SECTRA

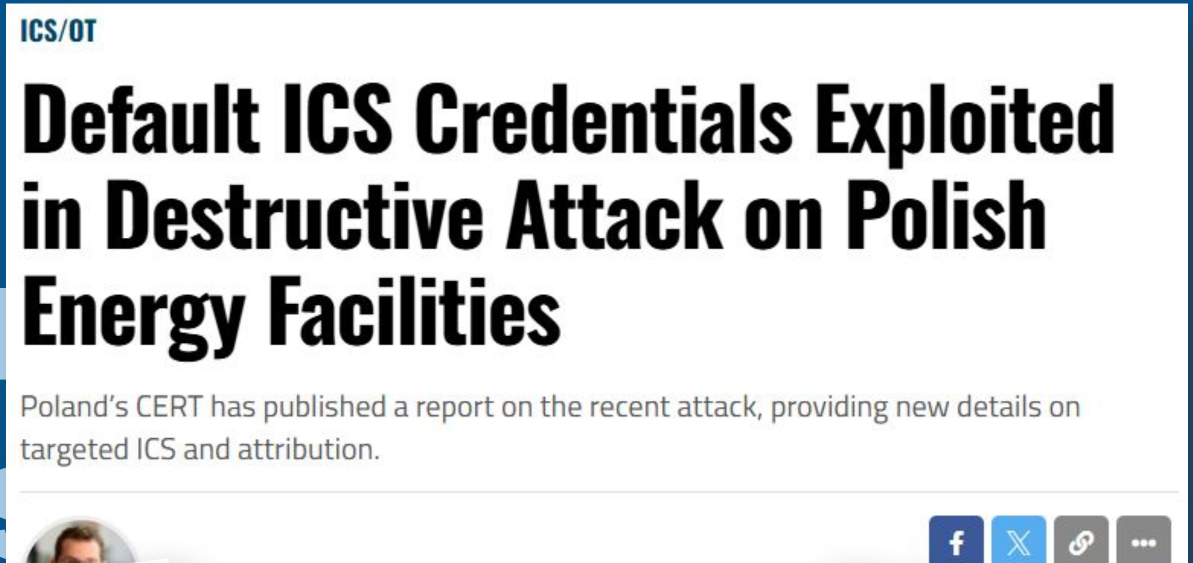
Defending Critical Infrastructure from Cyber Attacks

Lessons learned from recent examples of attacks, and how to detect future attacks

SECTRA

Defe

Infras



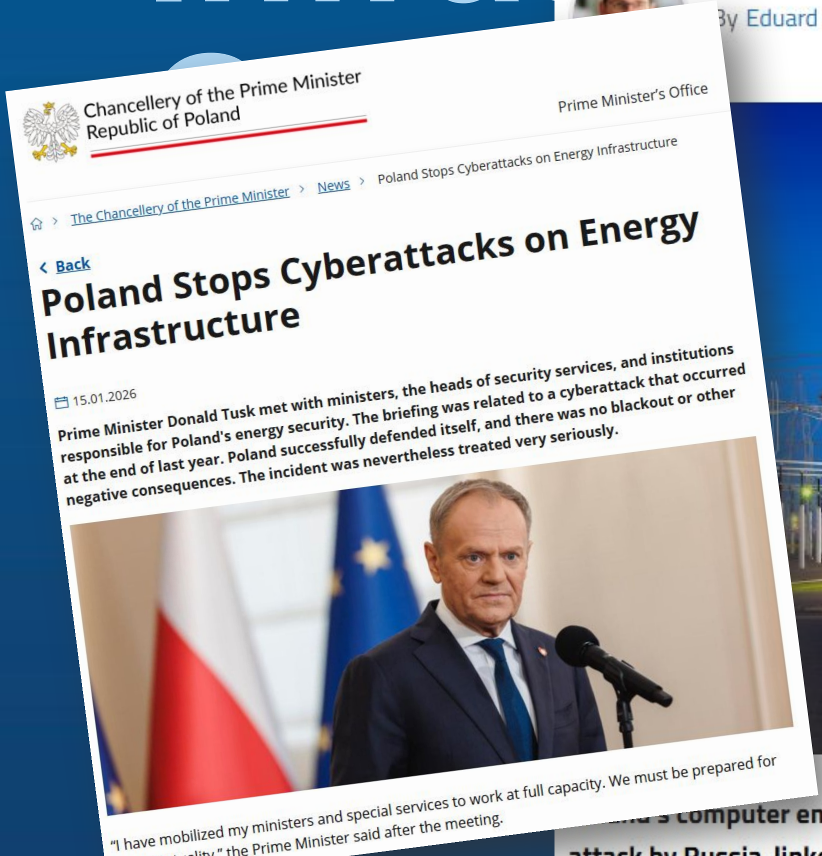
ICS/OT

Default ICS Credentials Exploited in Destructive Attack on Polish Energy Facilities

Poland's CERT has published a report on the recent attack, providing new details on targeted ICS and attribution.

By Eduard Kovacs | February 2, 2026 (8:50 AM ET)

...nd's computer emergency response team (CERT) has published a report detailing the recent attack by Russia-linked hackers on the country's power grid.



