NOZOMI NETWORKS

PRODUCT OVERVIEW

Threat Intelligence

Quickly Detect Threats to OT/IoT Systems and Defend Against Cyberattacks

With organizations leveraging OT and IoT solutions from different vendors, all running proprietary software and applications, there are more cybersecurity risks and entry points for potential attacks. Identifying and defending against emerging threats and vulnerabilities has become even more challenging.

Nozomi Networks Threat Intelligences service, available as an add-on for Guardian sensors, enables you to effectively manage OT/IoT threats and strengthen the security posture of your OT/IoT environments. Leveraging the extensive expertise and research of Nozomi Networks Labs, Threat Intelligence enables security analysts to quickly and accurately identify vulnerabilities and emerging threats, prioritize critical threats for immediate attention, and respond with actionable intelligence to protect your OT/IoT environments.

Our Threat Intelligence provides detailed threat information for an extensive list of threat indicators:

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

Rules detecting vulnerabilities and threats are subject to rigorous testing to minimize false positives.

Nozomi Networks' Threat Intelligence is also available as a feed that can be used outside our Guardian and Vantage platforms, with other third-party security products.

Nozomi Networks' Threat Intelligence helps you:

Rapidly detect
threats and vulnerabilities

Prioritize action
with detailed alerts

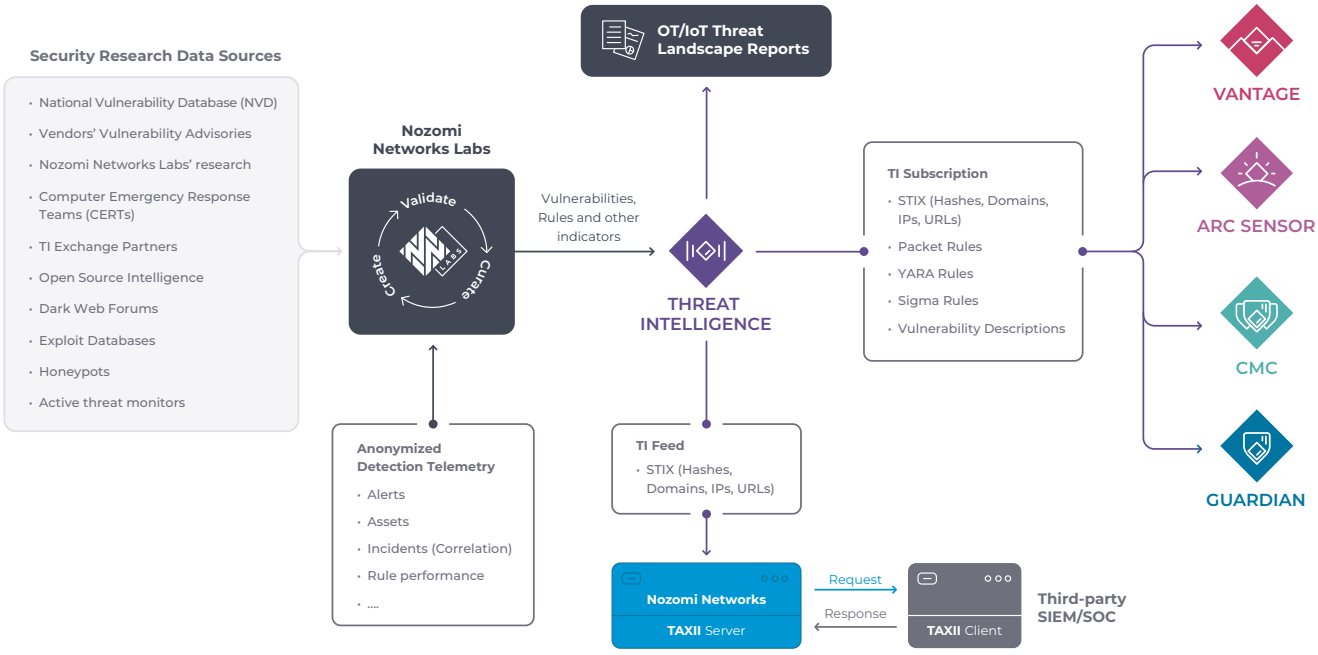
Quickly respond
with accurate information

Prioritize Action with Detailed Alerts

With hundreds or thousands of alerts that need to be waded through daily, critical alerts needing immediate attention can be easily overlooked. Nozomi Networks Threat Intelligence groups alerts into incidents, providing security and operations staff with a clear, consolidated view of what's happening on their network. Alerts contain detailed information pinpointing security and reliability anomalies, enabling security analysts to address critical alerts immediately and minimize disruption to operations.

Quickly Respond to Incidents with Accurate Information

In an ever-evolving threat landscape, security analysts need thorough knowledge of the threats that are imperative to their environment in order to respond accordingly. New or "malicious" device activities are analyzed with the operational and security context of the device to detect vulnerabilities. The Time Machine feature helps decode incidents by comparing before and after system snapshots to gain a deeper understanding of what is happening on the network. You can also drill down further into vulnerabilities with the ad-hoc query tool.



Want to Know More?

Visit the Threat Intelligence webpage to learn more or to 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

© 2023 Nozomi Networks, Inc. | All Rights Reserved.

nozominetworks.com