



Securing Tomorrow. Tackling OT/IoT Cyber Risks and AI Challenges

Emanuele Temi - Staff Sales Engineer

The risk is real and starting to be addressed



OT/IoT cyber incidents are common

85% of OT asset operators reported at least one adverse cyber incident in the past 12 months that significantly impacted operations



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

Cyber incidents are impacting OT/IoT operations

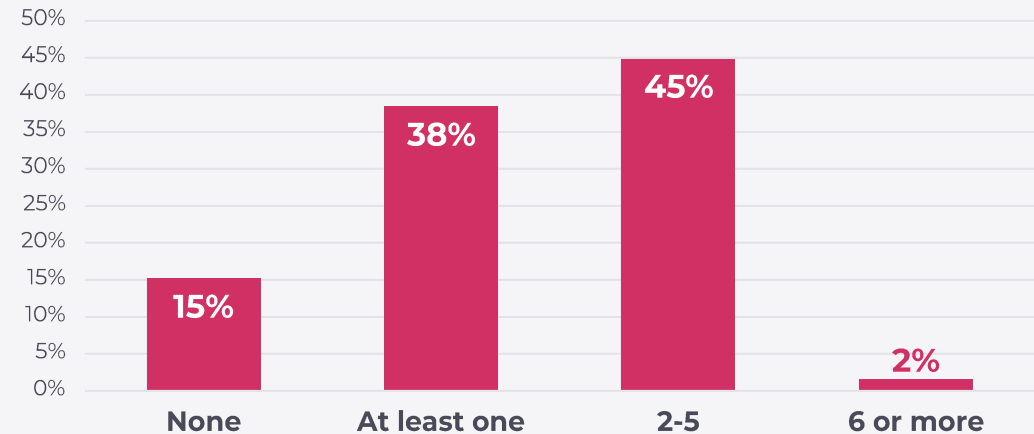
Global Survey Results

Survey of 310 cybersecurity leaders

85%

cybersecurity leaders from five major countries report at least one cyber incident that impacted their OT environment this year

Have you experienced an adverse cyber incident in your OT environment this year that significantly impacted operations? (n=310)



Source: ABI Research, commissioned global study to be published in early 2025.

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?

Innovative Uses of AI/LLMs in Malware

Adversaries are moving to embedding LLMs directly into malware logic



PromptLock

AI-Powered Ransomware

- Research/prototype project
- Uses a **locally hosted LLM**
- Generates scripts for filesystem reconnaissance, data exfiltration, file encryption, potential data destruction.

Source: <https://www.welivesecurity.com/en/ransomware/first-known-ai-powered-ransomware-uncovered-eset-research/>



LameHug

AI-Powered Malware

- Real-world attack
- Uses **external LLM API**
- Generate commands for system info collection, recursive search of user directories, data exfiltration via HTTP POST / SFTP.

Source: <https://cert.gov.ua/article/6284730>

Behavior adapts to the environment, making detection harder.

OT/IoT Security Can't Ignore AI-based Attacks

Large language models (LLMs) enabled attack techniques currently seen in the wild:

- Reconnaissance
- Scripting techniques
- Malware development
- Social engineering
- Vulnerability research
- Payload crafting
- Anomaly detection evasion
- Security feature bypass
- Backdoor deployment
- Automated collection
- Data manipulation
- Deepfake for Impersonation



Source: github.com/cybershujin/Threat-Actors-use-of-Artificial-Intelligence

Nozomi Vantage IQ



Nozomi **Vantage IQ** is an AI engine that automates tedious tasks of reviewing, correlating and prioritizing tasks to provide meaningful infrastructure insights, effectively extending the impact of the cybersecurity team.

Vantage IQ insights are adaptable and available across the vantage GUI and can also provide complex answers in human language, as well as recommendations on threat remediation.

