OT Under Pressure: The Evolving Threat Landscape in the Baltics

Davide Boglioli

Vulnerability Assessment Technical Lead,
Nozomi Networks



Three findings before the evidence

Findings from regional assessments and incident reports

01

Deliberate disruption is a credible threat

Regional assessments and the Polish energy attacks justify planning for it.

02

Familiar weaknesses can open unexpected routes

Remote access, credentials and private connectivity can cross organisational boundaries.

03

Detection and recovery can limit the consequences

Operational outcomes depend on the controls and response available at each site.

SAB Annual Report 2025; CERT Polska energy-sector reports

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

From regional pressure to operational decisions

Evidence and operational actions, followed by questions

01	**The regional picture**	Actors, Baltic reporting and infrastructure dependencies
02	**The Polish case**	A detailed path into OT and the outcomes at each target
03	**Recurring weaknesses**	PLC campaigns, HMI access and production dependencies
04	**What is changing**	Remote access, endpoint and wireless visibility, and AI
05	**What works**	Controls, Lithuanian requirements and conclusions

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Motives differ, access can overlap

Three actor groups and a separate lens on trusted access

State-linked actors

Espionage, strategic access and deliberate disruption.

Financially motivated groups

Extortion through data theft, encryption or service disruption.



Hacktivist groups

Political signalling and disruption, sometimes with physical effects.

Insiders and suppliers

Legitimate access can be misused or compromised. This describes access risk, not one motive.

Attribution helps explain intent. Actual access determines what an actor can reach.

SAB Annual Report 2025; NIST SP 800-82 Rev. 3

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Who targets the Baltics: what the services say

2026 assessments: intent, capability and attribution

Persistent Russian pressure

VDD identifies Russian services as Latvia's main national-security threat; Lithuania's assessment stresses long-term military ambition.

Industrial systems in scope

SAB reports Russian hacktivists' intent and capability to target industrial control systems.

Physical sabotage by proxy

KAPO attributes Milrem's August 2026 arson to Russian services.

VDD; VSD / AOTD; SAB; KAPO and the Estonian government · 2026 publications

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

2025–26: four events around the Baltic Sea

Cyber incidents, physical damage and successful preparation



9 FEB 2025

Grid resilience

The Baltics synchronised with Continental Europe.



29 DEC 2025

Cyber sabotage

Polish energy facilities were disrupted; customer supplies continued.



31 DEC 2025

Physical damage

Two telecom cables were damaged in the Fitburg case.



22 JUN 2026

IT disruption

Latvian State Forests detected an attack; IT services and deliveries were affected.

ENTSO-E; CERT Polska; Finnish Police; CERT.LV; Latvian State Forests

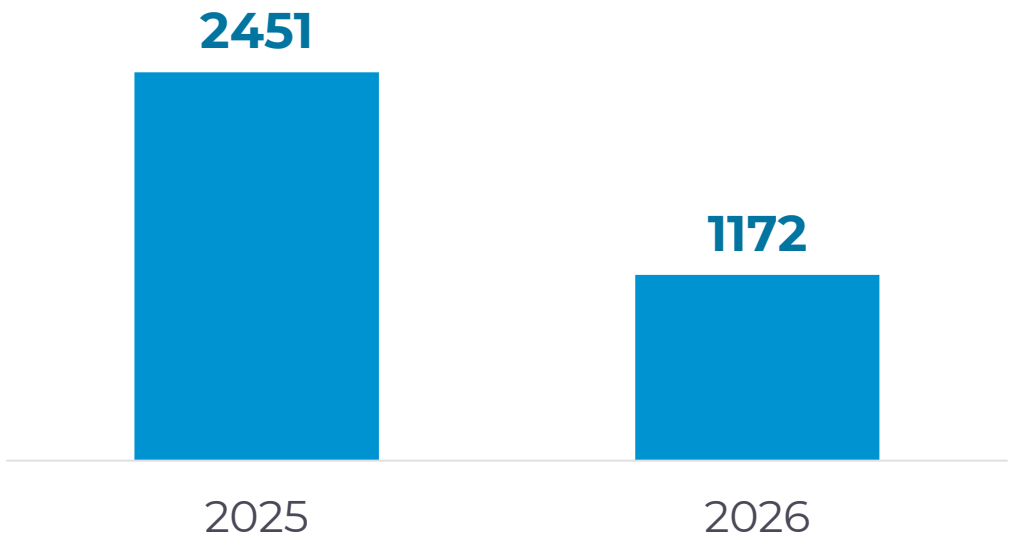
© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Lithuania: fewer reported incidents in 2026

