NOZOMI NETWORKS

Cybersecurity per OT e IoT: Le Sfide del Futuro e le Soluzioni di Oggi

Milano, 13 Febbraio 2025

Nozomi Networks

Building Cyber Resilience in OT/IoT Environments

(Cyber Physical Systems¨CPS¨ Security)

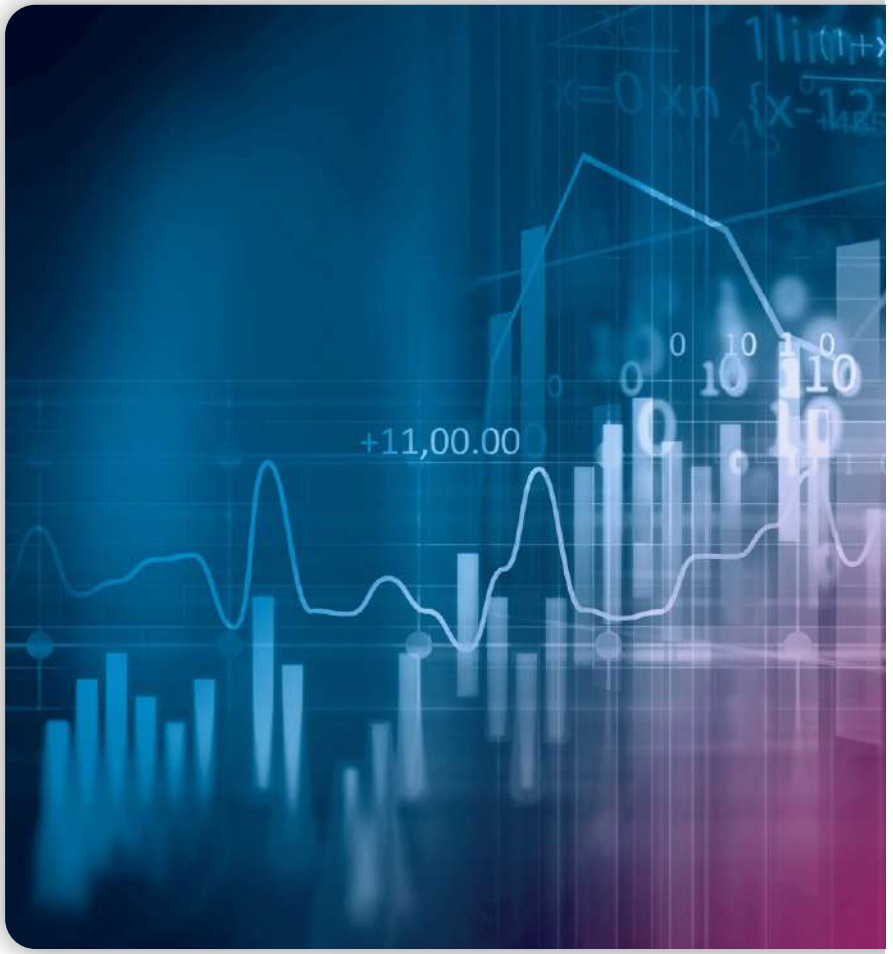
Davide Ricci
Regional Sales Director, Italy
Nozomi Networks

NOZOMI NETWORKS

The digital transformation is now touching industrial and critical infrastructure

Digital transformation has driven great ROI:

- Automation and interoperability of facilities and grids
- Global connectivity, visibility and analytics
- Improved operational efficiency
- Increased production output
- More effective asset utilization



