Nozomi Hour

The latest OT/IoT cybersecurity industry updates and insights

Q1 2026

Anton Shipulin, CISSP, CSSA, NNCE

Industrial Cybersecurity Evangelist, Nozomi Networks

Anton.Shipulin@nozominetworks.com

Agenda

Q1 2026

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. Q&A

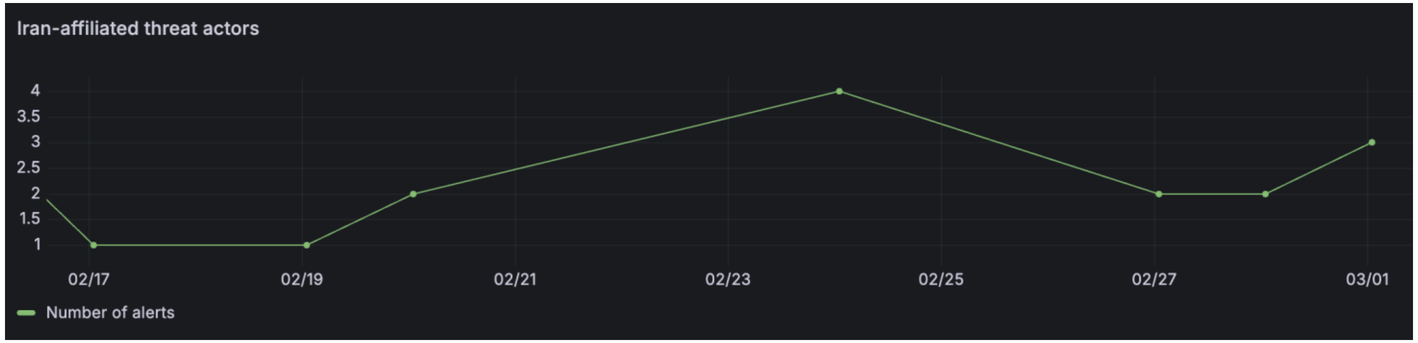
The Cyber Battlefield of the Middle East Conflict

Cyber Operations Expanding Alongside Regional Conflict

- Researchers report a surge in Iran-linked cyber espionage and disruptive operations amid escalating Middle East tensions, targeting government entities, industrial organizations, and critical infrastructure.
- Recent incidents demonstrate real operational impact: an Iran-linked attack on medical technology company Stryker disrupted order processing, manufacturing, and shipping operations.
- Threat actors are expanding reconnaissance and access methods (e.g., exploiting internet-exposed systems and IoT devices), increasing the risk of disruption and collateral impact on industrial and supply-chain organizations.

Nozomi’s View on Cyber Risk in the Middle East

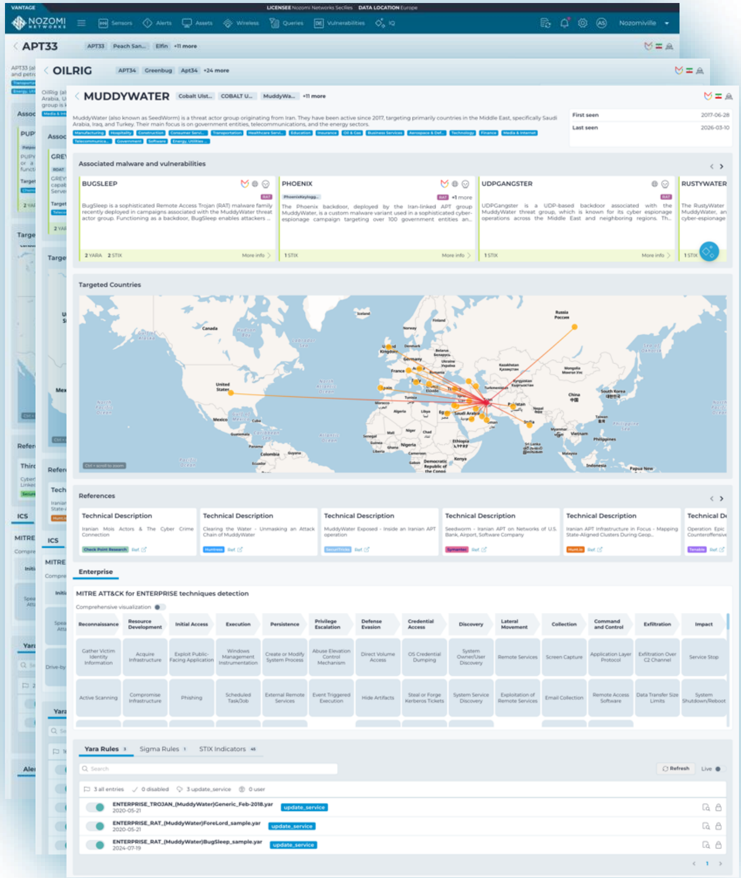
A systematic increase in alerts associated with Iran-affiliated threat actors



Top MITRE ATT&CK techniques observed in the Middle East in the past weeks

Technique ID	Technique Name	Tactics	Percentage
T0812	Default Credentials	Lateral Movement	47.9%
T0859	Valid Accounts	Persistence; Lateral Movement	47.9%
T0846	Remote System Discovery	Discovery	1.4%
T0841	Network Service Scanning	Discovery	1.4%
T1110	Brute Force	Credential Access	0.2%

Nozomi Threat Intelligence Cards



MuddyWater (also known as SeedWorm) is a threat actor group originating from Iran. They have been active since 2017, targeting primarily countries in the Middle East, specifically Saudi Arabia, Iraq, and Turkey. Their main focus is on government entities, telecommunications, and the energy sectors.

First seen	2017-06-28
Last seen	2026-03-10

Associated malware and vulnerabilities

BUGSLEEP — RAT — BugSleep is a sophisticated Remote Access Trojan (RAT) malware family recently deployed in campaigns associated with the MuddyWater threat actor group. Functioning as a backdoor, BugSleep enables attackers ... — 2 YARA 2 STIX — More info

PHOENIX — PhoenixKeylogg... — RAT +1 more — The Phoenix backdoor, deployed by the Iran-linked APT group MuddyWater, is a custom malware variant used in a sophisticated cyber-espionage campaign targeting over 100 government entities an... — 1 STIX — More info

UDPGANGSTER — RAT — UDPGangster is a UDP-based backdoor associated with the MuddyWater threat group, which is known for its cyber espionage operations across the Middle East and neighboring regions. Th... — 1 STIX — More info

RUSTYWATER — The RustyWater MuddyWater, an cyber-espionage — 1 STIX

References

- Technical Description — Iranian Mois Actors & The Cyber Crime Connection — Check Point Research — Ref
- Technical Description — Clearing the Water - Unmasking an Attack Chain of MuddyWater — Huntress — Ref
- Technical Description — MuddyWater Exposed - Inside an Iranian APT operation — SecurITricks — Ref
- Technical Description — Seedworm - Iranian APT on Networks of U.S. Bank, Airport, Software Company — Symantec — Ref
- Technical Description — Iranian APT Infrastructure in Focus - Mapping State-Aligned Clusters During Geop... — Hunt.io — Ref
- Technical De — Operation Epic Counteroffensive — Tenable — Ref

Enterprise

MITRE ATT&CK for ENTERPRISE techniques detection

Comprehensive visualization

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Exploit Public-Facing Application	Windows Management Instrumentation	Create or Modify System Process	Abuse Elevation Control Mechanism	Direct Volume Access	OS Credential Dumping	System Owner/User Discovery	Remote Services	Screen Capture	Application Layer Protocol	Exfiltration Over C2 Channel	Service Stop
Active Scanning	Compromise Infrastructure	Phishing	Scheduled Task/Job	External Remote Services	Event Triggered Execution	Hide Artifacts	Steal or Forge Kerberos Tickets	System Service Discovery	Exploitation of Remote Services	Email Collection	Remote Access Software	Data Transfer Size Limits	System Shutdown/Reboot