NKSC national cyber reporting, January–September 2025 vs 2026

RECORDED CYBER INCIDENTS



52% fewer recorded incidents

1,172 in January–September 2026, compared with 2,451 in the same period of 2025.

Information gathering in 2026

499 incidents involved information gathering: 43% of the 1,172 recorded in January–September 2026.

National cyber reporting does not establish an impending OT attack.

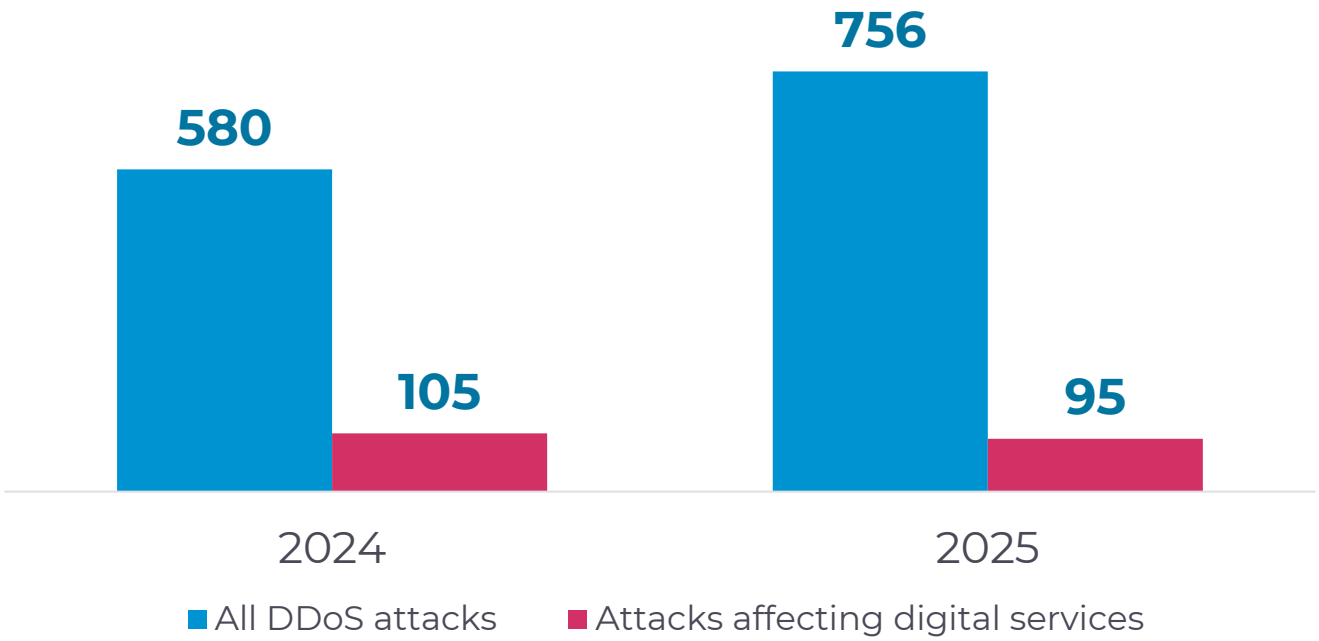
NKSC · 14 October 2026 update

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Estonia: more DDoS attacks, fewer with impact

Service impact: outages or slowdowns of websites and online services



95 of 756

DDoS attacks caused outages or slowdowns on websites and online services in 2025

SEPARATE NATIONAL TOTAL

10,185 incidents with impact across all categories in 2025

RIA links lower disruption to DDoS protection services.

RIA · DDoS statistics and Cyber Security in Estonia 2026

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Latvia: high activity, visibility and real consequences

CERT.LV reporting spans all sectors

923 → 846

Manually handled incidents, Q4 2025 → Q1 2026.