NOZOMI NETWORKS

The digital transformation journey for operational and critical infrastructure

1950s-1970s
MMIs/OIs

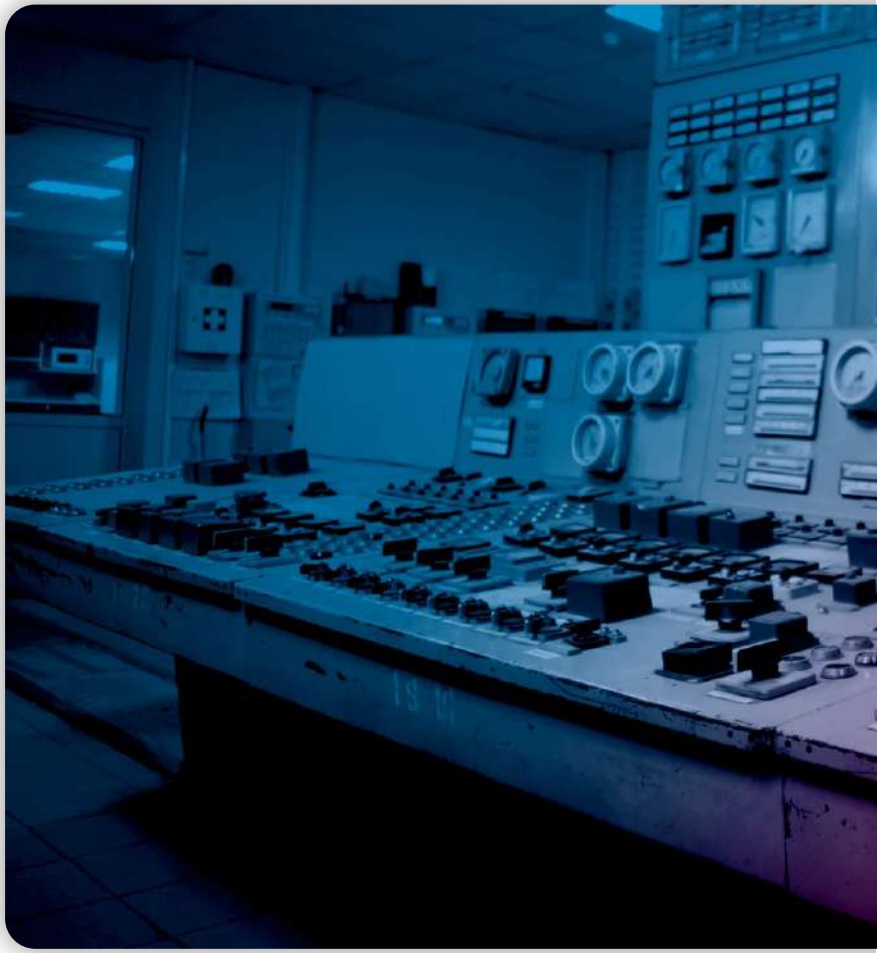
1980s-1990s
HMIs

2000s-2010s
Workstations

2010s-Today
Internet / IoT

Sixty-year-old powerplants, pipelines and production facilities are now connected to the Internet.

What could possibly go wrong?



The risk is real and starting to be addressed

OT/IoT cyber incidents are common

75% of OT asset operators experienced at least one cybersecurity attack in the past 12 months

Operational impacts are real

60% of the OT/ICS incidents resulted in operational disruption

Increased government regulation

Regulations are starting to include punitive remedies, including legal and financial penalties

CISOs now own OT/IoT risk

Now CISOs must ramp understanding of SCADA, DCS, and other OT/IoT systems

Today's OT and CPS Threat Landscape

300+

New vulnerability advisories for OT/IoT products, 2024*

188

Publicly disclosed cyber incidents with physical consequences, 2010 - 2023*

$4,73M

Average cyber attack cost in manufacturing, 2024*

100K+

OT/IoT devices connected directly to the Internet globally, 2024*

280

Publicly disclosed ransomware attacks in manufacturing, H1 2024*

$1M

Average ransom demand, 2024*

OT and CPS Security Requires a Different Strategy

Information Technologies	Operational Technologies
Data confidentiality and integrity is paramount	Human safety is paramount
Mostly Non-real time. High delays and rebooting are generally acceptable.	Real time. High delays and rebooting are unacceptable.
Enough resources for cyber security solutions.	Resources are limited for cyber physical security solutions.
Standard network protocols. Easy to monitor	Industry specific protocols, require knowledge to monitor.
Updates are straightforward and automated	Updates must be planned, and End-of-Support OSs may be in use
Lifetime: 3 to 5 years	Lifetime: 10 to 15 years
Components are local and easy to access	Components may be Isolated, remote, and hard to access

The OT/IoT Cyber Questions Being Asked

What the Board of Directors Ask

- Give me context – how much OT/IoT risk do we have today?
- How do we compare with our peers in our industry? Benchmarks?
- Where we are green, amber or red in our OT/IoT cyber framework? Scorecards?