Chancellery of the Prime Minister
Republic of Poland

Prime Minister's Office

The Chancellery of the Prime Minister › News › Poland Stops Cyberattacks on Energy Infrastructure

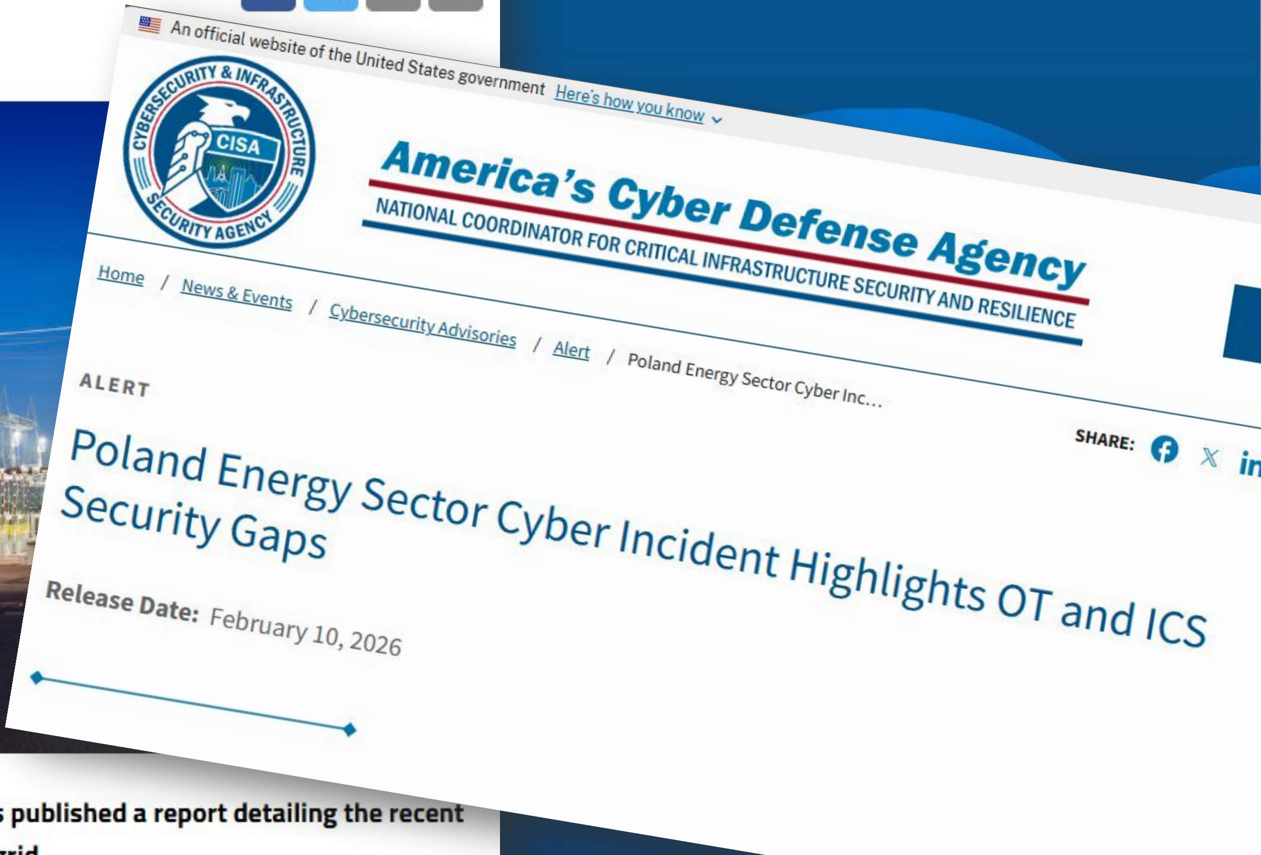
‹ Back

Poland Stops Cyberattacks on Energy Infrastructure

15.01.2026

Prime Minister Donald Tusk met with ministers, the heads of security services, and institutions responsible for Poland's energy security. The briefing was related to a cyberattack that occurred at the end of last year. Poland successfully defended itself, and there was no blackout or other negative consequences. The incident was nevertheless treated very seriously.

"I have mobilized my ministers and special services to work at full capacity. We must be prepared for ...ality," the Prime Minister said after the meeting.



An official website of the United States government Here's how you know

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Home / News & Events / Cybersecurity Advisories / Alert / Poland Energy Sector Cyber Inc...

