaviors

With hundreds or thousands of alerts that need to be waded through daily, critical alerts needing immediate attention can be easily overlooked. Nozomi Threat Intelligence groups alerts into incidents, providing a clear, consolidated view of what's happening in your network. Vantage IQ further highlights the most urgent alerts in context, for instant awareness to critical issues.

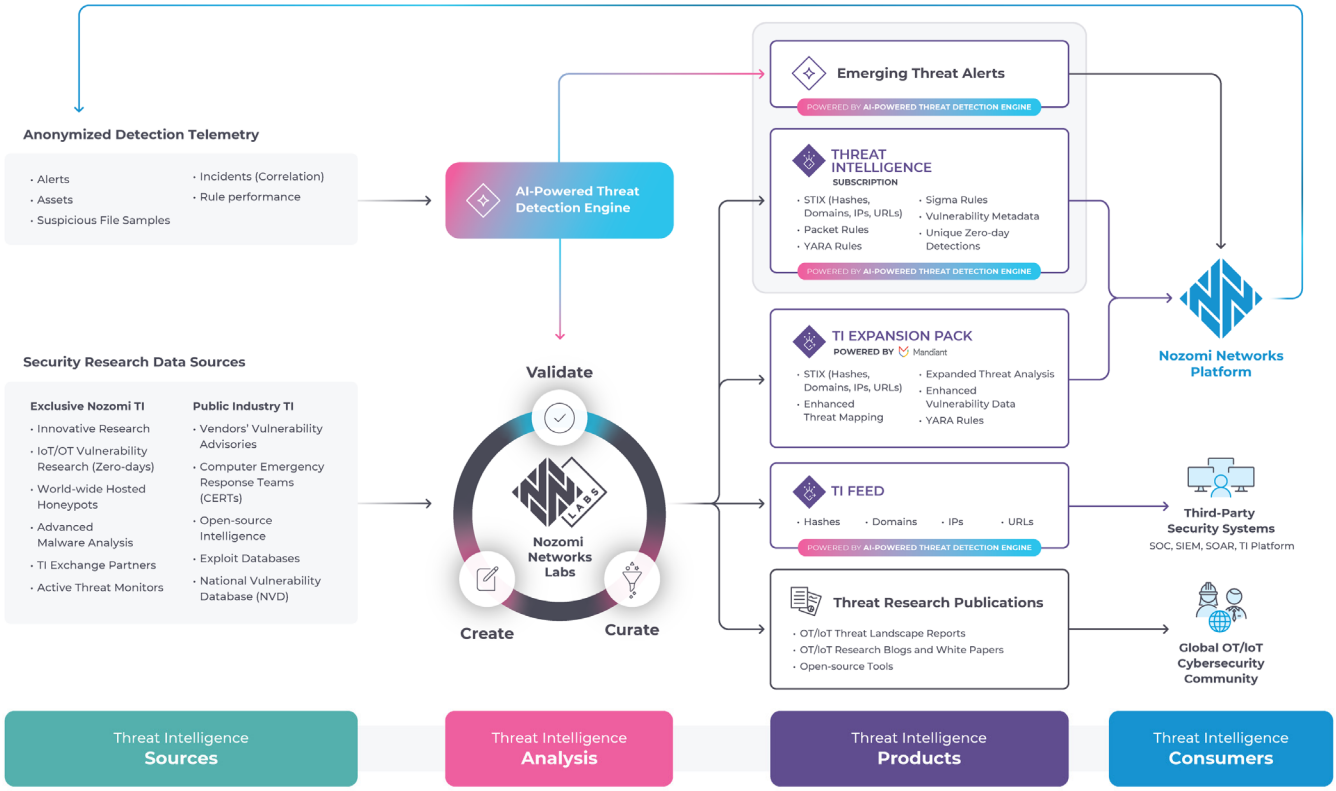
At-a-Glance Threat Cards

Threat intelligence is distilled into information-packed threat cards available in Vantage, with details on threat actors and associated exploits, malware, vulnerabilities and MITRE ATT&CK® TTPs, with mitigation suggestions and links to external references. The Nozomi TI Expansion Pack, Powered by Mandiant, integrates relevant Mandiant IOCs and TTPs into our threat intelligence feed and threat cards, including IT-borne threats that can move into OT.



More Than a Raw IoC Feed

The Nozomi Networks Labs team analyzes threat and vulnerability information from more than a dozen public and private data sources, anonymized telemetry from across our customer base and confirmed malware samples from our AI-powered threat detection engine.



Want to Know More?

Visit the Threat Intelligence webpage to learn more or request a demo.

Learn More

nozominetworks.com/products/threat-intelligence/

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com