757,286 devices flagged

Q1 2026 · CERT.LV. Mostly configuration weaknesses; broader monitoring also increased visibility.



LVM, June 2026

An IT attack disrupted digital services and timber deliveries; recovery included paper delivery notes.



National Cybersecurity Law

Reporting and cybersecurity ownership duties already apply to covered entities.

CERT.LV · Q4 2025 and Q1 2026 reviews, incident and legal guidance; LVM

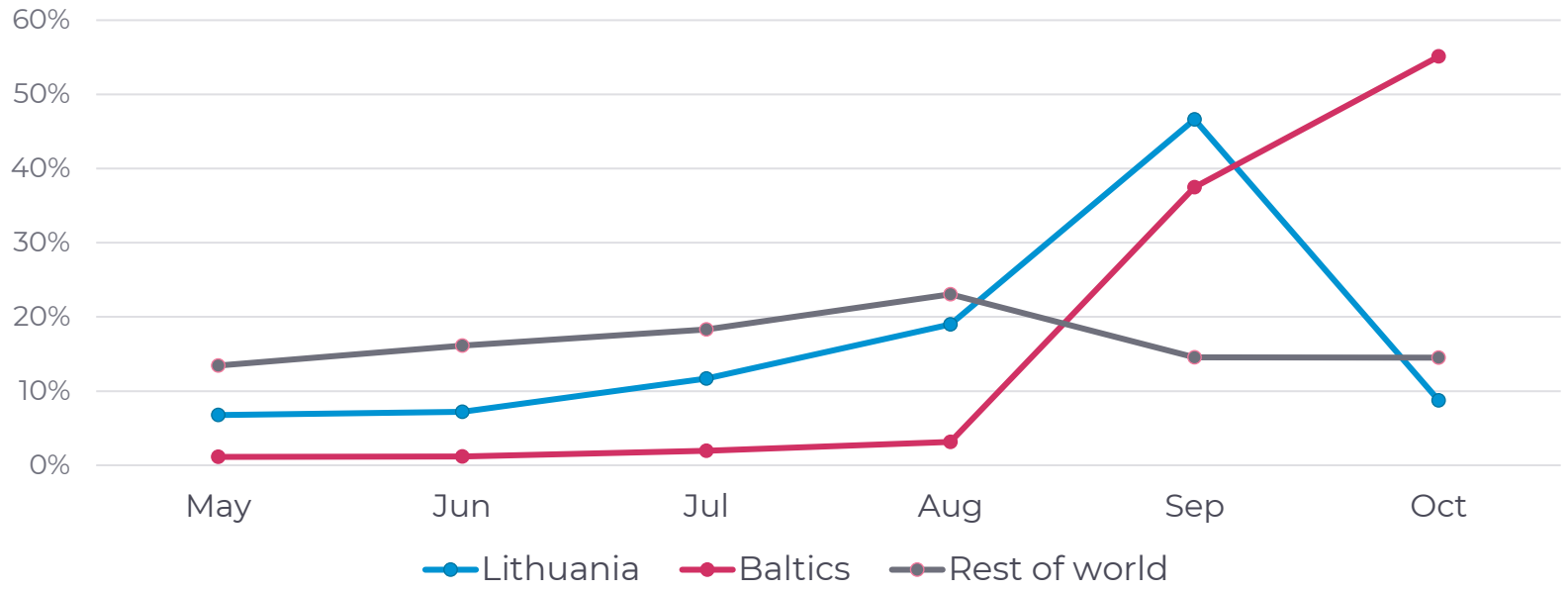
© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Six months of recorded alerts

Each line distributes its own May–October alert total across the months. Lithuania is part of the Baltics.

Monthly records ÷ same sample's May–October total × 100



916

Lithuania
May–October records

5,508

Baltic sample
May–October records

143.6M

Rest of world
May–October records

Estonian telemetry appears in September. Coverage affects the observed trend.

Source: Nozomi Networks telemetry in Grafana / Loki. Six-month lookback ending 1 Nov 2026, 00:00 UTC.

