



Nozomi Hour

The latest OT/IoT
cybersecurity industry
updates and insights

04.2025 – 06.2025

Anton Shipulin, CISSP, CSSA, NNCE

Industrial Cybersecurity Evangelist, Nozomi Networks

Anton.Shipulin@nozominetworks.com

Introduction / Anton Shipulin

- An Industrial Cybersecurity Evangelist at **Nozomi Networks, NNCE, NNSA**
- A professional with **15+ years of experience** in Industrial Cybersecurity
- A coordinator for the Middle East at the Spain-based **Industrial Cybersecurity Center**
- A contributor to multiple industrial cybersecurity **community projects**
- Certified SCADA Security Architect (**CSSA**), **CISSP**

Agenda

04.2025 – 06.2025

1. OT/IoT **threat landscape** updates: incidents, vulnerabilities, and attack techniques
2. OT/IoT security **regulation, standards**, and frameworks news
3. OT/IoT security **technology trends, research, tools**, and best practices
4. A dedicated **discussion** for company-specific interests and concerns

1. Threat landscape updates

2. Regulation news

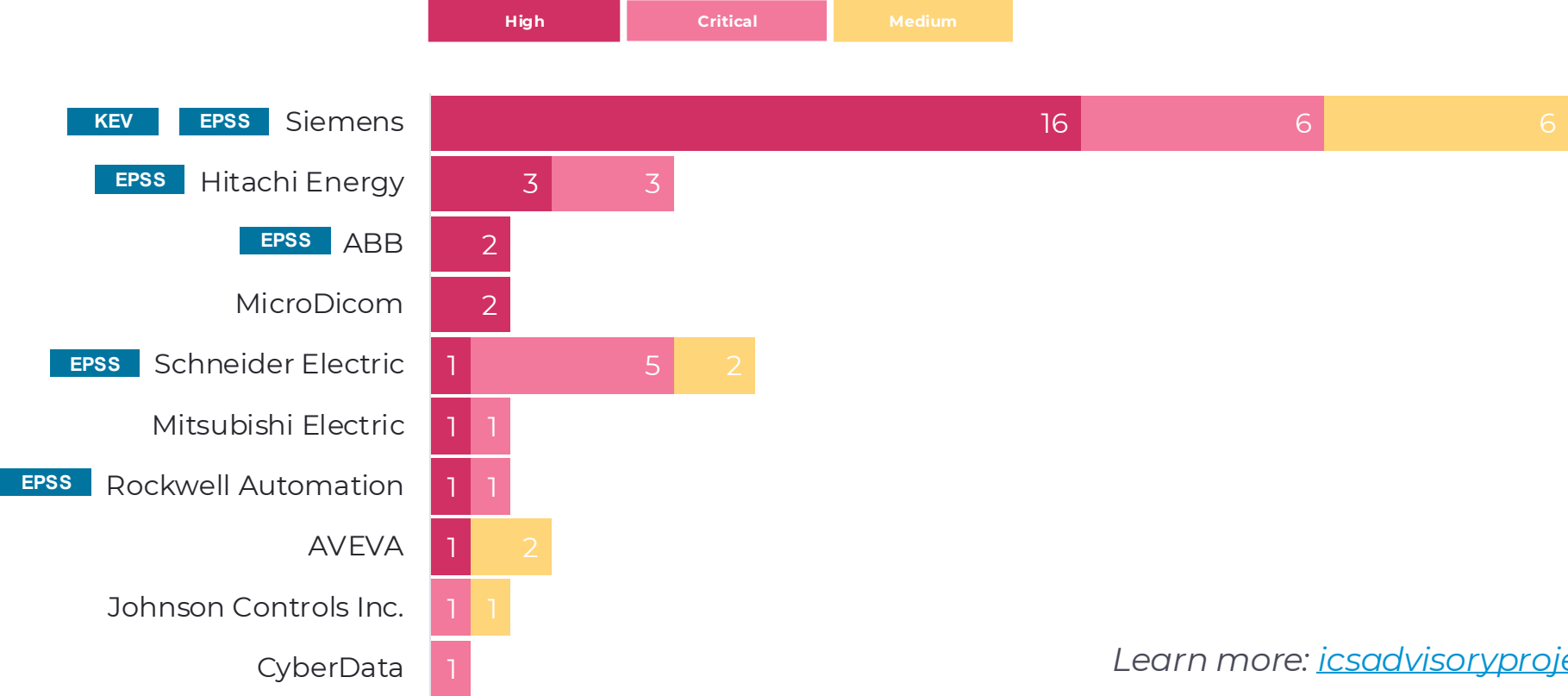
3. Technology trends

4. Discussion time



OT Vulnerability Snapshot





Number of CISA ICS Advisories by Vendor and CVSS Severity



Learn more: icsadvisoryproject.com

Vulnerability Prioritization Example / Vantage








Assets with KEVs

Asset	KEVs	%
 Catalyst 4500 Series	34	33.7% <div><div></div></div>
 iPad Pro 12.9" 2nd Gen (Wi-Fi)	33	32.7% <div><div></div></div>
 iPad	33	32.7% <div><div></div></div>
 EC2AMAZ-UGLRFRT	1	1.0% <div><div></div></div>

CVE criticality vs exploitability



Assets with exploitable CVEs

Asset	CVEs	%
 Catalyst 4500 Series	496	21.6% <div><div></div></div>
 iPad Pro 12.9" 2nd Gen (Wi-Fi)	483	21.1% <div><div></div></div>
 iPad	483	21.1% <div><div></div></div>