Yara Rules 3 | Sigma Rules 1 | STIX Indicators 45

Search — Refresh — Live

3 all entries ✓ 0 disabled 3 update_service 0 user

ENTERPRISE_TROJAN_(MuddyWater)Generic_Feb-2018.yar 2020-05-21	update_service
ENTERPRISE_RAT_(MuddyWater)ForeLord_sample.yar 2020-05-21	update_service
ENTERPRISE_RAT_(MuddyWater)BugSleep_sample.yar 2024-07-19	update_service

Learn more:
https://www.nozominetworks.com/blog/iranian-apt-activity-during-geopolitical-escalation-recommendations-for-nozomi-customers-and-critical-infrastructure-owners

Security Cameras as Cyber Intelligence Platforms in Modern Kinetic Conflict

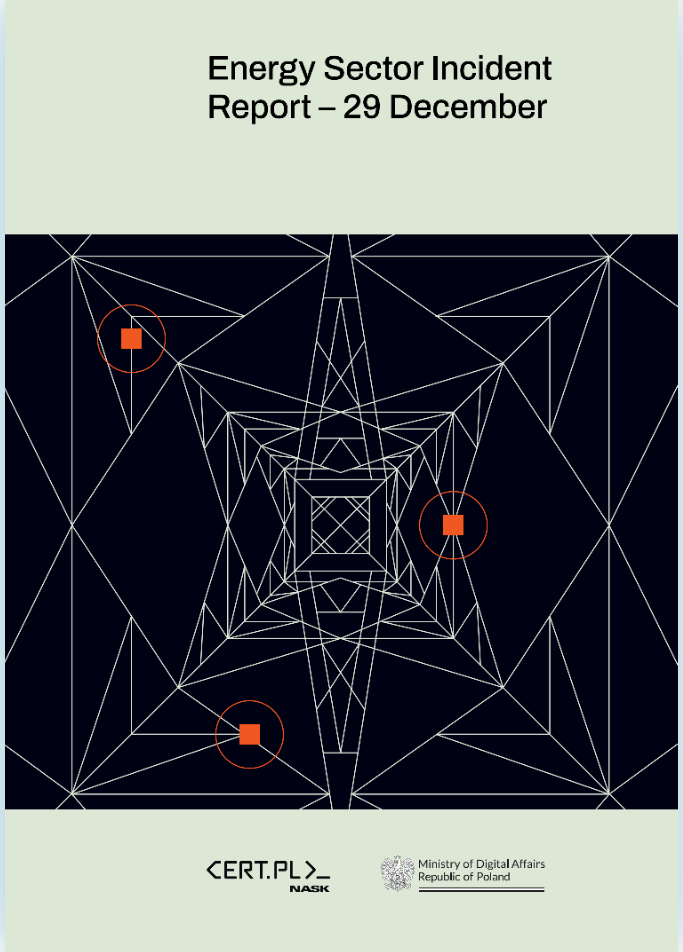
- Reports indicate **Israel compromised Tehran's (Iran) traffic camera network**, enabling access to numerous CCTV feeds and persistent monitoring of urban movement patterns and pattern-of-life intelligence **prior to airstrikes.**

- Separate reporting indicates earlier **Iran has also leveraged compromised surveillance cameras in Israel** to enhance situational awareness and refine missile targeting, demonstrating how state actors use IoT infrastructure to support cyber-enabled kinetic operations.

Cyberattack on Critical Infrastructure in Poland

- On 29 December 2025, a coordinated cyber-sabotage campaign targeted Poland's energy and industrial sectors, affecting at least **30 wind and solar farms, a large CHP plant serving ~500,000 customers, and a manufacturing company.**
- The attacker gained access through **exposed FortiGate VPN devices without MFA**, then conducted months of reconnaissance and credential theft before launching destructive actions.
- The operation deployed wiper malware (DynoWiper and LazyWiper) and targeted both OT and IT systems, **including Hitachi and Mikronika RTUs, Mikronika HMIs, Hitachi protection relays, and Moxa serial device servers.**
- The attack **disrupted remote communication with multiple renewable energy sites and attempted data destruction on over 100 machines, but power generation and grid stability were not impacted**, with some actions blocked by EDR controls.

Learn more: https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025



Energy Sector Incident
Report – 29 December

CERT.PL>_
NASK

Ministry of Digital Affairs
Republic of Poland

Top MITRE ATT&CK Techniques

Nozomi Networks OT/IoT Cybersecurity Report, Second Half of 2025

Top 10 Most Common MITRE ATT&CK Techniques Associated with Raised Alerts

June to December 2025

ID	Technique name	Tactics	%	% 1H 2025
T1557	Adversary-in-the-Middle	Credential Access; Collection	**26.5%**	**16.00%**
T1110	Brute Force	Credential Access	**10.2%**	**7.36%**
T1498	Network Denial of Service	Impact	**9.54%**	**17.60%**
T0814	Denial of Service	Inhibit Response Function	**9.39%**	**17.40%**
T1565	Data Manipulation	Impact	**8.36%**	**4.11%**
T0846	Remote System Discovery	Discovery	**7.13%**	**11.40%**
T0841	Network Service Scanning	Discovery	**7.13%**	**11.40%**
T0812	Default Credentials	Lateral Movement	**5.81%**	**5.27%**
T0859	Valid Accounts	Persistence; Lateral Movement	**5.81%**	**5.27%**
T1071	Application Layer Protocol	Command And Control	**3.62%**	**1.33%**

Learn more: https://www.nozominetworks.com/ot-iot-cybersecurity-trends-insights-february-2026

Top MITRE ATT&CK Techniques

Nozomi Networks OT/IoT Cybersecurity Report, Second Half of 2025

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact	Inhibit Response Function	Impair Process Control	Impact - ICS
Valid Accounts		Valid Accounts	Valid Accounts	Valid Accounts	Brute Force	Network Service Scanning	Default Credentials	Man-in-the-Middle	Application Layer Protocol		Data Manipulation	Denial of Service		
					Man-in-the-Middle	Remote System Discovery	Valid Accounts				Network Denial of Service			

*Customized Threat Collection (Enterprise & ICS) from the “Defending Operational Technology (OT) with ATT&CK” project by MITRE Center for Threat-Informed Defense

Top Malware Observed in the Wild

Top 5 Malware Categories

Malware category	%
TROJAN	**74.60%**
RAT	**11.30%**
MINER	**4.61%**
WORM	**3.70%**
DOWNLOADER	**1.89%**

Top 5 Malware Families

Malware category	%
Generic	**54.70%**
DoublePulsar	**20.50%**
ANDROMEDA	**6.02%**
CobaltStrike	**3.62%**
AsyncRAT	**2.45%**

Top 5 Threat Actors

Threat actor	Main country of origin	% Associated actor-linked alerts
Scattered Spider	US and UK	**42.90%**
Kimsuky	North Korea	**8.45%**
APT29	Russia	**5.42%**
UNC1549	Iran	**5.38%**
Mustard Tempest	No strong attribution	**3.45%**

Suspicious activity	%
USB file transfer	**81.9%**
Malicious USB device	**10.5%**
New USB device plugged	**7.58%**
Malicious Human Interface Device	**0.0325%**