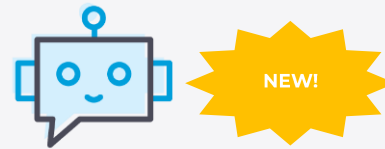
What is it? An add-on to Vantage that uses AI to replicate learned experiences of seasoned security analysts over extremely large cloud-scaled networks at a fraction of the time and cost.



Real-time, adaptable insights to increase focus, reduce administrative overhead and close security gaps



Prioritized actions to help prioritize remediation efforts



Human language to deliver better results easier and faster



Recommendations to help streamline forensics, tuning and security enhancements

Features

IQ Assistant

- Meaningful and accurate answers to complex questions made in human language using Nozomi's own LLM.
- We go way beyond query creation and deliver context-aware, intelligent results.

Good day Gabe, what can I assist with?

Ask anything
Is my system compliant with the NIS2 directive?

AI responses may contain errors. Data is processed externally outside Vantage infrastructure. Always verify important information.

Compliance Score: Partial Compliance (60-70%)

To achieve full NIS2 compliance, you'll need to address the open vulnerabilities, enhance your incident response capabilities, and implement more robust risk management processes.

Would you like me to help you develop a detailed roadmap for improving your NIS2 compliance?

A large red arrow points from the compliance score text to the left, towards the list of features.

It takes Vantage IQ less than a minute to deliver these results!

Features

Prioritized actions

- Enhances problem identification and supports corrective measures by enhancing operational effectiveness and redirecting the attention to the most important tasks.

The screenshot shows the Nozomi Vantage IQ interface. The navigation bar includes icons for Sensors, Alerts, Assets, Wireless, Queries, Vulnerabilities, and IQ. The main content area displays a list of items with filters for Scope, Category, and Severity. A yellow box labeled "Severity" points to the "High severity" tag of the first item, and another yellow box labeled "Type" points to the "Security enhancement" tag of the fourth item. A large grey box at the bottom of the list is labeled "Prioritized, actionable items".

Severity

Type

Prioritized, actionable items

Stories from the field

How a synthetic assistant enhances data analysis

Unexpected communication towards China

Deep Dive: Communications to China

Based on my comprehensive analysis, here's what I found regarding communications to China (CN):

Hosts Involved

You have **3 hosts** communicating to China across **5 separate connections**:

- Host [REDACTED]**
 - **Device Type** [REDACTED]
 - **Zone:** Undefined
 - **Communications to China:**
 - **14.17.91.17** (Alibaba Cloud / Aliyun - Shanghai)
 - HTTP [REDACTED]
 - HTTPS [REDACTED]
 - **Total:** [REDACTED] bytes
- Host [REDACTED] - CRITICAL**
 - **Device** [REDACTED] (Xiaomi Mobile Phone)
 - **Type:** Mobile phone (personal device)
 - **OS:** Android
 - **Risk Score:** 12.0
 - **Zone** [REDACTED]
 - **Captured by** [REDACTED] (wireless sensor)
 - **Communications to China:**
 - **103.235.46.115** (China IP)
 - HTTPS [REDACTED]
 - **Total** [REDACTED] bytes

- Host [REDACTED] - CRITICAL**
 - **Device** [REDACTED] (Windows Server)
 - **Type:** Computer (Virtual Machine)
 - **OS** [REDACTED] ⚠️ **CRITICAL: End-of-Support OS**
 - **Vendor:** Microsoft
 - **Risk Score:** 8.0
 - **Zone:** Supervisor (Management Network)
 - **MAC Address** [REDACTED] (Microsoft Hyper-V)
 - **Last Activity** [REDACTED] (seconds ago - **ACTIVE**)
 - **Protocols** [REDACTED]
 - **Remediations Needed** [REDACTED]
 - **Communications to China:**
 - **1.3.1.15** (China IP - Likely command & control)
 - NetBIOS-SSN [REDACTED]
 - TCP/445 [REDACTED]
 - **Total** [REDACTED] bytes

NIS2 Compliance – Where Do We Stand?