ALERT

SHARE:

Poland Energy Sector Cyber Incident Highlights OT and ICS Security Gaps

Release Date: February 10, 2026

Defending Critical Infrastructure from Cyber Attacks

1 Intro to Operational Technology (OT)

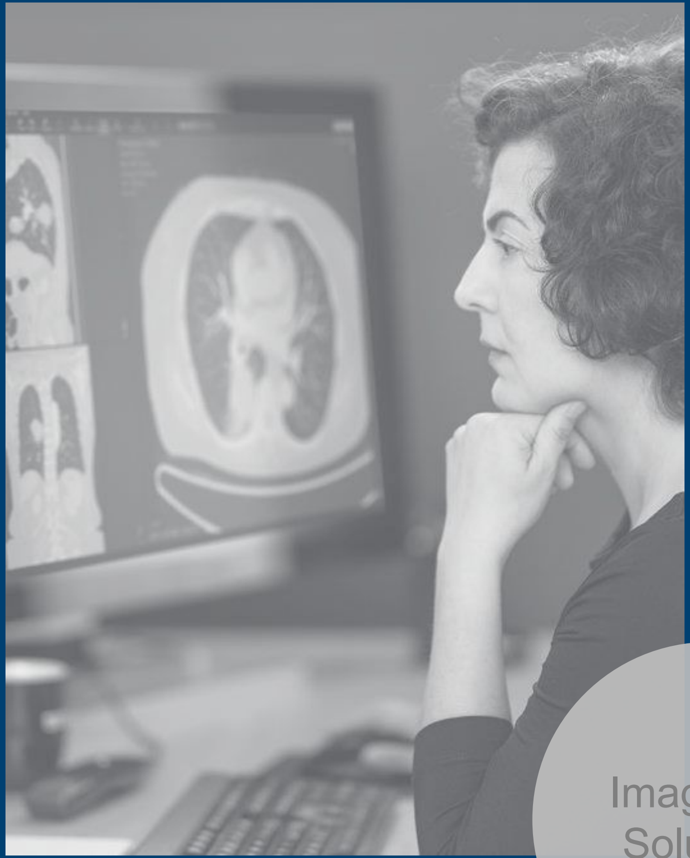
2 The December attacks in Poland

3 Key takeaways & why detection engineer matters

Joakim Elgh
Senior Detection Engineer
Sectra Critical Infrastructure

What we do at Sectra

Secure Communications



Imaging IT Solutions

SECTRA

This is what we do

Supporting society’s critical functions

Communication systems for National Security

High assurance up to NATO/EU SECRET

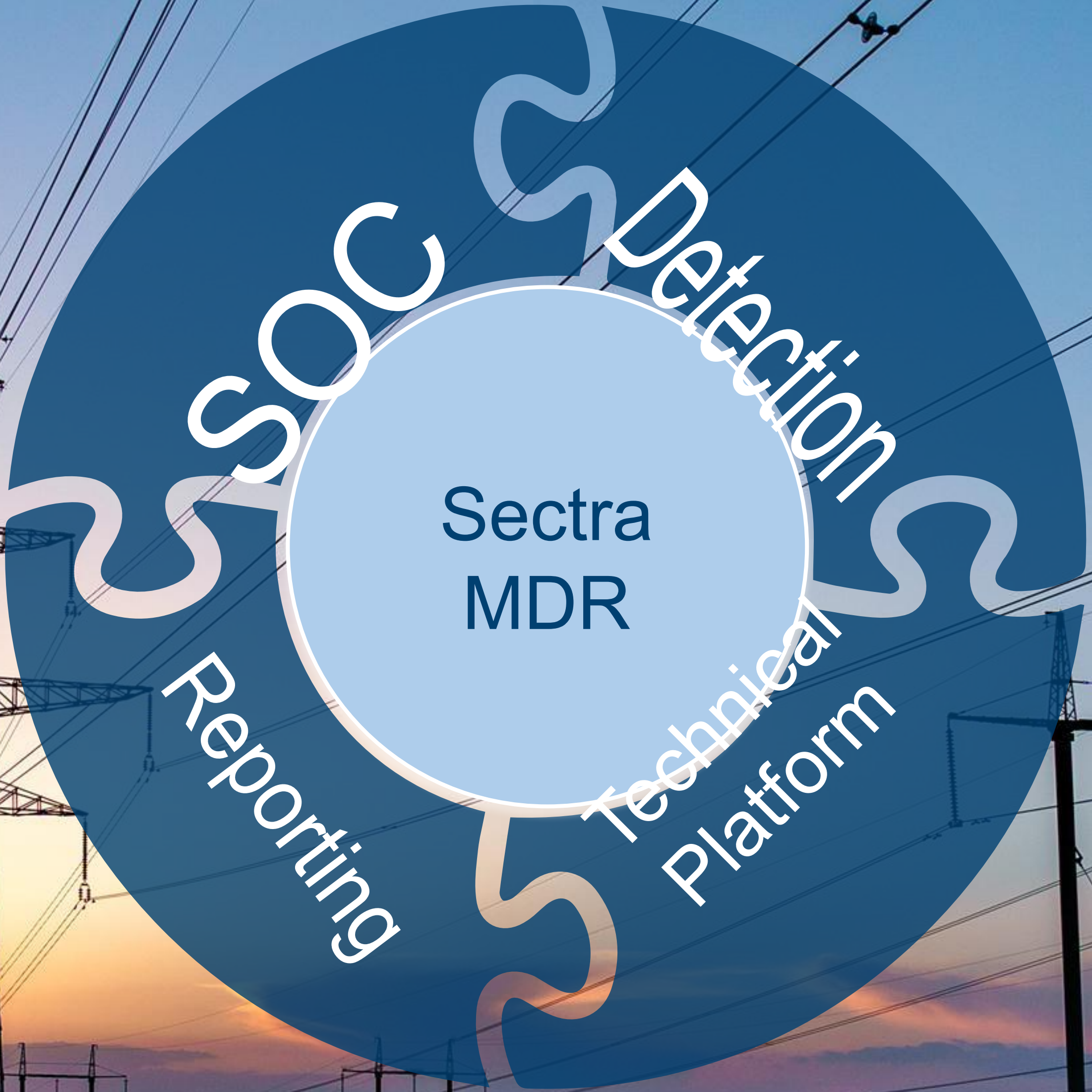
Mobile solutions for Civil Authorities and Enterprises