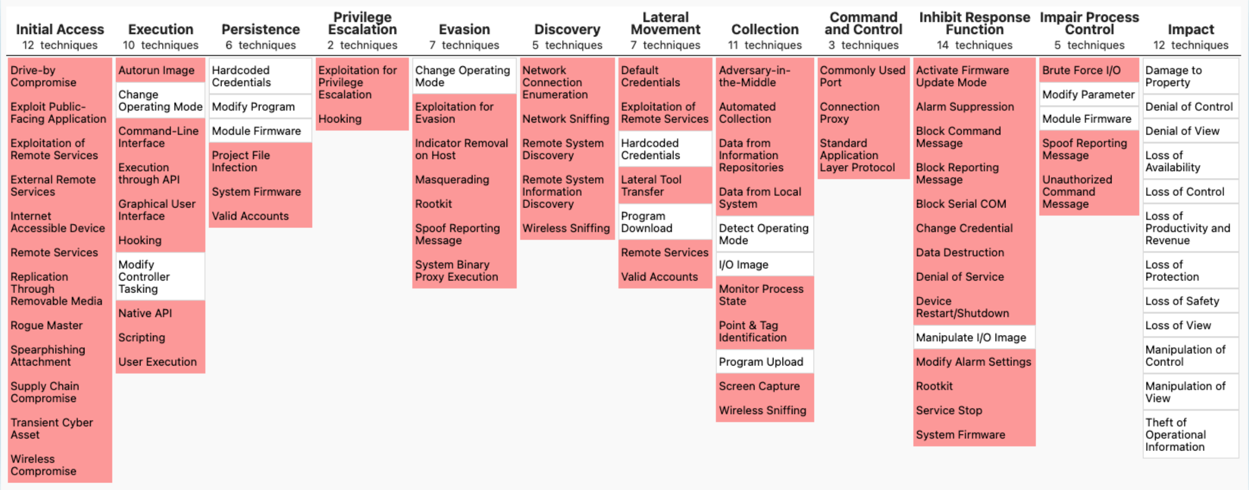
Learn more: https://www.nozominetworks.com/ot-iot-cybersecurity-trends-insights-february-2026

Most Attack Techniques Target OT Endpoints

72%

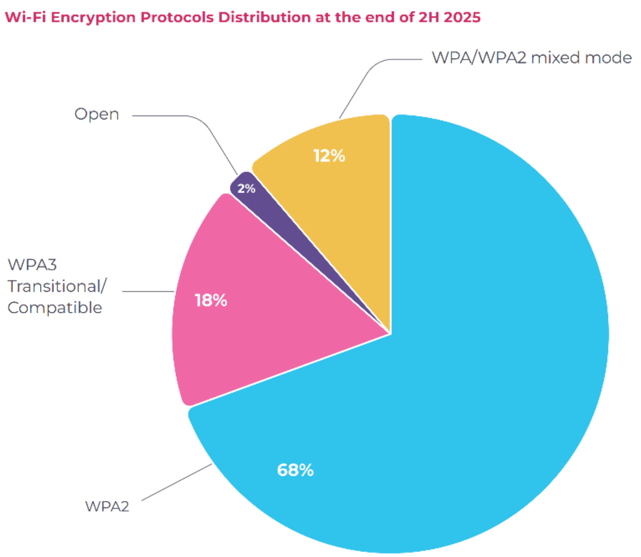
of MITRE ATT&CK for ICS attack techniques on different attack stages, based on real-world observations are focused on such OT endpoint devices as:

- Human-Machine Interfaces (HMI)
- Engineering Workstations
- Application Servers
- Control Servers
- Data Gateways
- Data Historians
- Jump Hosts

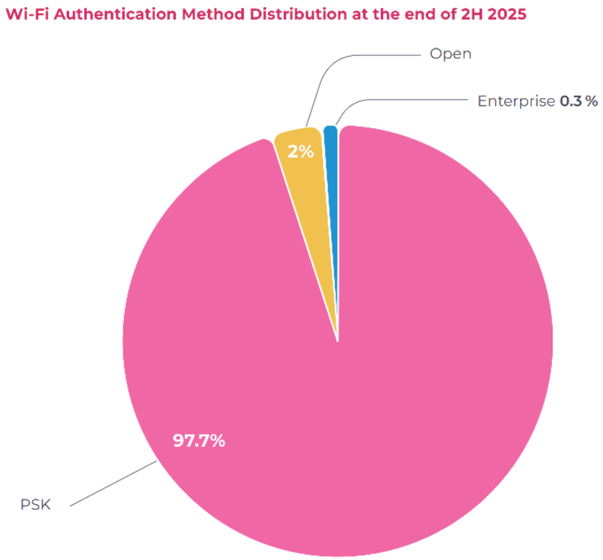


Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

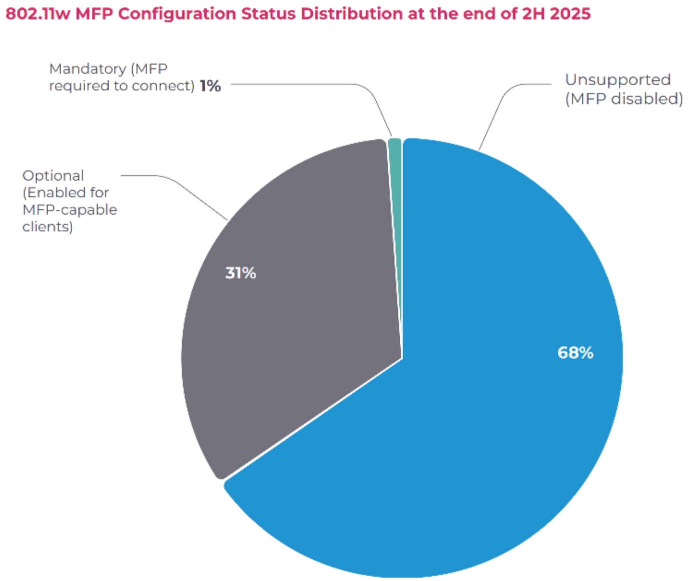
Wireless Exposure in Industrial Environments



14% of observed networks use open or legacy security modes



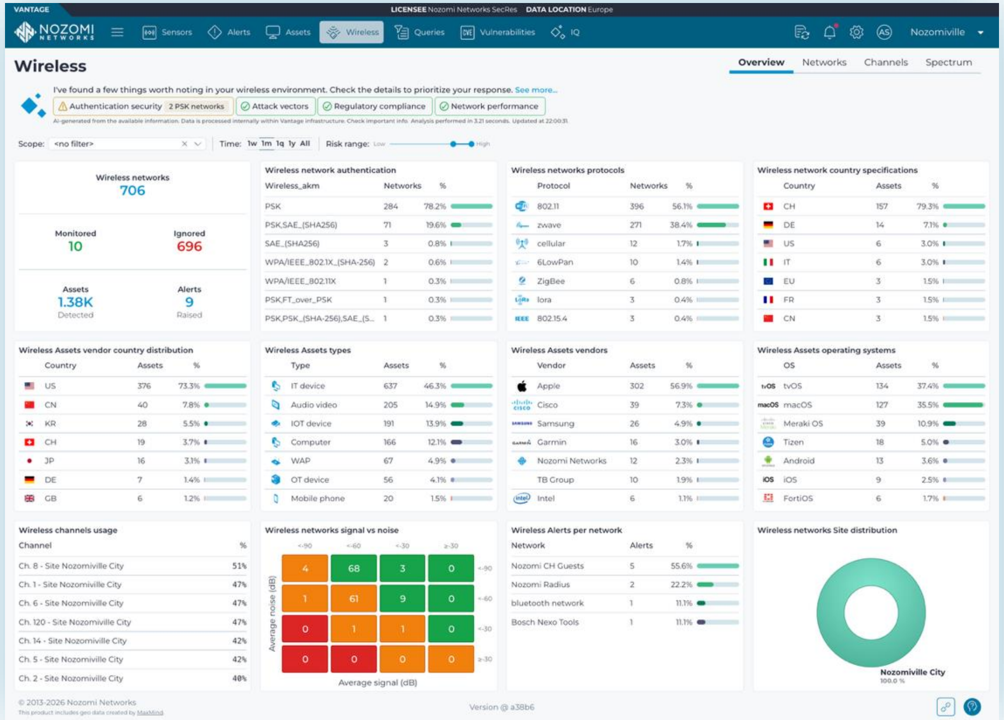
Enterprise-grade authentication such as 802.1X is observed in only 0.3% of detected Wi-Fi networks



68% of observed wireless networks still operate without Management Frame Protection (MFP), which provides protection against deauth attacks

Learn more: https://www.nozominetworks.com/ot-iot-cybersecurity-trends-insights-february-2026

OT Wireless Assesment with Nozomi Guardian Air



LICENSEE Nozomi Networks SecRes DATA LOCATION Europe

Wireless

I've found a few things worth noting in your wireless environment. Check the details to prioritize your response. See more...