1 GOVERNANCE & POLITICHE (NIS2 Art. 20-21)

Gap Identificati:

Gap	Severità	Dettagli	Impatto NIS2
Asset inventory incomplete	Critica	15 asset (9% senza vendor/product info)	Manca inventario completo richiesto
Missing lifecycle tracking	Critica	8 asset end-of-life/support attivi	Violazione requirement 16 (patch management)
Risk assessment non formalizzato	Alta	Risk score non allineato a metodologia standard	Manca risk assessment strutturato
Configurazione asset incomplete	Alta	6 asset con MAC address unconfirmed	Asset posture management assente

Raccomandazioni:

- ✔ **Completare l'inventario:** Eseguire discovery completo per i 15 asset senza informazioni (vendor/product)
- ✔ **Ritirare asset EOL/EOS:** Sostituire gli 8 dispositivi Siemens S7-300 con versioni supportate
- ✔ **Implementare Asset Management Policy** conforme NIS2: classificazione per criticità, lifecycle tracking, change management

2 SECURITY TECNICA & CONTROLLI (NIS2 Art. 22)

2.1 Gestione delle Vulnerabilità

Gap Identificati:

Aspetto	Stato Attuale	Gap vs NIS2	Priorità
Vulnerabilità critica	0 CVE EPSS > 0.5 rilevati	✔ Conforme	Bassa
End-of-support firmware	8 dispositivi S7-300	❌ Non conforme	Critica
Patch management	3 remediazioni firmware disponibili	⚡ Parziale	Alta
Supply chain vulnerabilities	Non monitorata	❌ Assente	Alta

Remediazioni Critiche Urgenti:

- Windows OS Updates** (Risk Reduction: 160 punti / 4.2%)
 - Upgrade Windows 7 → Windows 11 per 10 asset
 - Stato: **URGENTE** - Windows 7 non è supportato
- Software Updates** (Risk Reduction: 194 punti / 5.09%)
 - Upgrade Internet Explorer → Edge per 5 asset
 - Stato: **URGENTE** - IE è deprecated
- Firmware Updates Siemens** (Risk Reduction: 41 punti / 1.08%)
 - Update S7-300 firmware v3.3.10 → v3.x.18 per 3 device
 - Update S7-315-2 firmware v1.2.1 → v3.3.17 per 2 device
 - Stato: **ALTA** - Disponibili patch critiche

2.2 Comunicazioni Insecure

Protocol Analysis:

RISKY PROTOCOLS RILEVATI:

- VNC (3 occorrenze) - Inencrypted remote access
- Telnet (1 occorrenza) - Unencrypted credentials
- SSH (1 occorrenza) - Without signing
- FTP (1 occorrenza) - Unencrypted auth

HTTPS: 0 sole occorrenze - Coverage insufficiente

Raccomandazioni:

- ✔ Disabilitare Telnet e VNC, migrare a SSH/SCP con TLS
- ✔ Forzare HTTPS su tutti gli asset web-enabled
- ✔ Implementare segmentazione network per Storm e Proton DCP

2.3 Comunicazioni Esterne Rischiose

Comunicazioni OT verso Internet: ⚠️ **CITRICA**

82 connessioni a IT
73 connessioni a US
55 connessioni a DE

204 connessioni a IT
13 connessioni unknown

Cap NIS2: Mancava esplicita filtering policy per OT networks

3 GESTIONE DEGLI INCIDENTI & THREAT INTELLIGENCE (NIS2 Art. 23)

Gap Identificati:

Aspetto	Stato	Gap
Alert tuning	Non conforme	❌ No threshold management
Incident response plan	Non rilevato	❌ Assente
MITRE ATT&CK mapping	Supportato da VeriTag	✔ Disponibile
Threat intelligence feed	Attivo	✔ Conforme

Raccomandazioni:

- ✔ Configurare incident response playbook per OT threats
- ✔ Sincronizzare con CSIRT nazionale (CIS)