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Access-related alerts: 37% of the Baltic sample

Five leading Baltic alert types · May–October 2026

Share of each sample's alerts · ATT&CK Enterprise mapping

Alert type · ATT&CK	Baltics	Lithuania	Rest of world
Access denied · T1110	24.80%	15.72%	3.95%
Malicious domain · T1071 / T1095	15.85%	0.00%	3.74%
Malformed traffic · T1565	14.34%	12.34%	2.63%
Unsuccessful logins · no tag	11.98%	0.00%	4.74%
Packet rule match · T1190 + others*	10.28%	0.00%	1.72%
Other	22.75%	71.94%	83.22%

Alerts do not necessarily indicate a confirmed attack.

Source: Nozomi Networks, Grafana/Loki · Baltic ATT&CK tags; *additional packet-rule techniques in notes.

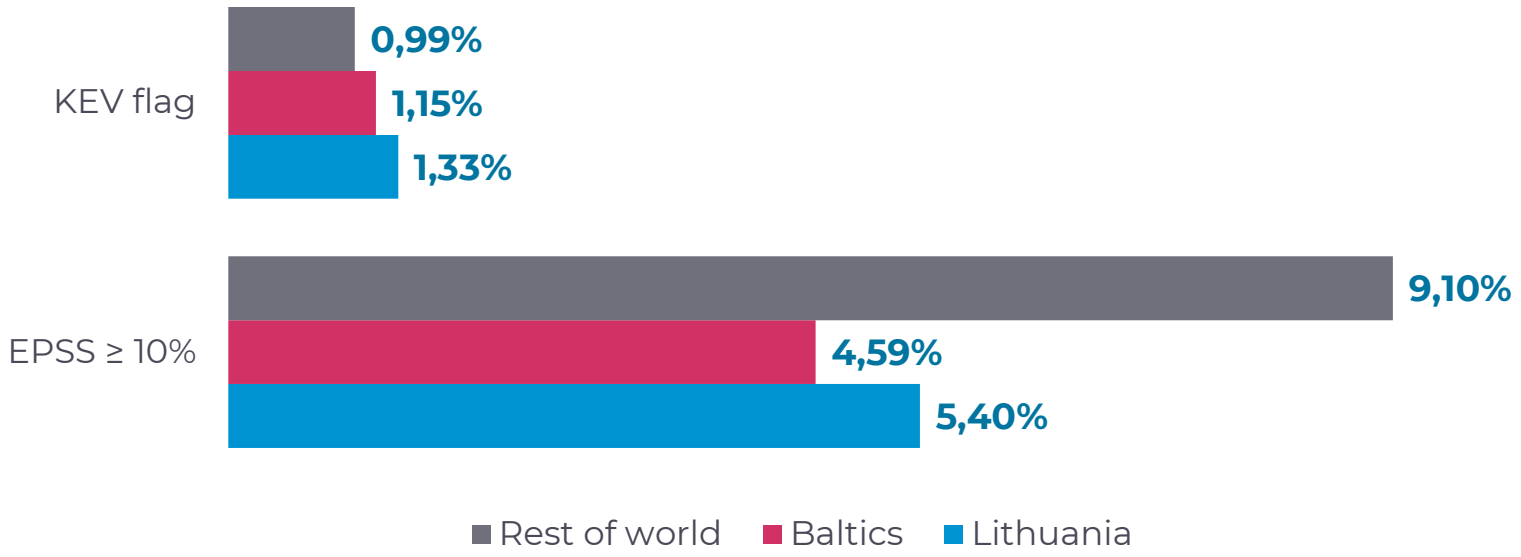
© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

CVE priorities differ across the observed samples

Share of distinct CVE IDs that met each condition at least once.

Share of distinct observed CVE IDs



7,312

Distinct CVE IDs in Lithuania

11,443

Distinct CVE IDs in the Baltics

83,356

Distinct CVE IDs in the rest of the world

KEV and EPSS groups overlap. An observed CVE does not prove exploitation.

Source: Nozomi Networks telemetry in Grafana / Loki. Six-month lookback ending 1 Nov 2026, 00:00 UTC.