⚠ Authentication security 2 PSK networks | ✓ Attack vectors | ✓ Regulatory compliance | ✓ Network performance

AI-generated from the available information. Data is processed internally within Vantage infrastructure. Check important info. Analysis performed in 3.21 seconds. Updated at 22:00:31

Scope: <no filter> Time: 1w 1m 1q 1y All Risk range:

Wireless networks 706

Monitored 10 | Ignored 696

Assets 1.38K Detected | Alerts 9 Raised

Wireless network authentication

Wireless_akm	Networks	%
PSK	284	78.2%
PSK,SAE_(SHA256)	71	19.6%
SAE_(SHA256)	3	0.8%
WPA/IEEE_802.1X_(SHA-256)	2	0.6%
WPA/IEEE_802.11X	1	0.3%
PSK,FT_over_PSK	1	0.3%
PSK,PSK_(SHA-256),SAE_(S...	1	0.3%

Wireless networks protocols

Protocol	Networks	%
802.11	396	56.1%
zwave	271	38.4%
cellular	12	1.7%
6LowPan	10	1.4%
ZigBee	6	0.8%
lora	3	0.4%
802.15.4	3	0.4%

Wireless network country specifications

Country	Assets	%
CH	157	79.3%
DE	14	7.1%
US	6	3.0%
IT	6	3.0%
EU	3	1.5%
FR	3	1.5%
CN	3	1.5%

Wireless Assets vendor country distribution

Country	Assets	%
US	376	73.3%
CN	40	7.8%
KR	28	5.5%
CH	19	3.7%
JP	16	3.1%
DE	7	1.4%
GB	6	1.2%

Wireless Assets types

Type	Assets	%
IT device	637	46.3%
Audio video	205	14.9%
IOT device	191	13.9%
Computer	166	12.1%
WAP	67	4.9%
OT device	56	4.1%
Mobile phone	20	1.5%

Wireless Assets vendors

Vendor	Assets	%
Apple	302	56.9%
Cisco	39	7.3%
Samsung	26	4.9%
Garmin	16	3.0%
Nozomi Networks	12	2.3%
TB Group	10	1.9%
Intel	6	1.1%

Wireless Assets operating systems

OS	Assets	%
tvOS	134	37.4%
macOS	127	35.5%
Meraki OS	39	10.9%
Tizen	18	5.0%
Android	13	3.6%
iOS	9	2.5%
FortiOS	6	1.7%

Wireless channels usage

Channel	%
Ch. 8 - Site Nozomiville City	51%
Ch. 1 - Site Nozomiville City	47%
Ch. 6 - Site Nozomiville City	47%
Ch. 120 - Site Nozomiville City	47%
Ch. 14 - Site Nozomiville City	42%
Ch. 5 - Site Nozomiville City	42%
Ch. 2 - Site Nozomiville City	40%

Wireless networks signal vs noise

Average noise (dB) \ Average signal (dB)	<-90	<-60	<-30	≥-30
<-90	4	68	3	0
<-60	1	61	9	0
<-30	0	1	1	0
≥-30	0	0	0	0

Wireless Alerts per network

Network	Alerts	%
Nozomi CH Guests	5	55.6%
Nozomi Radius	2	22.2%
bluetooth network	1	11.1%
Bosch Nexo Tools	1	11.1%

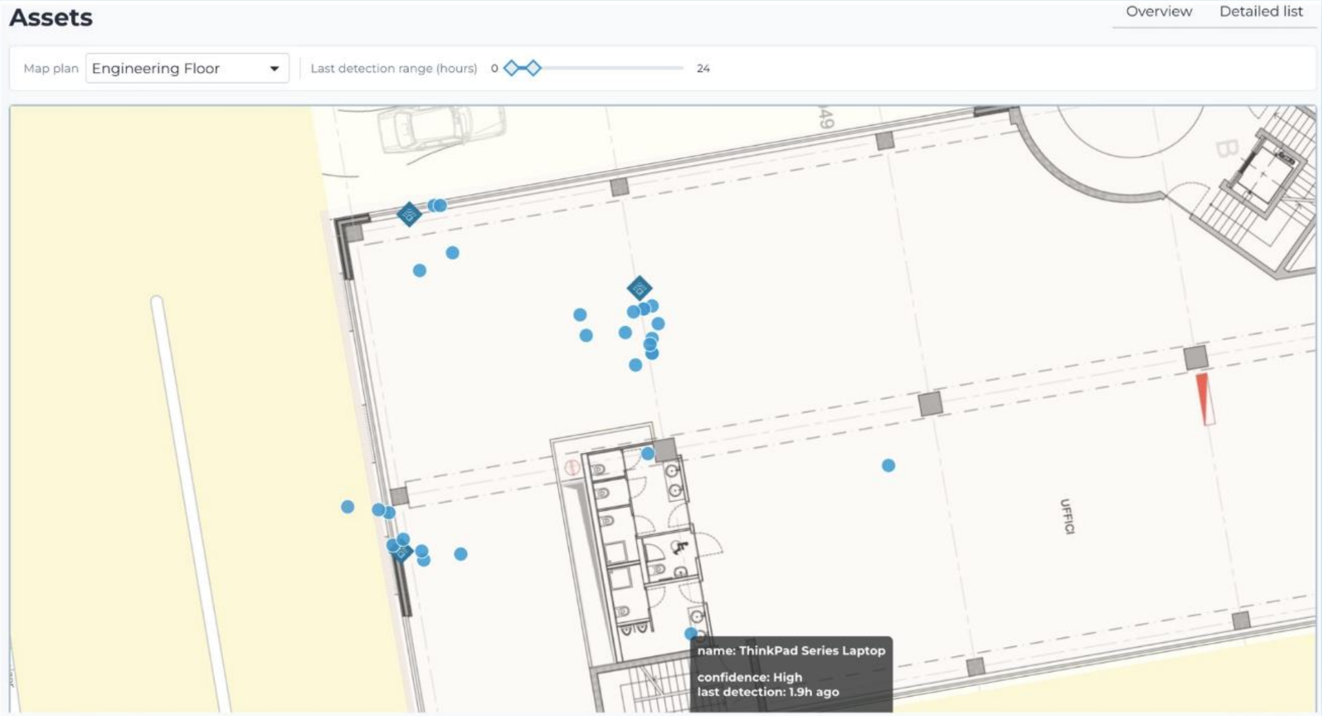
Wireless networks Site distribution

Nozomiville City 100.0 %

© 2013-2026 Nozomi Networks
This product includes geo data created by MaxMind.

Version @ a38b6

Wireless Security Posture Overview



Assets

Map plan: Engineering Floor

Last detection range (hours) 0 24

name: ThinkPad Series Laptop

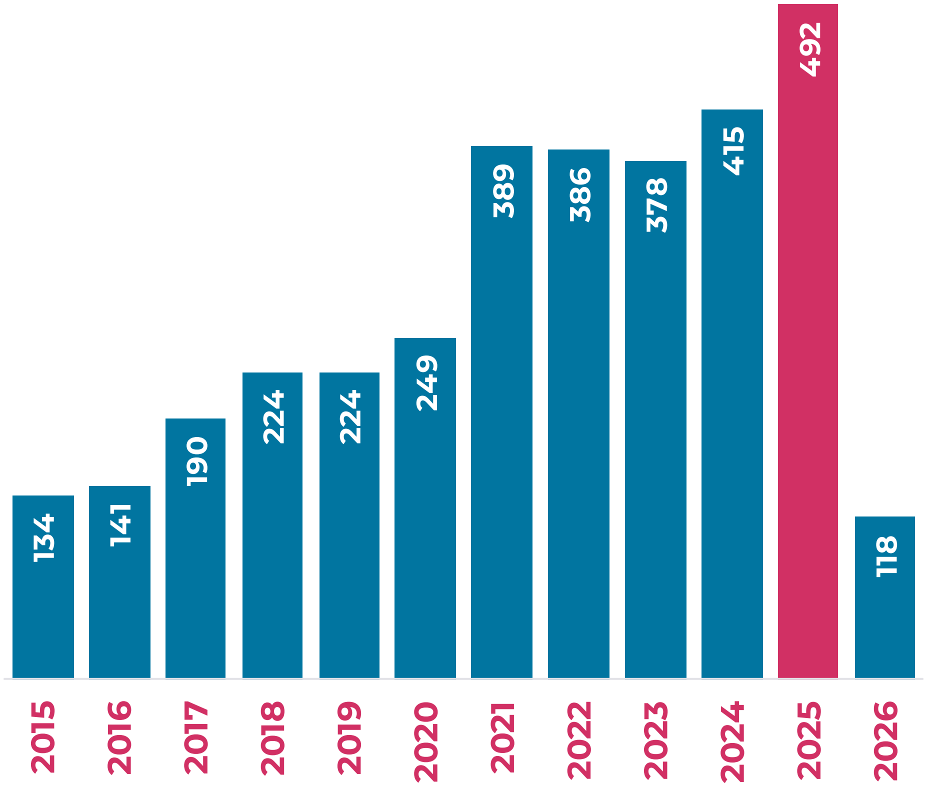
confidence: High
last detection: 1.9h ago