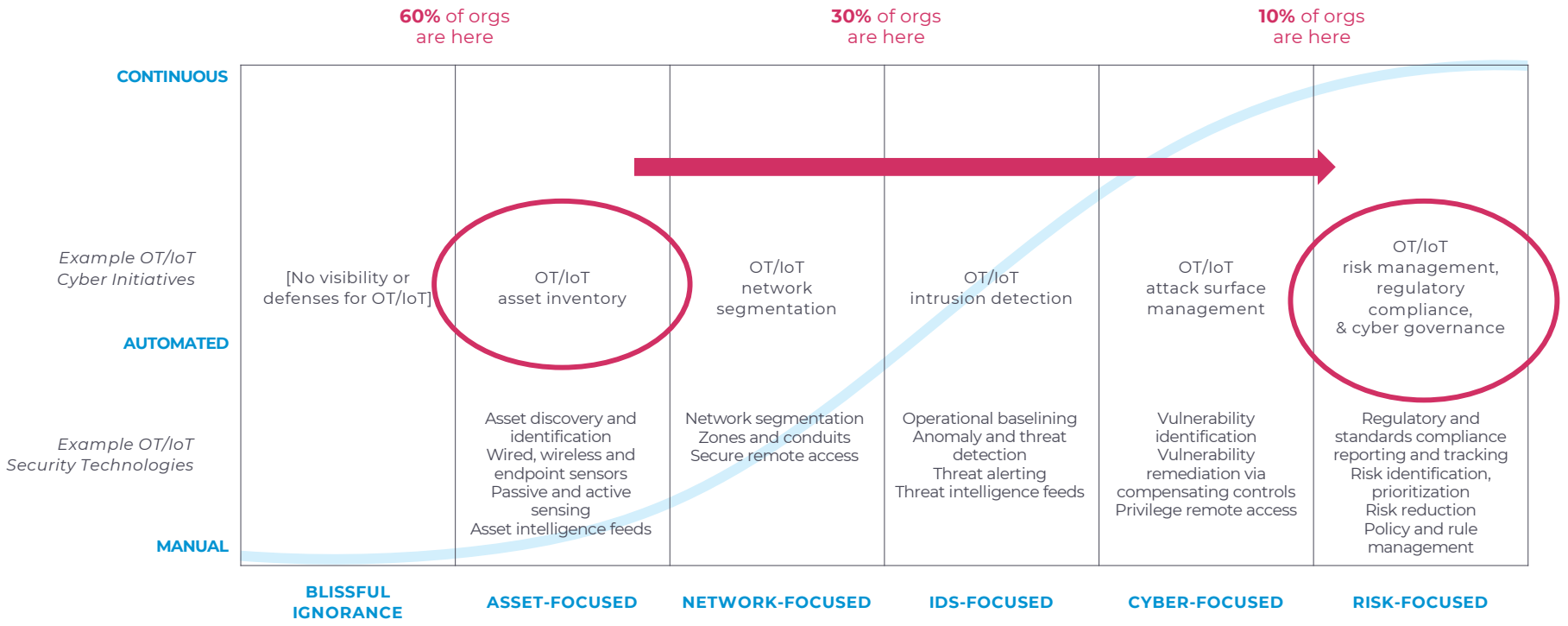
What the CIO Asks

- How do we develop and implement an OT/IoT cyber program to reduce risk? Where to start? Who can help?
- I am not close enough to OT or IoT – how can I be confident in managing this complexity?
- How do I comply with current regulations and reporting?
- Can I leverage the cyber investments I've already made?