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Baltic operations depend on physical connections

Cables and interconnectors: physical dependencies, separate from cyber intrusion

ESTLINK 2

650 MW



25 Dec 2024 – 20 Jun 2025

Transmission capacity unavailable for about six months.

Fitburg

Two telecom cables damaged; Finland's June 2026 investigation identified four suspects.

Regional resilience

Baltic Sentry strengthens protection of undersea infrastructure.

Harmony Link

700 MW planned; construction from 2027, operation expected by end-2030.

Physical dependency failures belong in continuity planning.

Elering; Finnish Police; NATO; ENTSO-E; Litgrid · Sources and scope in notes

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Hacktivist DDoS: pressure continues after disruption

Availability attacks require a separate operational risk assessment



Lithuania, June 2022

Killnet-linked DDoS disrupted public and private websites.



DDoSia, July 2024–July 2025

Over 3,700 distinct targeted hosts; about 50 daily, including repeat targets.



Eastwood, July 2025

Authorities disrupted 100+ systems; NoName057(16) remained active in 2026.

Online service disruption alone does not demonstrate control-system access.

Lithuanian Ministry of Defence; Recorded Future; Europol; Bitsight

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Cyberattack on critical infrastructure in Poland

29 December 2025



30+ renewable sites

Remote control lost; electricity generation continued.



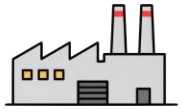
Large CHP

EDR blocked DynoWiper; heat supply maintained.



Small CHP

PLC STOP disrupted cogeneration.



Manufacturer

LazyWiper deployed through Group Policy.

Customer electricity and heat supplies remained continuous.

CERT Polska · January and August 2026 incident reports

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

An unexpected route across a private APN

Reconstructed path into the smaller CHP

WIND-FARM NETWORK

1 FortiGate VPN



VPN accounts without MFA.

2 Teltonika RUTX50



SSH access. Entry method unknown.

DSO PRIVATE APN

3 Private APN



Reachability across sites.

SMALL CHP NETWORK

4 WAGO PFC200



Default login. Probable SSH tunnel.

5 Siemens PLCs



STOP mode and password lockout.

18–25 December: reconnaissance. 29 December: disruption.

Private connectivity allowed a route between operational environments.

CERT Polska · Private-APN follow-up, August 2026

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Poland: what held, what failed

Control boundaries mattered more than network labels



Segmentation

Restrict what each remote session can reach.



Private APNs

Verify isolation between connected sites.



Endpoint protection

Large CHP: DynoWiper blocked.



Operational recovery

Small CHP: customer supplies maintained.

EU and UK attributed the campaign to FSB Centre 16 in July 2026.

Validate reachability, detection and recovery as separate capabilities.

CERT Polska; Council of the EU and UK Government · July 2026 attribution

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Regional incidents, 2025–2026

Recent cases in the Baltics and neighbouring Poland

Incident	Access or control issue	Observed effect
Selver, Estonia **2 November 2026**	Refrigeration control compromised; setpoint changed to +50°C.	Actual rise: 2–3°C. Rapid response prevented product loss.
Latvian State Forests **June 2026**	Ransomware incident; IT disconnected for containment.	Timber deliveries interrupted; full digital deliveries restored 1 July.
Polish energy sector **29 December 2025**	VPN/APN access, weak segmentation and default controller credentials.	Remote control and processes disrupted; customer electricity and heat maintained.

Cyber incidents can disrupt operations through control systems or supporting IT.

ERR (operator and supplier interviews); CERT.LV; LVM; CERT Polska · Case-specific sources in notes

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

US PLC targeting: two distinct alerts

Overlapping techniques, different attribution

01 EXPOSED	**Exposed controller**
02 CHANGE	**Unauthorized changes**
03 LOCKOUT	**Operator lockout**
04 IMPACT	**Operational disruption**

AA26-097A · April–July 2026

Iranian-affiliated actors: PLC project manipulation and HMI/SCADA changes caused disruption.

FBI/EPA · 30 July 2026

MicroLogix targeting in at least seven states: changed passwords and IP addresses, operator lockout and reported water impacts. Actor unnamed.

Shared integrator configurations can repeat exposure.