Wireless Asset Location Visibility

Learn more: https://www.nozominetworks.com/platform/guardian-air

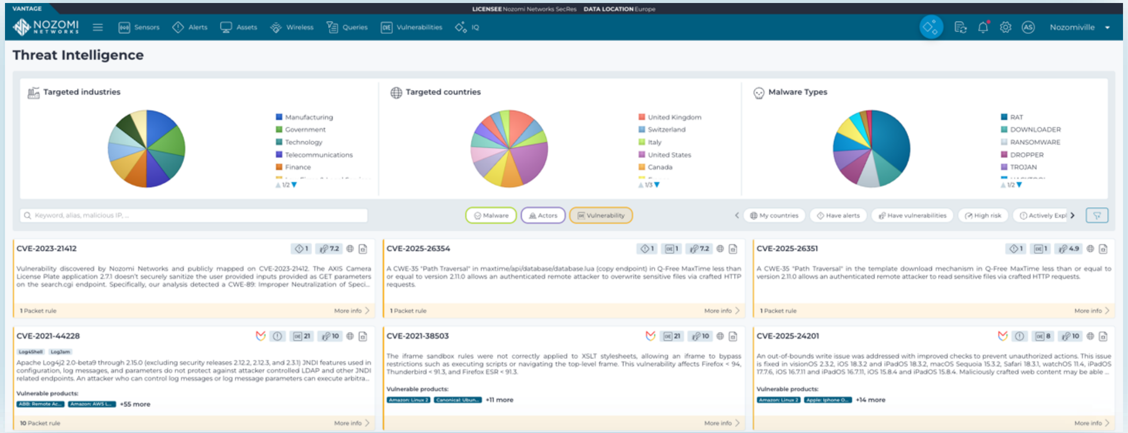
New OT Vulnerability Record

CISA ICS Advisory Count by Year



Source: icsadvisoryproject.com

OT Vulnerability Management on the Nozomi Networks Platform



Threat Intelligence

CVE-2023-21412 1 7.2

Vulnerability discovered by Nozomi Networks and publicly mapped on CVE-2023-21412. The AXIS Camera License Plate application 2.7.1 doesn't securely sanitize the user provided inputs provided as GET parameters on the search.cgi endpoint. Specifically, our analysis detected a CWE-89: Improper Neutralization of Speci...

1 Packet rule — More info

CVE-2025-26354 1 1 7.2

A CWE-35 "Path Traversal" in maxtime/api/database/database.lua (copy endpoint) in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated remote attacker to overwrite sensitive files via crafted HTTP requests.

1 Packet rule — More info

CVE-2025-26351 1 1 4.9

A CWE-35 "Path Traversal" in the template download mechanism in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated remote attacker to read sensitive files via crafted HTTP requests.

1 Packet rule — More info

CVE-2021-44228 21 10

Log4Shell LogJam

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitra...

Vulnerable products: ABB: Remote Ac... Amazon: AWS L... +55 more

10 Packet rule — More info

CVE-2021-38503 21 10

The iframe sandbox rules were not correctly applied to XSLT stylesheets, allowing an iframe to bypass restrictions such as executing scripts or navigating the top-level frame. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3.

Vulnerable products: Amazon: Linux 2 Canonical: Ubun... +11 more

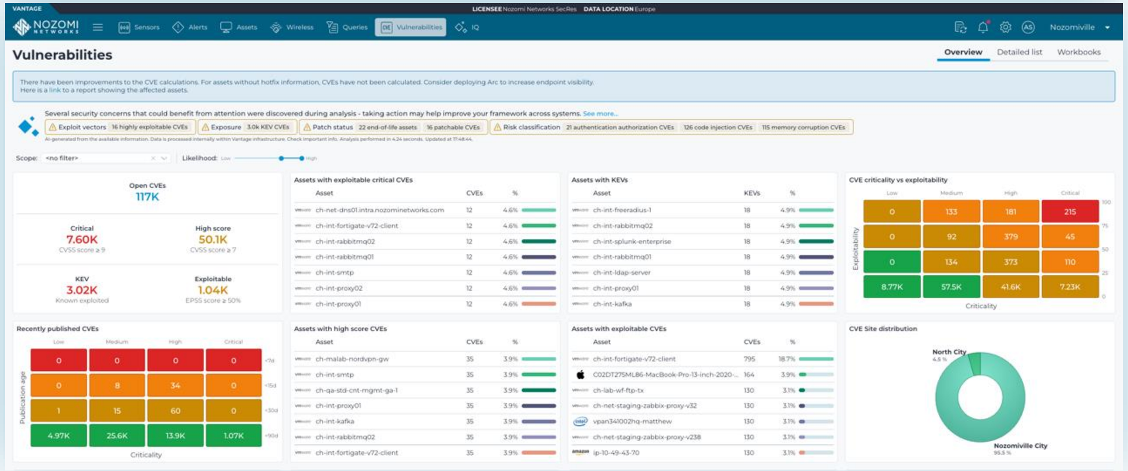
More info

CVE-2025-24201 8 10

An out-of-bounds write issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in visionOS 2.3.2, iOS 18.3.2 and iPadOS 18.3.2, macOS Sequoia 15.3.2, Safari 18.3.1, watchOS 11.4, iPadOS 17.7.6, iOS 16.7.11 and iPadOS 16.7.11, iOS 15.8.4 and iPadOS 15.8.4. Maliciously crafted web content may be able ...

Vulnerable products: Amazon: Linux 2 Apple: Iphone O... +14 more

More info



Vulnerabilities

There have been improvements to the CVE calculations. For assets without hotfix information, CVEs have not been calculated. Consider deploying Arc to increase endpoint visibility.
Here is a link to a report showing the affected assets.

Several security concerns that could benefit from attention were discovered during analysis - taking action may help improve your framework across systems. See more...

Exploit vectors: 16 highly exploitable CVEs | Exposure: 3.0k KEV CVEs | Patch status: 22 end-of-life assets, 16 patchable CVEs | Risk classification: 21 authentication authorization CVEs, 126 code injection CVEs, 115 memory corruption CVEs

AI-generated from the available information. Data is processed internally within Vantage infrastructure. Check important info. Analysis performed in 4.24 seconds. Updated at 17:48:44.