 plc179.ACME0.corporationnet.com	60	2.6% <div><div></div></div>
 plc160.ACME0.corporationnet.com	60	2.6% <div><div></div></div>
 plc180.ACME0.corporationnet.com	60	2.6% <div><div></div></div>
 plc167.ACME0.corporationnet.com	60	2.6% <div><div></div></div>

Open KEVs

KEV	Assets	%
CVE-2021-1782	3	3.0% <div><div></div></div>
CVE-2020-27930	3	3.0% <div><div></div></div>
CVE-2020-27932	3	3.0% <div><div></div></div>
CVE-2020-27950	3	3.0% <div><div></div></div>
CVE-2020-9934	3	3.0% <div><div></div></div>
CVE-2021-1789	3	3.0% <div><div></div></div>
CVE-2021-30661	3	3.0% <div><div></div></div>

Open CVEs

4.71K

Critical
760
CVSS score ≥ 9

High score
3.22K
CVSS score ≥ 7

KEV
101
Known exploited

Exploitable
97
EPSS score $\geq 50\%$

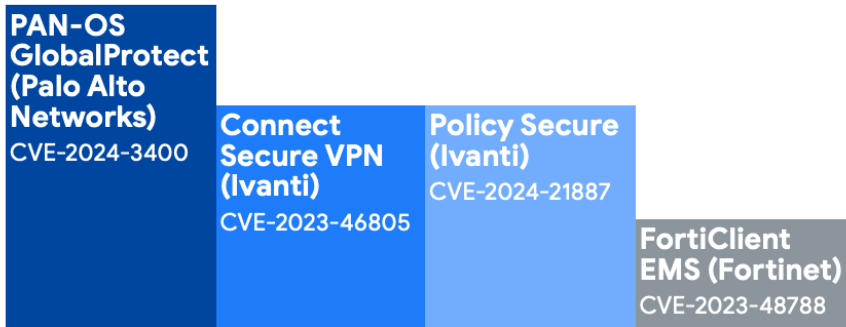
High EPSS score open CVEs

CVE	Assets	%
CVE-2019-12255	90	92.8% <div><div></div></div>
CVE-2016-3115	1	1.0% <div><div></div></div>
CVE-2016-6210	1	1.0% <div><div></div></div>
CVE-2016-6515	1	1.0% <div><div></div></div>
CVE-2018-15473	1	1.0% <div><div></div></div>
CVE-2023-38408	1	1.0% <div><div></div></div>
CVE-2013-3900	1	1.0% <div><div></div></div>

Mandiant Threat Report / M-Trends 2025

Data, Insights, and Recommendations From the Frontlines

Most Frequently Exploited Vulnerabilities



Initial Infection Vector, 2024



Initial Infection Vector, 2024
Ransomware-Related



Learn more: <https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025>

Notable Public Cyber-Physical Incidents



USA / Manufacturing

April 2025. A ransomware attack disrupted operations at **Sensata Technologies**, a global industrial sensor and controls manufacturer. The incident temporarily impacted critical business functions including shipping, receiving, manufacturing, and support services.