CISA AA26-097A; FBI / EPA I-073026-PSA · Separate 2026 advisories

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Pro-Russian hacktivists at the HMI

Joint advisory AA25-343A · December 2025



Access

Internet-exposed VNC and HMIs with weak, default or missing passwords.



Process changes

Settings changed, alarms disabled and operators lost reliable visibility.



Effects

Disruption and, in documented cases, physical damage.

Named groups: CARR, Z-Pentest, NoName057(16) and Sector16.

Limited technical sophistication can still create operational harm.

FBI, CISA, NSA and partners · Joint advisory AA25-343A, December 2025

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

When cyber incidents stop production

Supporting systems are part of the operational dependency map



JLR

Sep–Oct 2025

Cyber incident halted production; restart was phased.



Stryker

March 2026

Microsoft disruption affected manufacturing and shipping.



fairlife

July 2026

Ransomware temporarily halted US production.



West Pharmaceutical

May 2026

Containment halted production after theft and encryption.

Include shared systems and recovery dependencies in continuity planning.

Company disclosures · JLR, Stryker, fairlife and West Pharmaceutical

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Ransomware: data theft and recovery pressure

Mandiant's 2025 response cases · reported March 2026

77%

Suspected data theft in analyzed ransomware intrusions

~43%

Intrusions in which attackers targeted virtualization infrastructure

Encryption and extortion

Encryption and extortion can occur together.

Recovery preparation

Protect sensitive data and backup administration. Test recovery when shared infrastructure is unavailable.

Sample excludes incidents involving only data-theft extortion.

Google Threat Intelligence Group / Mandiant · 2025 response cases, reported March 2026

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Remote access defines a route into operations

The route into operations includes every remote-access path.

The entry point

Patch gateways, replace default credentials and require MFA.