Secure remote information access for users handling sensitive information

Security solutions for Critical Infrastructure

Operational continuity for IT/OT

SECTRA



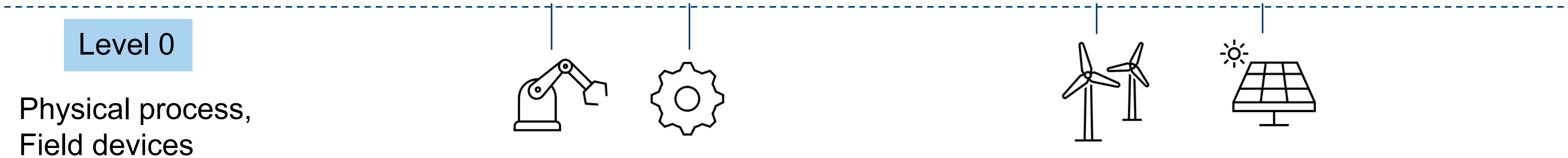
SECTRA

Intro to Operational Technology (OT systems)

SECTRA

Hierarchical visualization

Purdue model



Level 0

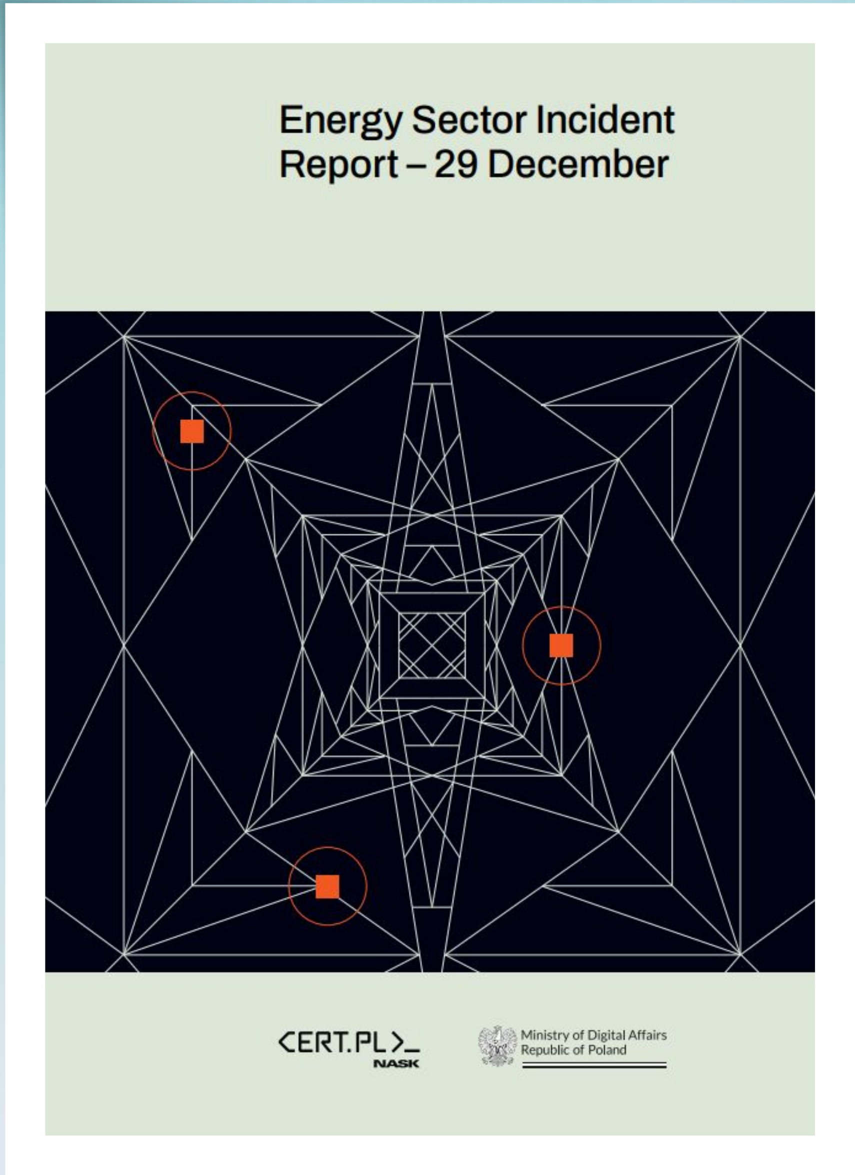
Physical process,
Field devices

Detection and Response challenges in OT

- Monitoring and the technical platform used should be tailored for OT environments
  - Low risk of performance issues,
  - Careful or no usage of automatic response – availability prioritized,
  - Acceptable by third party vendors