USA / Manufacturing

April 2025. A cyberattack caused production slowdowns at **Masimo Corporation**, a health technology manufacturer. Several facilities operated below normal capacity, leading to delays in processing, fulfilling, and shipping customer orders.



USA / Metallurgy

May 2025. Following a cyberattack involving unauthorized access to IT systems, **Nucor Corporation**, a leading steelmaker, temporarily halted production at multiple sites. The shutdown was a precautionary response to protect operations and data integrity.

All cybersecurity incidents were disclosed through an 8-K filing submitted to the U.S. Securities and Exchange Commission (SEC).

Sources:

- <https://icsstrive.com>
- <https://eurepoc.eu>

Notable Threat Reports with TTPs & IoCs

Microsoft

Void Blizzard targets critical sectors for espionage

<https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/>

Cisco Talos

Newly identified wiper malware “PathWiper” targets critical infrastructure in Ukraine

<https://blog.talosintelligence.com/pathwiper-targets-ukraine>

Fortinet

Investigating Iranian Intrusion into Strategic Middle East Critical Infrastructure

<https://www.fortinet.com/blog/threat-research/fortiguard-incident-response-team-detects-intrusion-into-middle-east-critical-national-infrastructure>

US CISA

Russian GRU Targeting Western Logistics Entities and Technology Companies

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a>

1. Threat landscape updates

2. Regulation news

3. Technology trends

4. Discussion time



Post-Quantum Cryptography (PQC) Migration Roadmap

- **Preparation:** Learn how to identify relevant stakeholders, assess vulnerabilities, and align organizational goals with migration timelines.
- **Baseline Understanding:** Develop an inventory of cryptographic assets and prioritize critical resources.
- **Planning and Execution:** Acquire or develop quantum-safe solutions and implement them with precision.
- **Monitoring and Evaluation:** Establish robust tracking measures and continuously assess cryptographic security as quantum threats evolve.