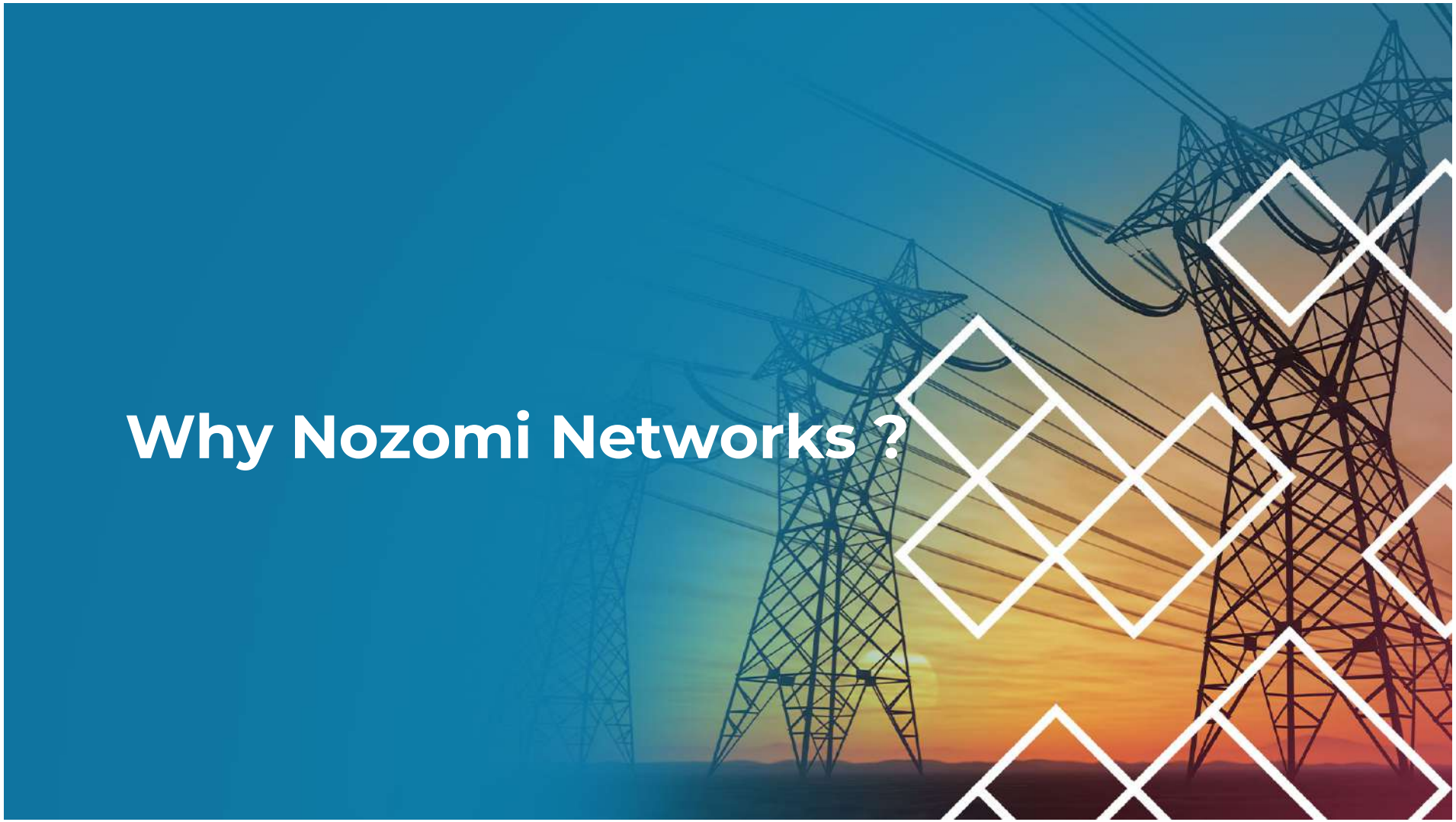
What the Plant Manager / GM of Operations Asks

- How will OT/IoT cybersecurity – both the people and the equipment – impact my operational requirements for productivity, safety and efficiency?
- How do I know your people won't break something critical?
- How can I build and maintain a good relationship with HQ?

Where are most companies in this OT/IoT cyber journey?