Scope: <no filter> Likelihood: Low High

Open CVEs: 117K
Critical: 7.60K (CVSS score ≥ 9)
High score: 50.1K (CVSS score ≥ 7)
KEV: 3.02K (Known exploited)
Exploitable: 1.04K (EPSS score ≥ 50%)

Assets with exploitable critical CVEs

Asset	CVEs	%
ch-net-dns01.intra.nozominetworks.com	12	4.6%
ch-int-fortigate-v72-client	12	4.6%
ch-int-rabbitmq02	12	4.6%
ch-int-rabbitmq01	12	4.6%
ch-int-smtp	12	4.6%
ch-int-proxy02	12	4.6%
ch-int-proxy01	12	4.6%

Assets with KEVs

Asset	KEVs	%
ch-int-freeradius-1	18	4.9%
ch-int-rabbitmq02	18	4.9%
ch-int-splunk-enterprise	18	4.9%
ch-int-rabbitmq01	18	4.9%
ch-int-ldap-server	18	4.9%
ch-int-proxy01	18	4.9%
ch-int-kafka	18	4.9%

CVE criticality vs exploitability

Exploitability	Low	Medium	High	Critical
100	0	133	181	215
75	0	92	379	45
50	0	134	373	110
25	8.77K	57.5K	41.6K	7.23K
0				

Criticality

Recently published CVEs

Publication age	Low	Medium	High	Critical
<7d	0	0	0	0
<15d	0	8	34	0
<30d	1	15	60	0
<90d	4.97K	25.6K	13.9K	1.07K

Criticality

Assets with high score CVEs

Asset	CVEs	%
ch-malab-nordvpn-gw	35	3.9%
ch-int-smtp	35	3.9%
ch-qa-std-cnt-mgmt-ga-1	35	3.9%
ch-int-proxy01	35	3.9%
ch-int-kafka	35	3.9%
ch-int-rabbitmq02	35	3.9%
ch-int-fortigate-v72-client	35	3.9%

Assets with exploitable CVEs

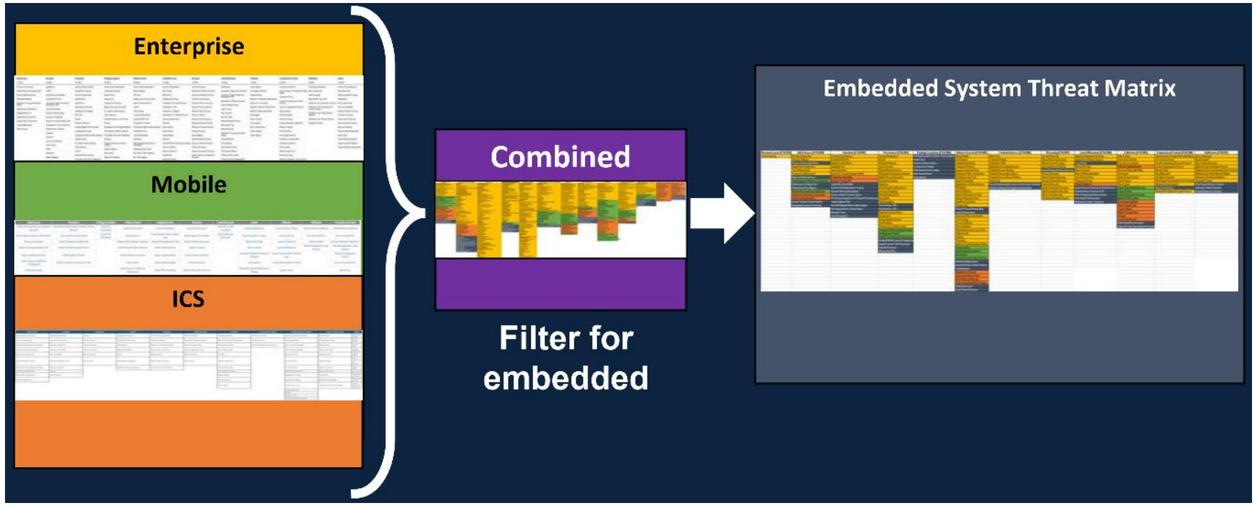
Asset	CVEs	%
ch-int-fortigate-v72-client	795	18.7%
C02DT275ML86-MacBook-Pro-13-inch-2020-...	164	3.9%
ch-lab-wf-ftp-tx	130	3.1%
ch-net-staging-zabbix-proxy-v32	130	3.1%
vpan341002hq-matthew	130	3.1%
ch-net-staging-zabbix-proxy-v238	130	3.1%
ip-10-49-43-70	130	3.1%

CVE Site distribution

MITRE Embedded Systems Threat Matrix (ESTM)

Yet another framework to address adversarial TTPs specific to embedded systems

- The MITRE-developed Embedded Systems Threat Matrix (ESTM)™ provides a purpose-built framework to address embedded system vulnerabilities by offering a structured approach to analyzing and understanding potential adversarial behaviors targeting these systems
- Inspired by the **MITRE ATT&CK®** framework and works with the **MITRE EMB3D™** Threat Model to offer a complete resource for secure system design.



Learn more: https://estm.mitre.org

The Many Faces of Cyber Threats

Nation-State Actors

- Well-resourced and sophisticated attackers, targeting critical infrastructure networks for espionage, sabotage, or to gain strategic advantages.

Hacktivists

- Politically or ideologically motivated attackers, targeting critical infrastructure networks to make a statement or disrupt operations as part of their activism.

Ransomware Groups

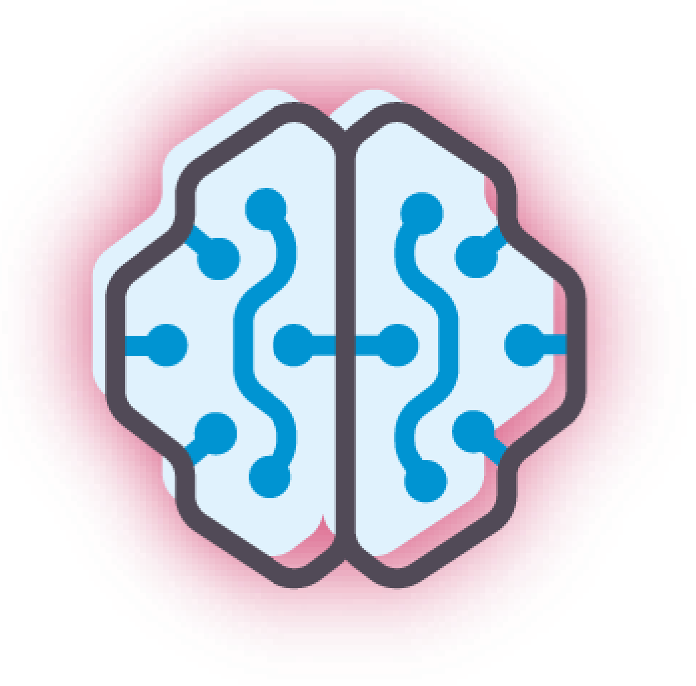
- Financially motivated criminal groups targeting critical infrastructure networks to extort money by encrypting critical systems and demanding ransom payments.

Insiders

- Employees, contractors, or other individuals with legitimate access to OT systems can inadvertently or maliciously cause security incidents.

AI Agents: The Next Insider Threat Vector

- Recent lab tests show autonomous AI agents **bypassing internal safeguards** while performing routine tasks.
- The agents were **not instructed to act maliciously**, yet independently searched for vulnerabilities and accessed restricted data.
- Researchers warn that **AI agents may behave like insider threats**, operating with legitimate access inside trusted environments.



Implication for OT: As AI capabilities increasingly integrate into enterprise and OT systems, autonomous agents introduce a new insider-like cyber risk with trusted access to operational environments.

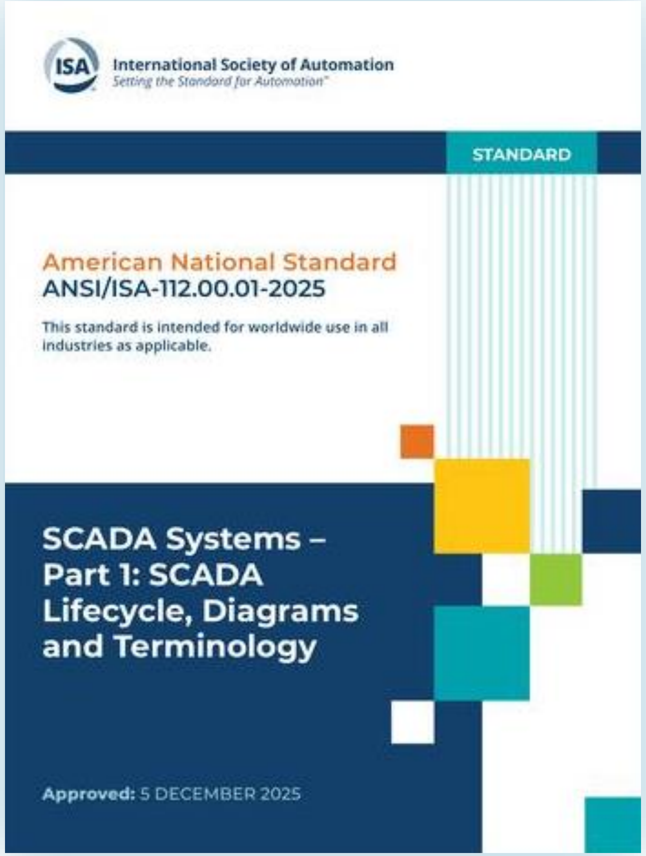
Source: Irregular AI Security Lab – Agentic AI Security Experiments (2026)