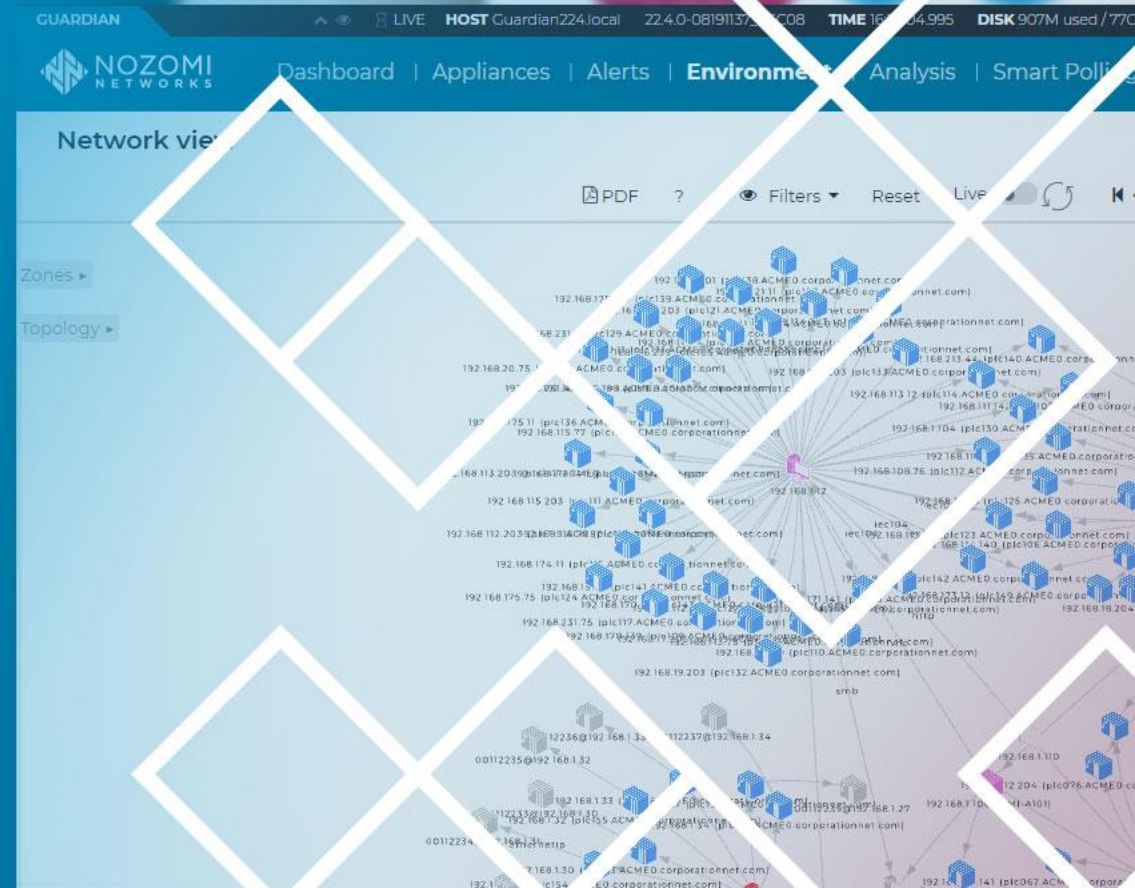
Learn more: <https://www.mitre.org/news-insights/news-release/post-quantum-cryptography-coalition-unveils-pqc-migration-roadmap>