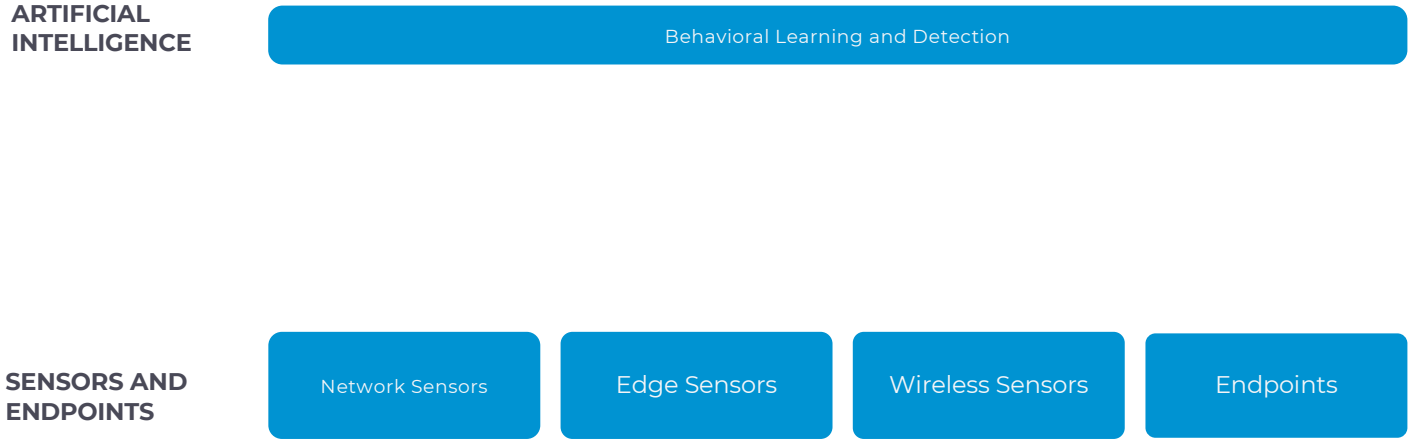


Why Nozomi Networks ?

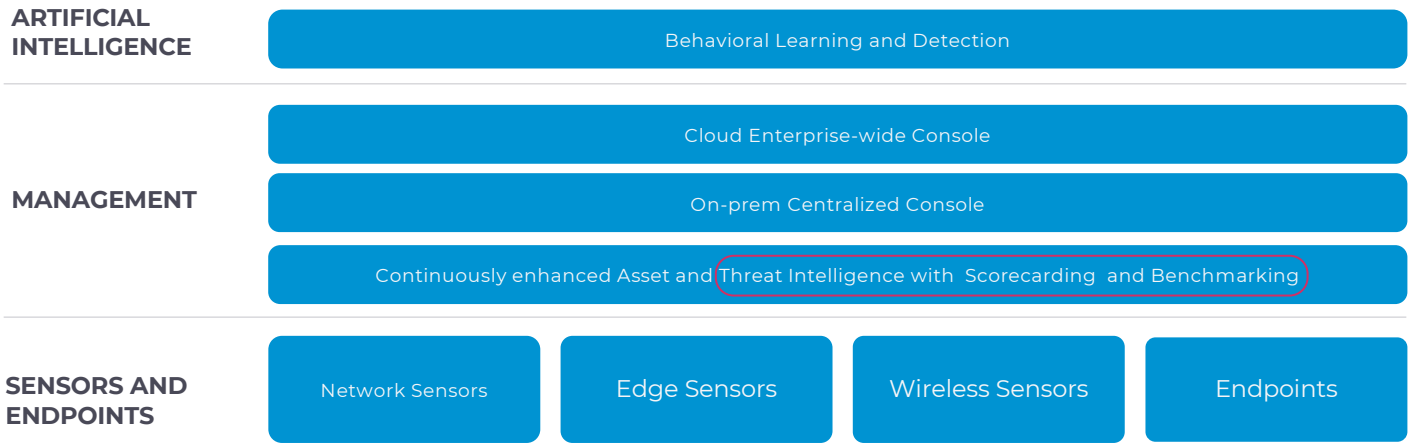


Nozomi Networks delivers unparalleled visibility AND A path to CPS Security Risk Management

Comprehensive sensors + AI delivers actionable, accurate asset details and vulnerabilities