- Physical processes are involved – incident response must be careful
  - Response actions can have expensive or dangerous effects – Safety prioritized
  - This differs from IT – where isolation or account lockouts usually is done fast

The coordinated attacks on the electric system in Poland, Dec 29, 2025



Energy Sector Incident Report – 29 December

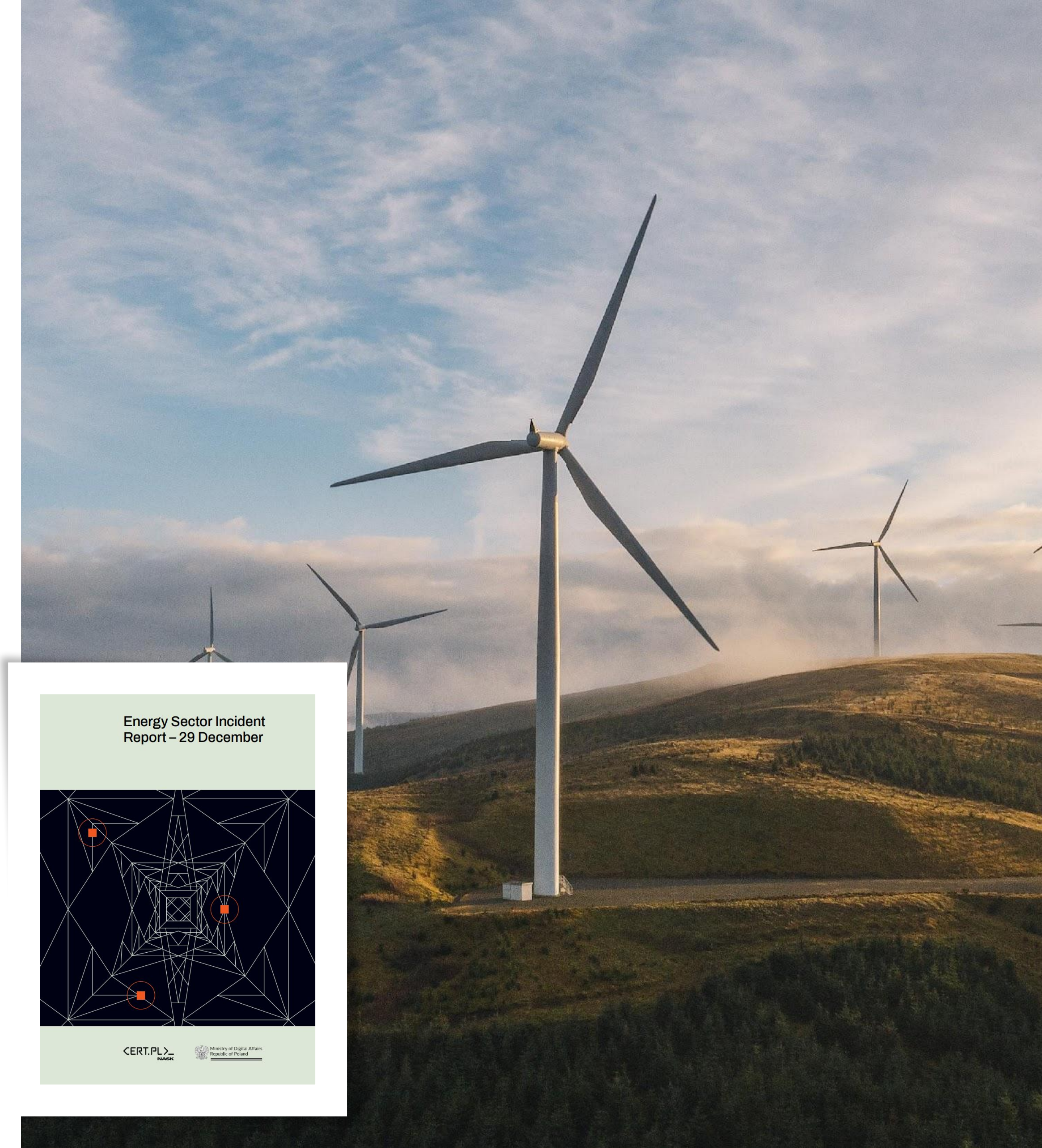
<CERT.PL>_
NASK

Ministry of Digital Affairs
Republic of Poland

https://cert.pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Report_2025.pdf