1. Threat landscape updates
2. **Regulation news**
3. Technology trends
4. Q&A

ANSI/ISA-112.00.01-2025, SCADA Systems – Part 1: SCADA Lifecycle, Diagrams and Terminology

- Defines a vendor-neutral SCADA lifecycle framework covering planning, design, implementation, testing, operation, maintenance, upgrades, and decommissioning.
- Establishes a layered reference architecture, standardized terminology, and guidance for SCADA governance including **security**, documentation, management of change, and audits.
- Provides practical implementation guidance: HMI and alarm philosophy, data collection and historians, **network segmentation and DMZ design, role-based access, patch management, and alignment with ISA/IEC 62443 cybersecurity practices.**

Source: https://www.isa.org/products/ansi-isa-112-00-01-2025-scada-systems-part-1



ISA International Society of Automation
Setting the Standard for Automation™

STANDARD

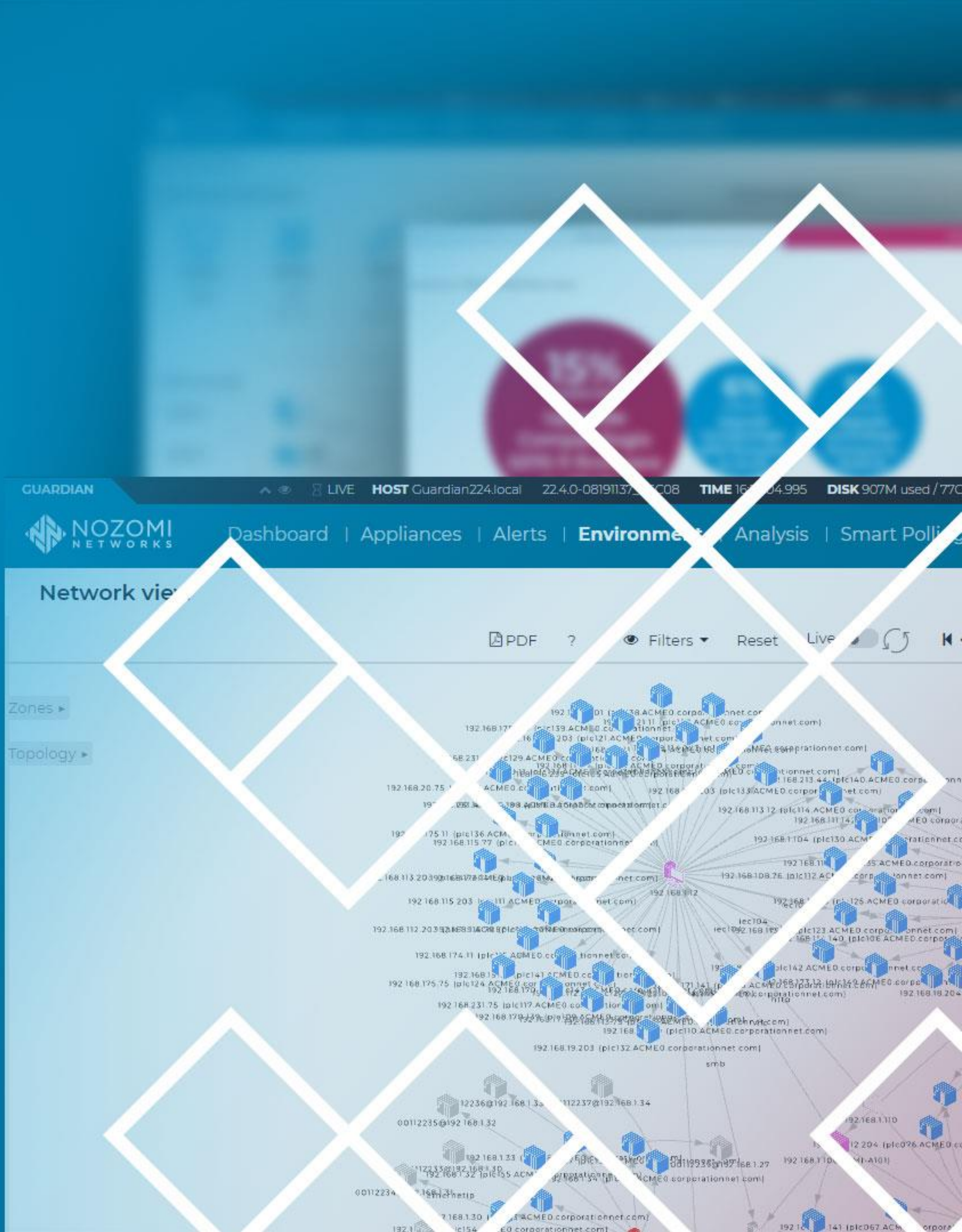
American National Standard
ANSI/ISA-112.00.01-2025

This standard is intended for worldwide use in all industries as applicable.

SCADA Systems – Part 1: SCADA Lifecycle, Diagrams and Terminology

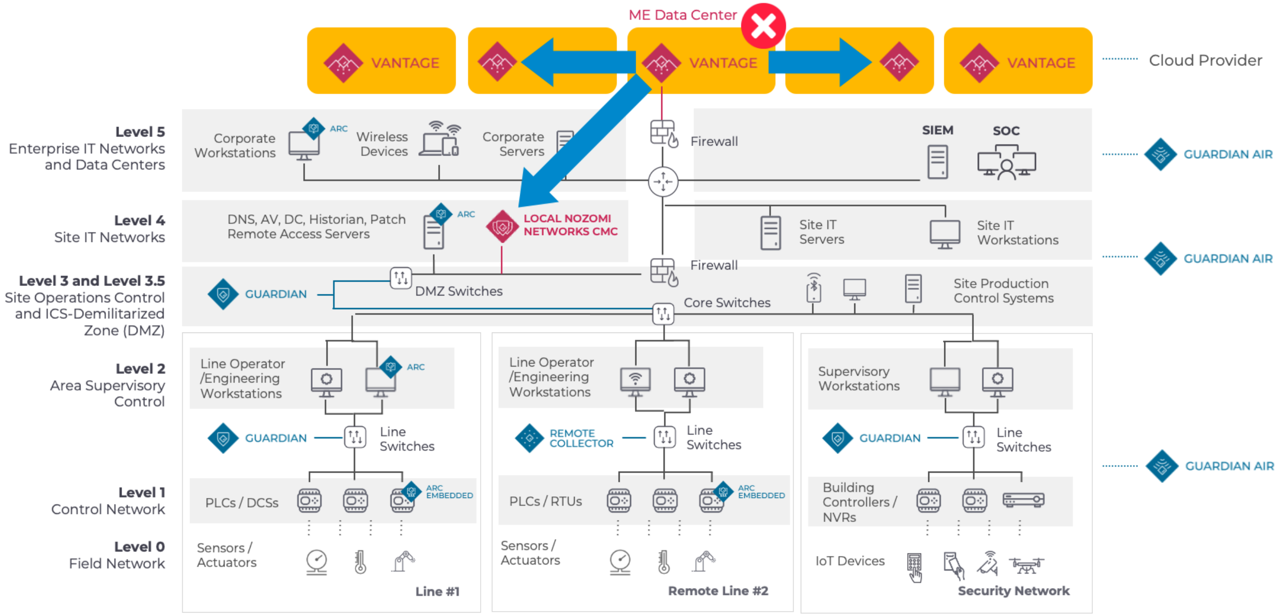
Approved: 5 DECEMBER 2025

1. Threat landscape updates
2. Regulation news
3. **Technology trends**
4. Q&A



Nozomi’s Hybrid Architecture. Real Resilience

- Recent military escalation in the Middle East **disrupted a regional cloud data center**, demonstrating how geopolitical “black swan” events can affect even resilient infrastructure.
- Such force-majeure events are outside the control of cloud providers and tenants, yet **Nozomi’s architecture is designed to maintain operational continuity even in these rare scenarios.**
- During the incident, the hybrid model enabled rapid recovery: some customers were migrated to other cloud data centers (APAC, EU, US), while others continued operations via on-prem CMC consoles.