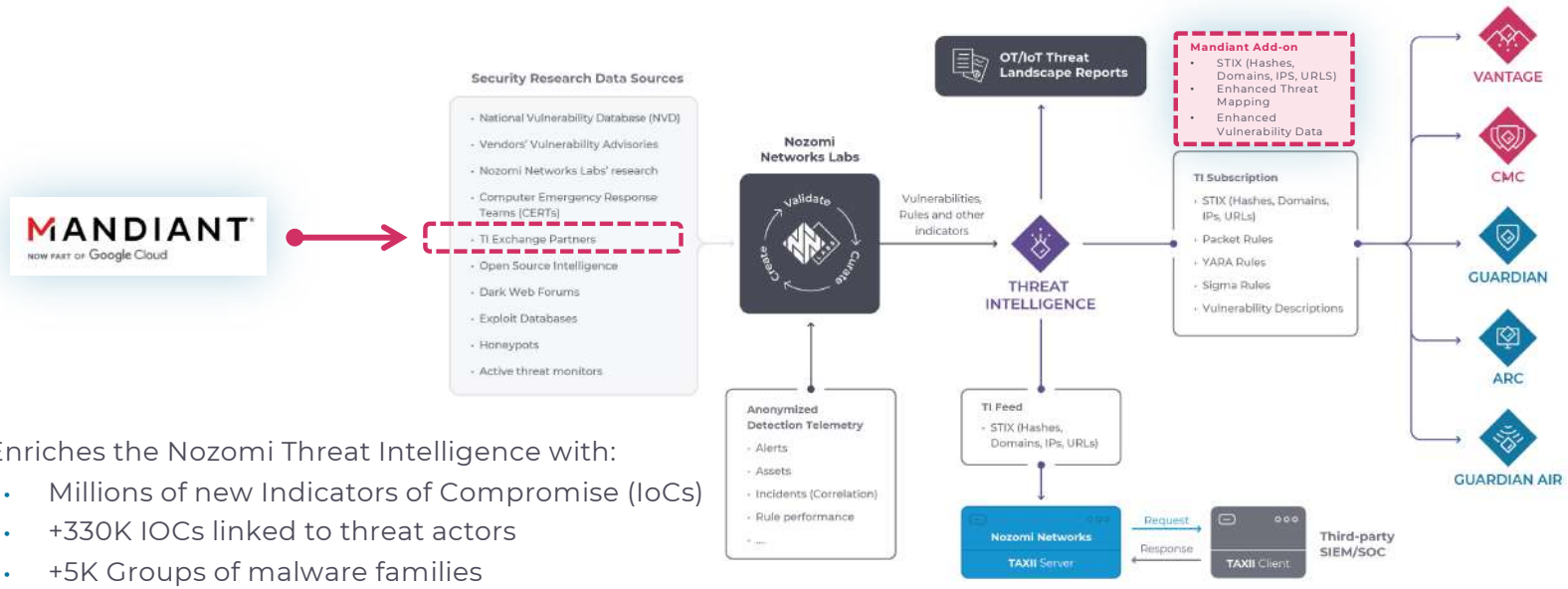


Nozomi Networks pinpoints security threats and process anomalies in near real-time



Extended Threat Intelligence and Detection

Nozomi TI Expansion Pack, Powered by Mandiant - additional IOCs and threat insights

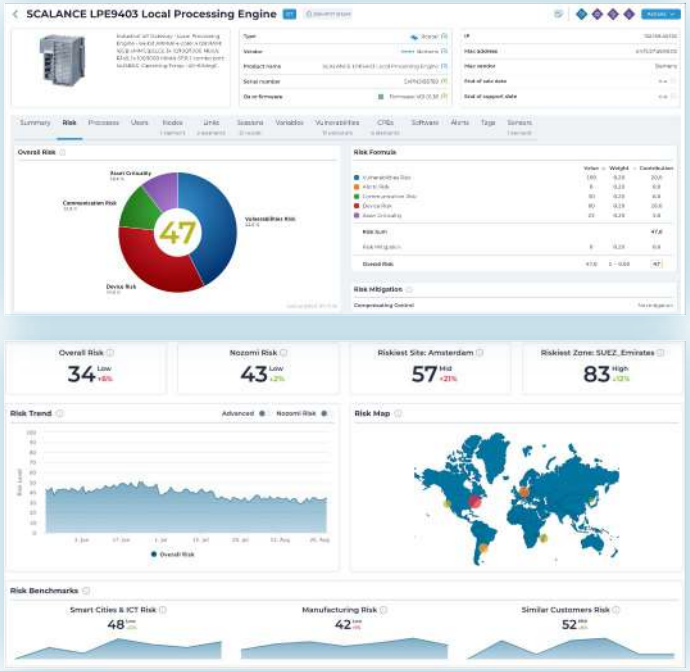


- Enriches the Nozomi Threat Intelligence with:
  - Millions of new Indicators of Compromise (IoCs)
  - +330K IOCs linked to threat actors
  - +5K Groups of malware families
  - +290K IOCs linked to OT industries

Advanced OT/IoT Risk Management

Nozomi Vantage asset risk scoring - dynamic, customizable risk assessment tool

- Risk Score for individual assets, sites, and the entire organization
- Transparent and customizable Asset Risk calculation process, based on the following risk factors:
  - Alert Risk
  - Vulnerability Risk
  - Communication Risk
  - Device Risk
  - Asset Criticality
- Risk Factor customization for specific Asset Criteria with Asset Risk Rules
- Risk Score plotted over time, trends
- Risk Score benchmarks for the industry and similar Customers