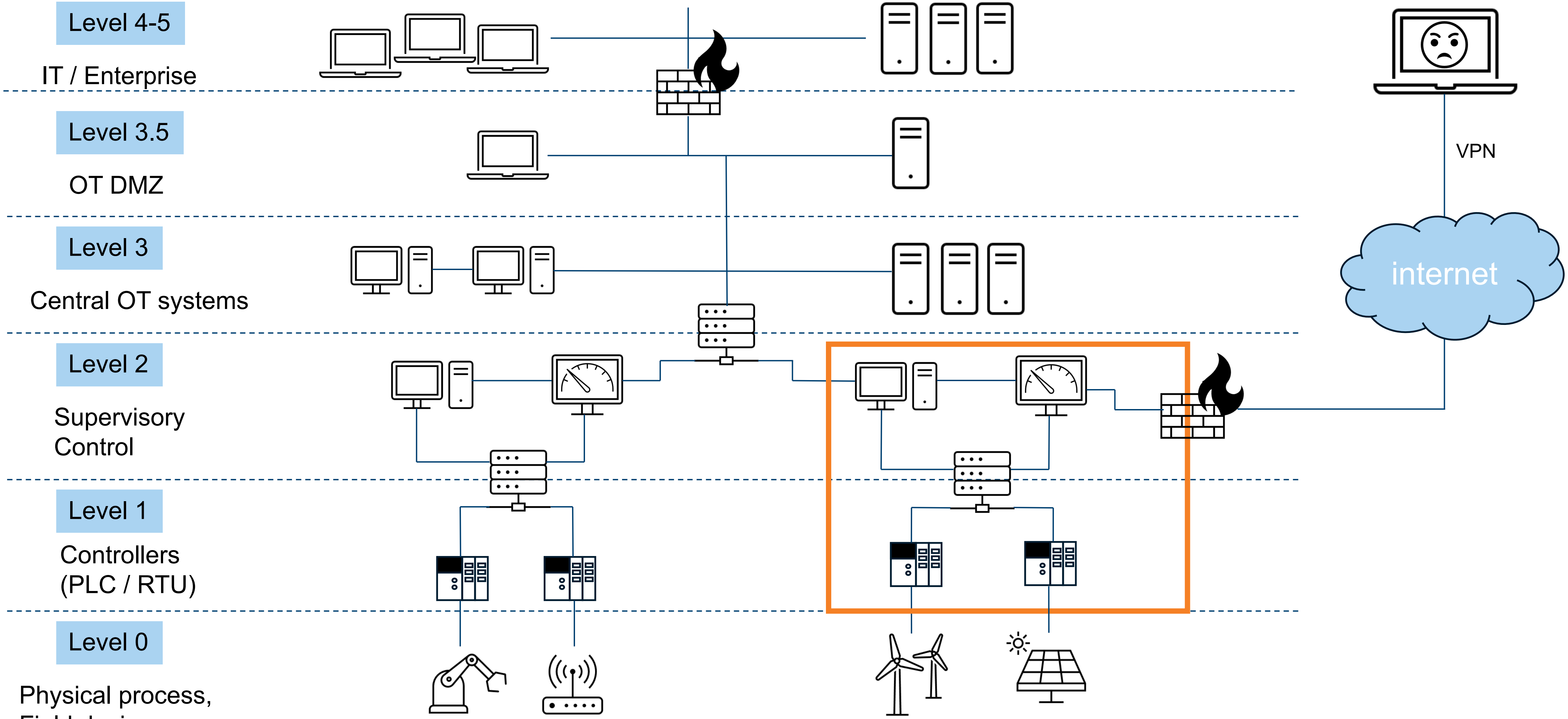
Poland Energy systems attack

- Several coordinated attacks
- >30 wind and solar farms
  - Destructive techniques against equipment in substations controlling the renewable energy farms
- A large combined heat and power plant
  - IT network infiltrated with information theft and attempt to use wiper malware
- A manufacturing sector company
  - PowerShell-based wiper



Energy Sector Incident Report – 29 December

Renewable energy farms, grid connection point (GCP) substations



Level 4-5

IT / Enterprise

Level 3.5

OT DMZ

Level 3

Central OT systems

Level 2

Supervisory Control

Level 1

Controllers (PLC / RTU)