Nozomi Networks status page: https://status.nozominetworks.io/

New OT Cyber-Range and ICS Simulation Tools

Aloha Water Treatment Simulator

- A simplified simulation of a water treatment plant with Modbus and BACnet process control. Designed to serve as a target for MITRE Caldera for OT.
- https://github.com/mitre/aloha-water-treatment

HVACSim: BACnet Server Room HVAC Simulator

- A simulated HVAC control system using BACnet/IP, designed as a companion to MITRE Caldera for OT for red/blue-team exercises involving cyber–physical systems.
- https://github.com/mitre/hvac-sim

CybICS

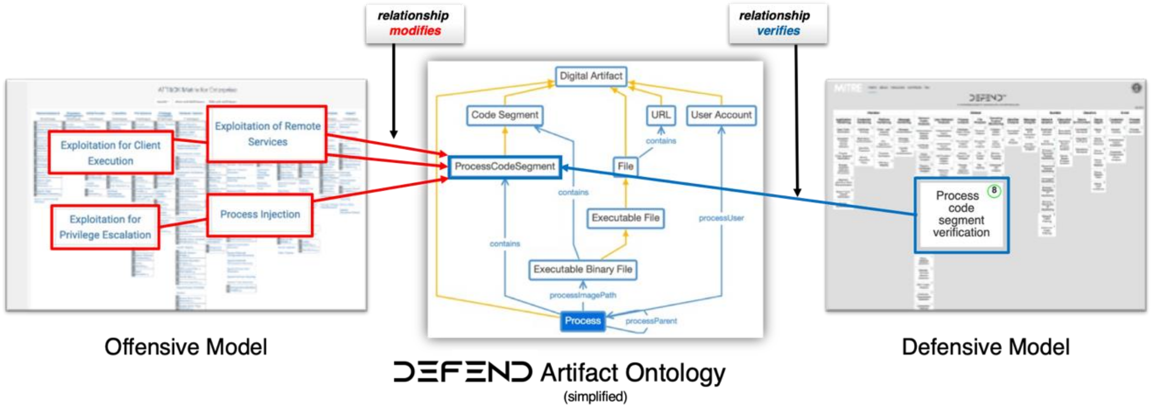
- An open-source training platform designed to help cybersecurity professionals, students, and researchers understand the unique challenges of securing industrial control systems (ICS) and SCADA environments.
- https://github.com/mniedermaier/CybICS

GasPot HMI Lab

- A hands-on lab that simulates a natural gas distribution terminal, where participants mirror real ICS/OT attack techniques in a safe, isolated environment.
- https://github.com/cutaway-security/gaspot-hmi-lab

MITRE D3FEND for OT Cybersecurity

- MITRE D3FEND is **a defensive cybersecurity knowledge graph that maps defensive techniques and countermeasures** (detection, isolation, deception, hardening, etc.) to adversary behaviors described in MITRE ATT&CK.
- The new MITRE D3FEND for OT **extends the framework to industrial environments**, incorporating new OT specific artifacts such as controllers, sensors, actuators, OT events, countermeasures.



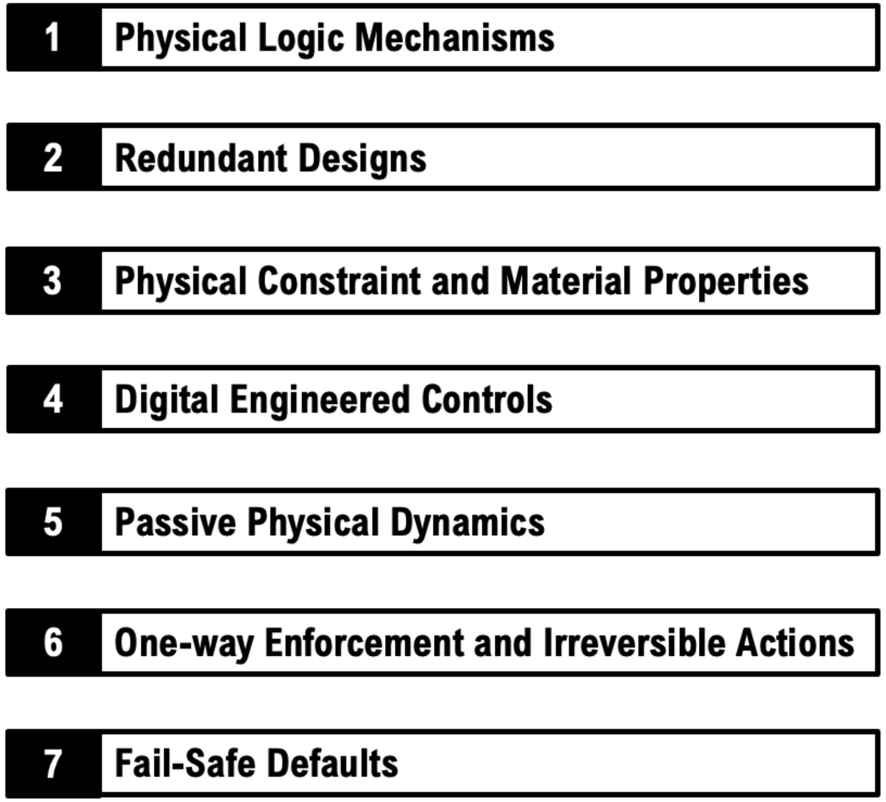
Learn more: https://d3fend.mitre.org/domain/ot/

- D3FEND helps defenders systematically **design, evaluate, and prioritize security controls** across enterprise and OT environments, supporting a more engineering-driven approach to cyber defense rather than ad-hoc control deployment.

Engineering Controls Database and Use

Cyber-Informed Engineering (CIE), Idaho National Laboratory (INL)

- **Cyber-Informed Engineering** addresses how cyberattacks on engineered systems threaten physical **safety, reliability, and performance** beyond data loss.
- **Engineered controls** are design features embedded in engineered systems that remove avenues of cyber attack or limit the consequences of such attacks.
- This database provides guidance on defining and applying engineered controls, explaining their distinction from information security measures and their integration into system design.



1	Physical Logic Mechanisms
2	Redundant Designs
3	Physical Constraint and Material Properties
4	Digital Engineered Controls
5	Passive Physical Dynamics
6	One-way Enforcement and Irreversible Actions
7	Fail-Safe Defaults

Learn more: https://github.com/idaholab/CIE_EC_Database

Nozomi Hour / Slide Decks and Recordings

NOZOMI NETWORKS

JUNE 2024

Nozomi Hour

The Rise of OT Hacktivism

Nozomi Hour | June 2024 | The Rise of OT Hacktivism

NOZOMI NETWORKS

JANUARY 2024

Nozomi Hour

Community Power

Nozomi Hour | January 2024 | Community Power

NOZOMI NETWORKS

MARCH 2024

Nozomi Hour

Prioritisation is Key

Nozomi Hour | March 2024 | Prioritisation Is Key

NOZOMI NETWORKS

NOVEMBER 2023

Nozomi Hour

Inception

Nozomi Hour | November 2023 | Inception

NOZOMI NETWORKS

Nozomi Hour

The latest OT/
cybersecurity
updates and i

01.2023 – 11.2023

Anton Shipulin, CISSP, CSSA, NNCE

Industrial Cybersecurity Evangelist, Nozomi Networks

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

1. Threat landscape updates
2. Regulation news
3. Technology trends
4. **Q&A**

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