We defend the world's largest organizations

9 of Top 20
Oil & Gas

7 of Top 10
Pharma

5 of Top 10
Mining

5 of Top 10
Utilities

- Airports
- Automotive
- Building Automation
- Data Centers
- Federal Government
- Financial Services
- Healthcare
- Manufacturing
- Maritime
- Military
- Mining
- Oil & Gas
- Pharma
- Rail Systems
- Retail
- Smart Cities
- Transportation & Logistics
- Utilities
- Water & Wastewater

We defend at global scale

12K+
Worldwide Installations

115M+
Devices Monitored Across Converged OT/IoT

6 Continents
Scalable Deployments Across 6 Continents

Global Expertise
Worldwide Network of GSIs, OEMs, MSSPs and Reseller Partners and 1,500+ Certified Professionals

NOZOMI NETWORKS

We integrate with your existing IT tech stack

Accelerate deployments; track threats across IT and OT/IoT; leverage your current investments

SIEM, SOAR and Data Integrations

Atos Codex
exabeam
FORTINET
IBM Security
LogRhythm
The Security Intelligence Company
MICRO FOCUS
splunk>
SWIMLANE
Chronicle
part of Google Cloud

OT / ICS Interoperability

ABB
EMERSON
GE Power
Honeywell
MITSUBISHI ELECTRIC
MITSUBISHI HEAVY INDUSTRIES
OMRON
Rockwell Automation
Schneider Electric
YOKOGAWA
SEL
SIEMENS

Other Network / IT and Security Technologies

Allied Telesis
CISCO
cervello
FORTINET
GARLAND TECHNOLOGY
GATEWATCHER
Gigamon
KEYSIGHT TECHNOLOGIES
paloalto NETWORKS
tdi
Tempered
WATERFALL
XONA
ZEDEDA

Cloud Services Platforms

aws
Google Cloud
Microsoft Azure
servicenow

Our solution provides extensive support for OT/IoT and IT protocols and is frequently updated. See the latest **Protocol Support List**.

OT/IoT cybersecurity delivers concrete outcomes

Improved operational resilience and safety

- Enhanced operational visibility into assets and processes
- Real-time anomaly and threat detection
- Accelerated response times
- Improved health, safety and environmental outcomes

Reduced risk

- Minimized attack surfaces
- Revenue protection (and eventually maximization)
- Reduction of reputational and brand risks/impacts

Enhanced regulatory compliance

- Operational compliance (NERC CIP, TSA, NIS2, OTCC, etc.)
- Industry standards support (ISA 62443, NIST CSF 2.0, etc.)
- Successfully passed audits
- Financial disclosure compliance
- Improved governance

Nozomi Networks strengths

Platform scalability

Proven Large Deployments
Deployed with some of the largest customers in the world

Cloud-Based Scale
Option to aggregate and analyze data on-premises through Guardian or with Vantage cloud

Consolidated Management
Management through CMC or from the cloud

Ease of deployment

Sensor Options to Fit Your Environment
Physical, virtual, cloud, edge, endpoint,
container sensors

Cloud Architecture
SaaS platform speeds onboarding, eliminates sizing issues

Industry's Largest Partner Ecosystem and Open API
Minimizes integration complexity

Industry-leading threat detection

Nozomi Network Labs
Premier research organization for new threats and latest cybersecurity research

Latest, Detailed Threat Intelligence
Most completed set of CVEs for cyber-physical systems across industries

Threat Feed for Non-Nozomi Solutions
Vendor agnostic threat feed for third-party security solutions

Actionable intelligence

Power of AI
Only vendor with AI/ML engine for more analysis of data and anomalies

Prioritized Remediation
Workbooks and customized playbooks prioritize and guide remediation efforts

Overcoming the Skills Gap
Intelligent automation to deal with low alerts, data deluge and security issues

Next steps

- What specific outcomes do you need to achieve?
- What does success look like?
- When do you need to achieve them?

- A deep dive into our technology with your technical team to show how we will help you achieve your outcomes

- Voice of customer touchpoints (peer reviews, reference calls, analyst inquiries)
- Optional: a proof of value to demonstrate the outcomes we will achieve together

- Engage our partners and pro services teams for design and scoping of your full implementation and deployment plan

What next step makes the most sense for you and your organization?

THANK YOU