1. Threat landscape updates

2. Regulation news

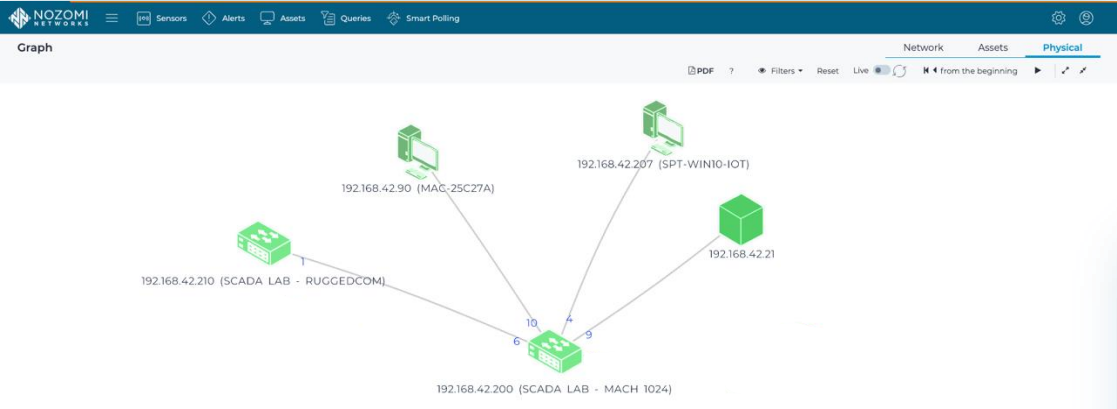
3. Technology trends

4. Discussion time

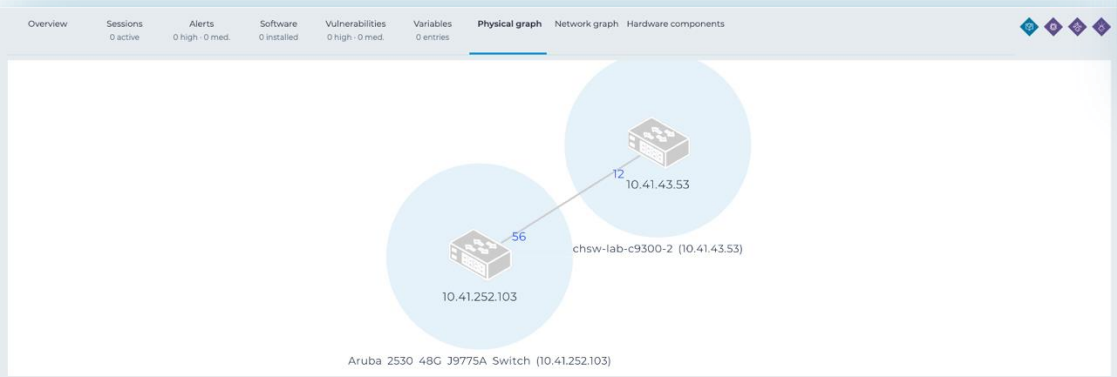


Nozomi Networks / Physical Network Mapping

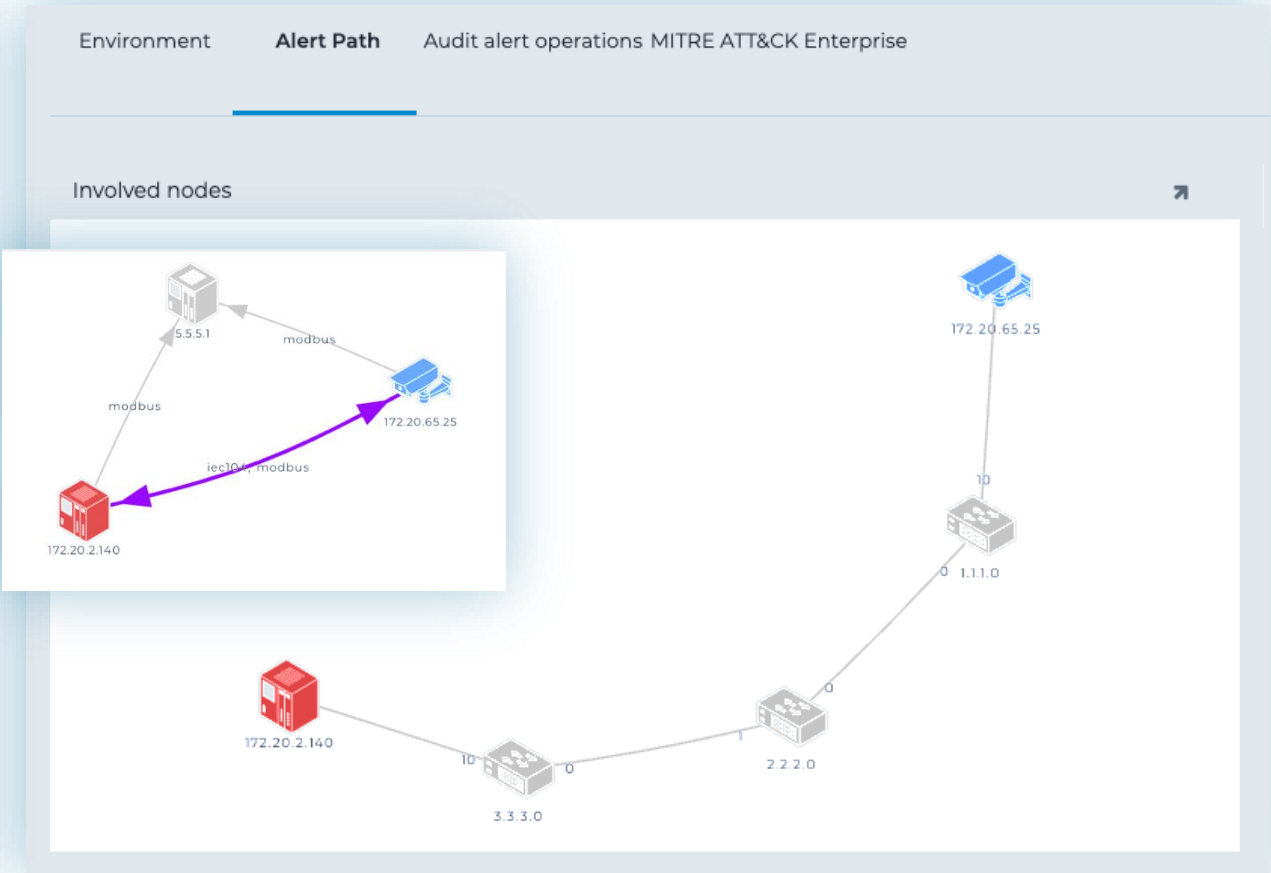
Trace physical connections from assets to network infrastructure