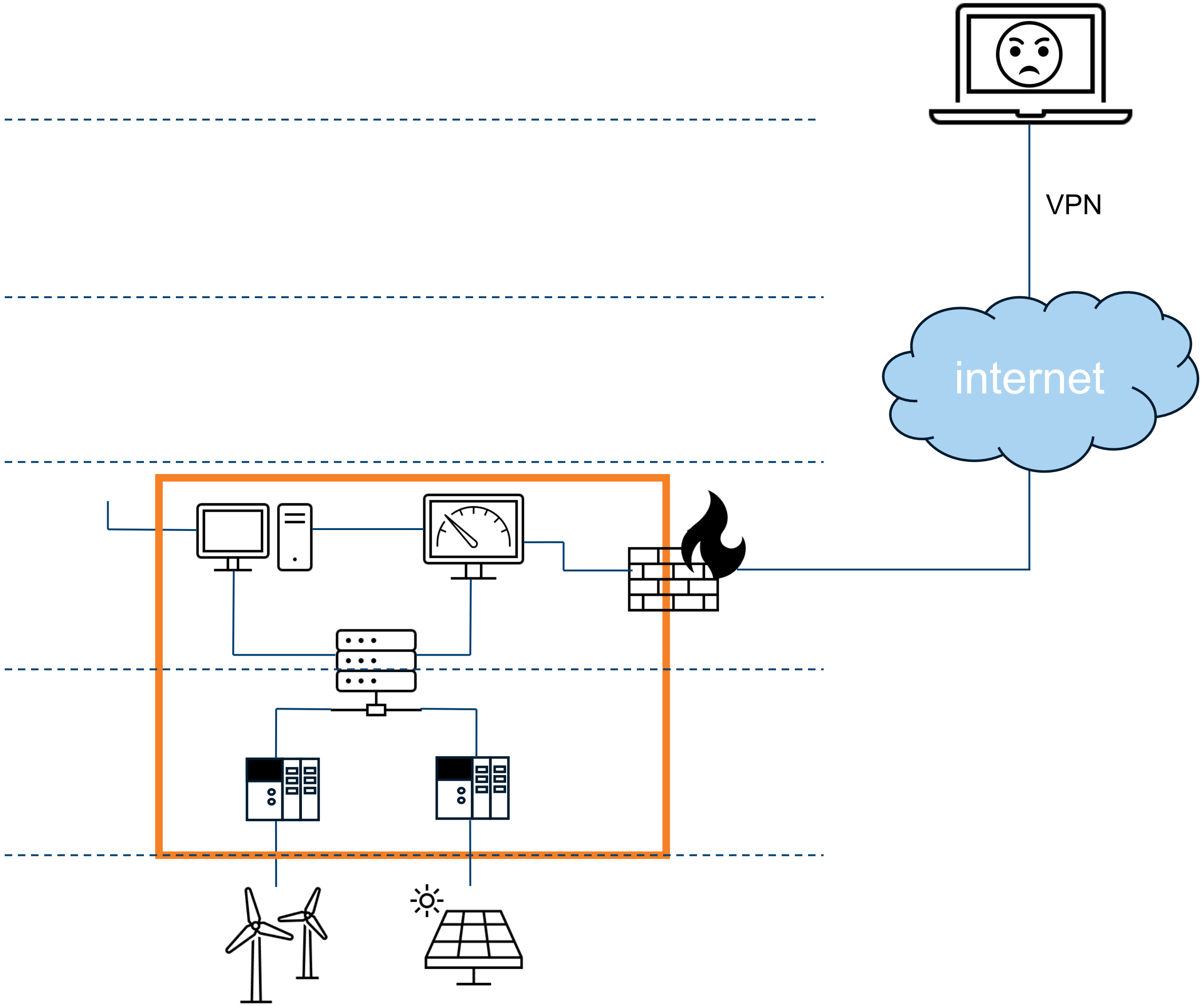
Level 0

Physical process, Field devices

SECTRA

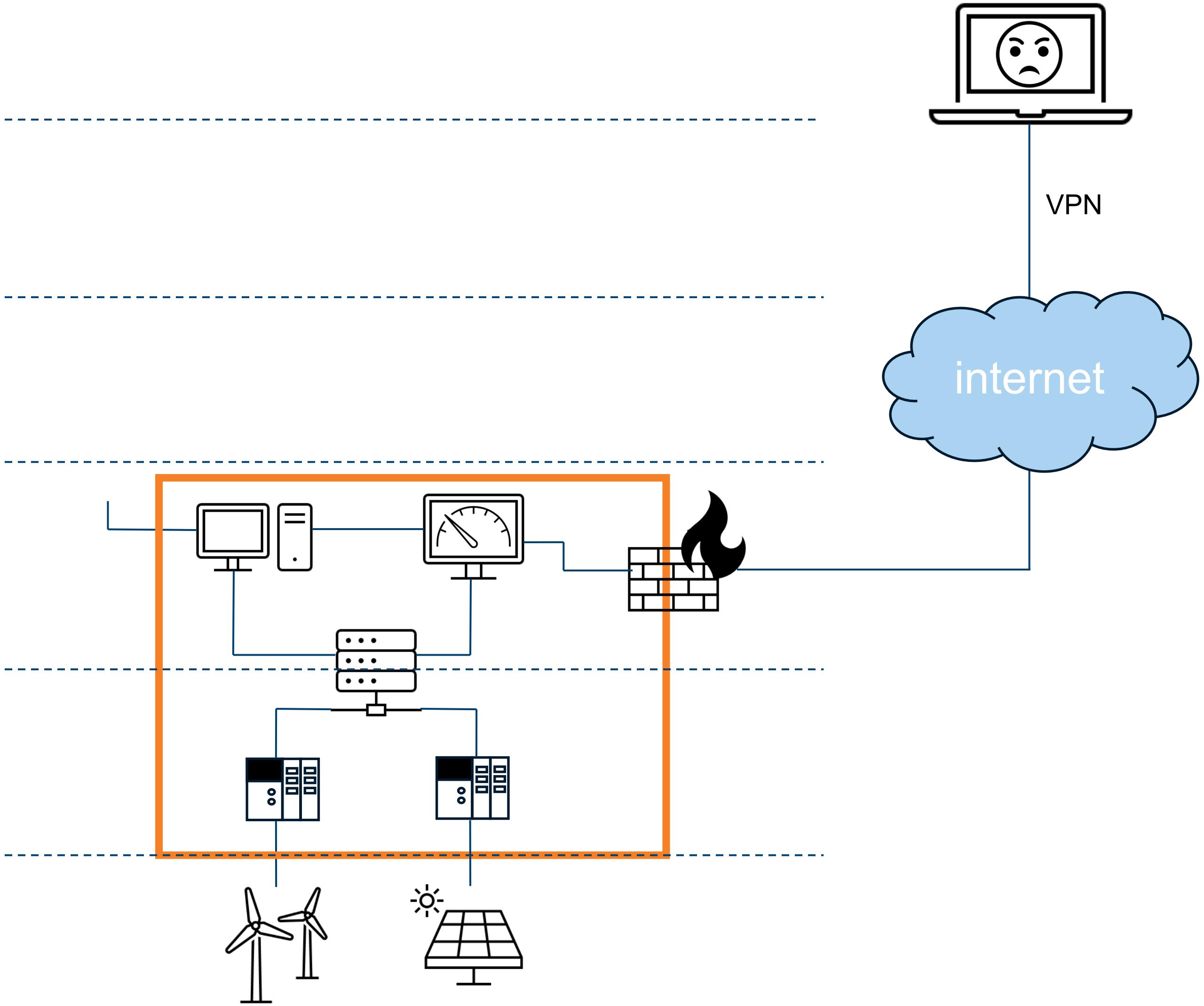
Renewable energy farms, grid connection point (GCP) substations