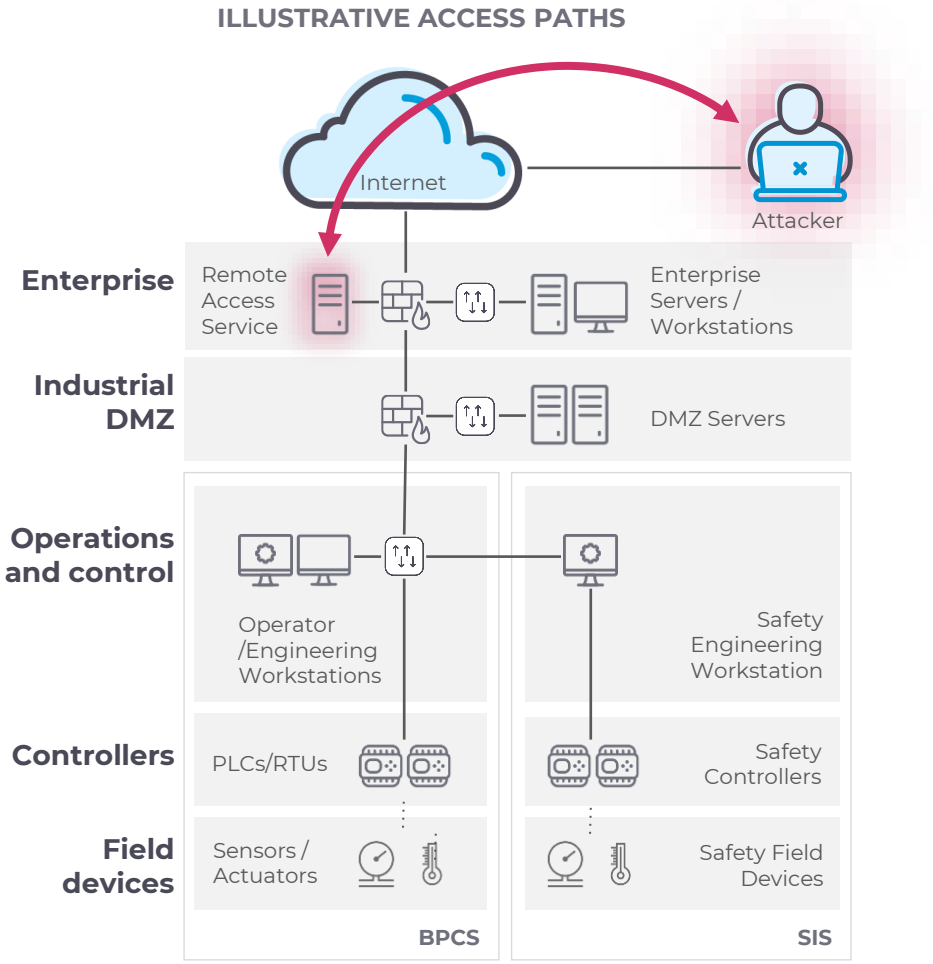
The permitted route

Use approved jump hosts and explicit access between zones.

Other connections

Review vendor, cellular and private-APN paths separately.

Limit reachability after gateway compromise.



CERT Polska; NIST SP 800-82 Rev. 3 · Illustrative defensive access model

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Visibility must connect access to process changes

Access, endpoint and network evidence answer different questions.

Access systems

Who connected, from where, and what could they reach?

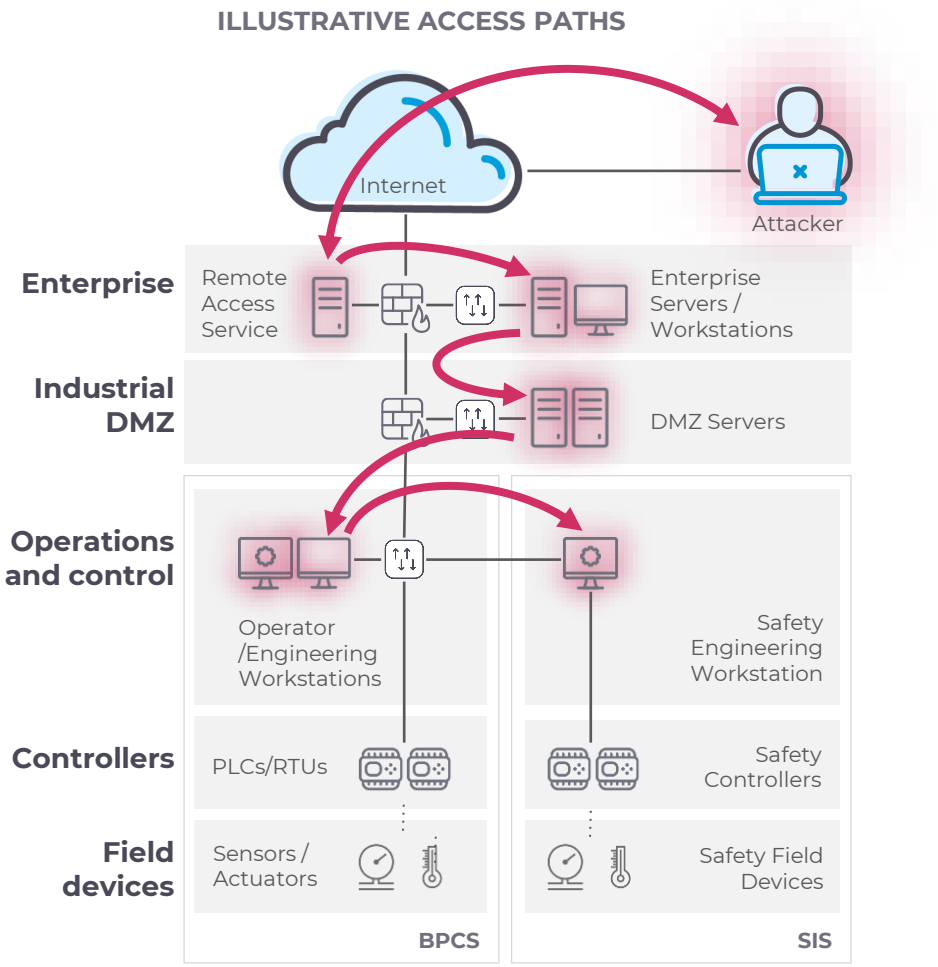
OT endpoints

Which process ran? Which host or project changed?

OT network

Which device received which command? Was it expected?