4 CONTINUITÀ OPERATIVA & DISASTER RECOVERY (NIS2 Art. 24)

Gap Identificati:

Aspetto	Valutazione	Cap NIS2
Sensor redundancy	3 sensori attivi	⚡ Parziale - No active/active
Backup completeness	Non verificato	❌ Assente
Geographic distribution	Ucrain location	⚠️ Single point of failure
RTO/RPO definiti	Non rilevati	❌ Assente

PIANO DI AZIONE PRIORITIZZATO (NIS2 Compliance Timeline)

IMMEDIATO (0-30 giorni)

1. Vulnerability Patching

- ☐ Update Windows 7 → Windows 11 (10 asset)
- ☐ Update IE → Edge (5 asset)
- Impact: 324 risk points (4.2%)

2. Eliminate EOL Devices

- ☐ Retirement plan per 8 Siemens S7-300
- ☐ Purchase S7-300/500 replacement
- Timeline: 60-90 giorni

3. Protocol Hardening

- ☐ Disable Telnet + VNC
- ☐ Force HTTPS on web interfaces
- ☐ Implement SSH/SCP encryption

BREVE TERMINE (30-90 giorni)

4. Asset Inventory Completion

- ☐ Discovery del 15 asset senza vendor info
- ☐ Update CMDB

5. Network Segmentation

- ☐ Isolate OT from public internet
- ☐ Implement DMZ for admin access

6. Sensor Optimization

- ☐ Reception Guards (DMZ port)
- ☐ Target 98%+ MAC authorization rate

MEDIO TERMINE (90-180 giorni)

7. Incident Response Program

- ☐ Develop OT specific IR playbook
- ☐ Align with NIS2 D Lgs. 104/2022

8. Supply Chain Security

- ☐ Vendor security assessment
- ☐ Firmware integrity verification process

9. Continuity Planning

- ☐ Define RTO/RPO per critical asset
- ☐ Develop strategy for OT configurations

SINTESI CONFORMITÀ NIS2

PIANO	Stato	Gap	Timeline Fix
Governance	⚡ 40% Policy incomplete		30gg
Security	❌ 45% Vulner critical + proto miscon		30gg
Risk Mgmt	⚡ 50% No formal assessment		30gg
Incident Response	❌ 20% IR plan missing		30gg
Continuity	⚡ 40% No RTO/RPO		30gg
Compliance Overall	❌ 43% Requires immediate action		30gg

Attack simulation

Sticking all together

Complete Attack Flow Diagram



Attack Success Factors

Factor	Status	Risk Level
Entry Point Vulnerabilities (CVE [redacted] EPSS 0.878)	[redacted]	Critical
Weak Authentication	Weak passwords detected	Critical
Network Segmentation	None between zones	Critical
Unencrypted Protocols	[redacted] enabled	High
Firewall Rules	No inter-zone restrictions	Critical
Endpoint Detection	Not evident	High

Mitigation Recommendations

Immediate (Next 24 Hours)

1. Isolate [redacted] SRV [redacted]
 - o Disconnect from network or segment with firewall rules
 - o Block all outbound connections to Internet
 - o Block HTTP traffic between zones
2. Patch Critical Vulnerabilities
 - o Apply Windows KB5068787 (latest cumulative update)
 - o Specifically patches CVE [redacted] and CVE [redacted]
3. Disable Weak Protocols
 - o Disable HTTP (enforce HTTPS only)
 - o Disable LLMNR
 - o Disable unnecessary SMB shares

Short-term (This Week)

4. Implement Network Segmentation
 - o Create strict firewall rules between [redacted]
 - o Only allow required OPC-UA traffic to controller
 - o Block HTTP/HTTPS to Zone1
5. Change Credentials
 - o Force password reset on all affected systems
 - o Implement strong password policy
 - o Deploy Multi-Factor Authentication (MFA)
6. Controller Hardening
 - o Apply WAGO firmware updates
 - o Implement OPC-UA authentication
 - o Enable controller-level audit logging



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.