Physical Graph: Device-to-Switch Physical Link



Physical Graph On Asset Details Page



Alert Path Graph On Alert Details Page

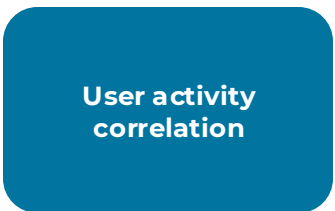
Nozomi Arc / Malicious file detection (YARA)



Arc Endpoint Security capabilities



Detect the use of USB devices and malicious HIDs



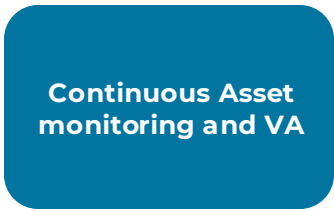
Correlate events with user's behavior



Monitor local events for signs of suspicious activity



Detect malicious file patterns also when not transferred over the network

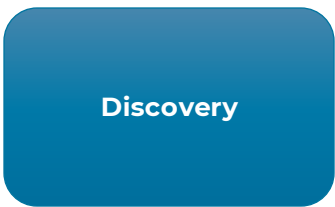


Collect endpoint inventory, security and performance data

Arc Network Sensor capabilities



Passive analysis



Standard lightweight network announcements to discover neighboring devices



Enrich asset data via surgical active queries

Nozomi Networks Academy Video / Alert Tuning

Learn how to tune alerts to better fit your needs and avoid alert fatigue



What is Alert Tuning?

Provides an overview of alert tuning.



Security Profiles (Advanced)

Provides an advanced look at security profiles.



Methods of Alert Tuning

Introduces common methods of tuning alerts.



Tuning Rules

Introduces how different rules can affect how alerts trigger.



Detection Approach

Introduces common detection approaches.



Tuning Rules (Advanced)

Provides an advanced look at tuning rules.



Security Profiles

Introduces how security profile changes affect alerts.



Thresholds

Introduces how different threshold settings affect alerts.

Learn more: <https://academy.nozominetworks.com/path/alert-tuning-essentials>

Nozomi Networks Professional Services Offering



Post-Deployment

Access to Deep Expertise

Optimization Services

40 hours bundle for flexible access to Professional Services' expertise to be consumed in 12 months

Health Check Services

Operational Checks, Architectural Assessments, and Alert Reviews performed twice a year at regular cadence.



Ongoing Operations

Maintain Value over Time

New

Operational Platform Statement of Work

Tailored operational services based on the customer's needs and budget through a fixed Price SOW

Designated Engineer

Part-Time (8hrs/w) or Full Time (40hrs/w) resource acting as an extended part of customer's team

New Nozomi PS service offering available from the 1st of July 2025

Nozomi Hour / Slide Decks and Recordings



Nozomi Hour | June 2024 |
The Rise of OT Hacktivism



Nozomi Hour | January 2024 |
Community Power



Nozomi Hour | March 2024 |
Prioritisation Is Key



Nozomi Hour | November
2023 | Inception



Learn more: <https://www.nozominetworks.com/customer-resources>

1. Threat landscape updates
2. Regulation news
3. Technology trends
- 4. Discussion time**





Anton Shipulin, CISSP, CSSA, NNCE
Anton.Shipulin@nozominetworks.com

Thank You!

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.

nozominetworks.com