Link evidence to process state and a response owner.



NIST SP 800-82 Rev. 3; CERT Polska · Operational interpretation

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Wireless coverage adds a different view

Observed networks in the Nozomi Networks H2 2025 customer sample

68%

Without Management Frame Protection

0.3%

Detected Wi-Fi networks using 802.1X

14%

Open or legacy security modes

These figures describe the observed sample, not all industrial wireless networks.



What a wired sensor can see

Wi-Fi traffic that crosses its monitored network point.



What requires radio visibility

Management frames and nearby or off-path wireless activity.

Nozomi Networks · OT & IoT Security Report, second half of 2025

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

AI-assisted tooling is documented

The evidence supports specific capabilities and bounded conclusions

Siemens S7 advisory, August 2026

AI-generated scripts supported reconnaissance and capability development, disguised as monitoring tools.

LAMEHUG, July 2025

Malware queried an LLM to generate reconnaissance and data-collection commands.

LazyWiper, December 2025

CERT Polska assessed that substantial parts of the wiper were likely generated with an LLM.



Siemens S7 family, illustrative image

These findings do not establish an autonomous AI attack causing physical damage.

Detection should cover behaviour even when the tooling changes.

Joint Siemens S7 advisory; CERT-UA LAMEHUG report; CERT Polska

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Controls that interrupt the attack path

Practical priorities aligned with CISA CPG 2.0 and OT operating constraints

Map assets and routes

Include vendors, cellular gateways and private APNs.

CPG 2.A, 2.E

Remove direct exposure

Restrict controller, HMI and management access.

NIST SP 800-82

Prioritise vulnerable systems

Consider exploitation, reachability and process criticality.

CPG 2.B

Protect remote access

Replace defaults. Require unique credentials and MFA.

CPG 3.A, 3.C, 3.F

Limit cross-zone access

Allow only required paths, even after gateway compromise.

CPG 3.I

Detect operational changes

Correlate endpoint, access and protocol evidence.

CPG 4.A, 4.B

Protect recovery material

Keep trusted projects, configurations, tools and licences.

CPG 3.O

Rehearse safe recovery

Test isolation, fallback and restoration with operations.

CPG 1.C, 6.A

CISA CPG 2.0; NIST SP 800-82 Rev. 3; CERT Polska · Applied defensive priorities

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Lithuania: obligations follow scope and timing

Entity registration, incident reporting and energy-sector requirements

12 / 24 months	**Implementation after entity registration** Organisational and specified technical measures have different implementation periods.
24h / 72h / 1 month	**Significant-incident reporting** Early warning, notification and final report. Confirm the trigger and NKSC reporting route.
>100 kW Pmax	**Generation and storage** Check remote-access restrictions, declaration and audit duties under the September 2026 rules.

Confirm your entity's scope, registration date and current reporting procedure.

NKSC FAQs; ESO · Requirements checked against September 2026 guidance

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Resilience is measurable

Observed outcomes from cases already discussed

Case	What held	Observed outcome
Poland: large CHP	Endpoint protection	DynoWiper deployment blocked
Poland: small CHP	Operator response	Customer heat and electricity supplies maintained
Estonia: DDoS	Protection services	95 attacks with impact in 2025, down from 105 in 2024

Protection and response can limit the consequences of a compromise.

CERT Polska · January and August 2026 reports; RIA · 2024–25 DDoS comparison

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.

Conclusions and next actions

Conclusion	Monday morning
Deliberate disruption belongs in the Baltic threat model.	Identify one critical process and its external dependencies.
Familiar weaknesses can enable unexpected routes into OT.	Trace vendor, VPN and cellular access across trust boundaries.
Detection and recovery can limit operational consequences.	Validate one alert and rehearse restoring that process.

Keep critical services running and restore trustworthy control.

Conclusions and proposed actions drawn from the evidence discussed

© 2026 Nozomi Networks Inc. | All rights reserved. | nozominetworks.com

Internal — This document contains propietary information intended only for Nozomi Networks personnel.



Questions

Thank you

nozominetworks.com

Davide Boglioli

Vulnerability Assessment Technical Lead

Nozomi Networks