- Several reasons for success
- **Edge firewalls**
  - VPN exposed to internet and required no MFA
  - Likely vulnerable
  - Weak credentials



Renewable energy farms, grid connection point (GCP) substations

- Several reasons for success
- **Inside stations**
- Access to computers, software and devices through default credentials, then
  - Upload of corrupt firmware to RTU:s
  - Deleted system files on RTU:s
  - Disabled IED:s (Intelligent Electronic Devices)
  - Factory-reset serial servers
  - Wipers on Windows HMI hosts

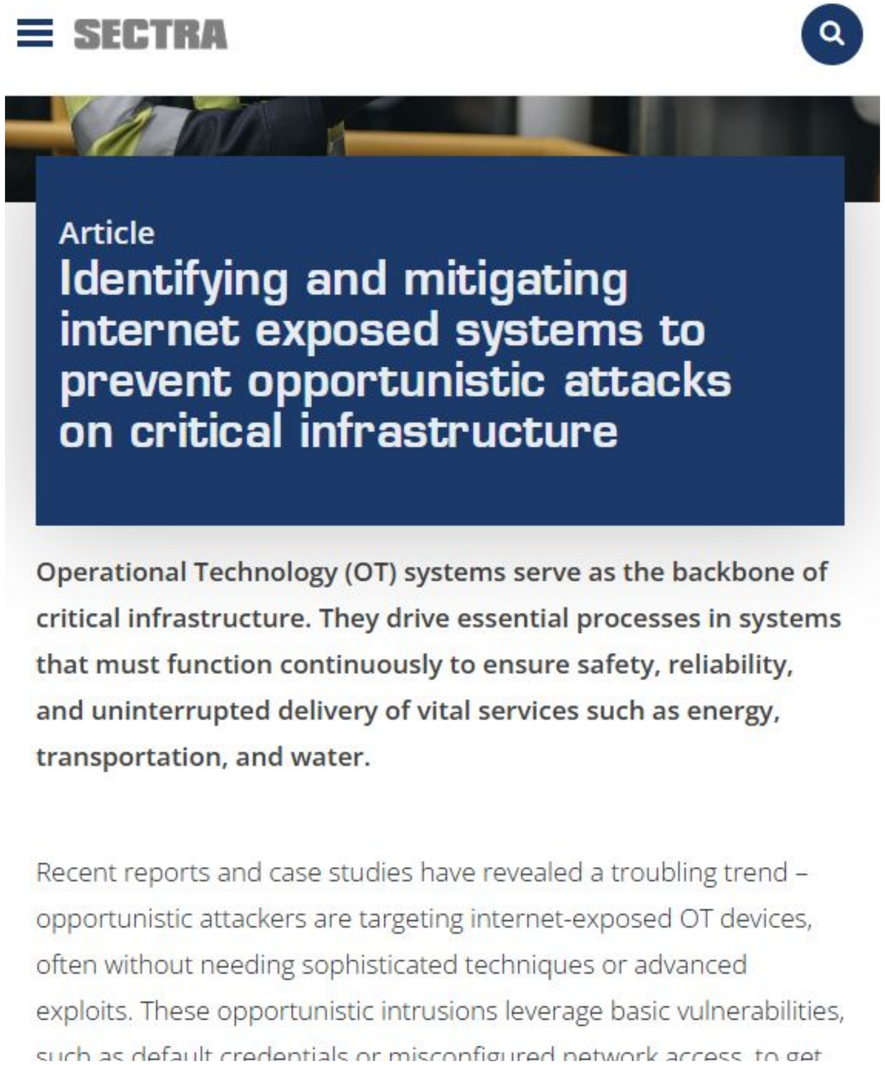


SECTRA

Key takeaways and how to detect future attacks

Recommendations to mitigate similar attacks

- An extreme example
  - But this is what many OT attacks currently look like
- OT assets should not be accessible from the internet
  - Even though there was segmentation, attackers got access directly to all the network segments
- Default credentials must be changed and stored securely
  - Very common, credentials can often be found unsecured in logs and command history
- MFA for VPN or non-VPN-based remote access solutions



Article

Identifying and mitigating internet exposed systems to prevent opportunistic attacks on critical infrastructure

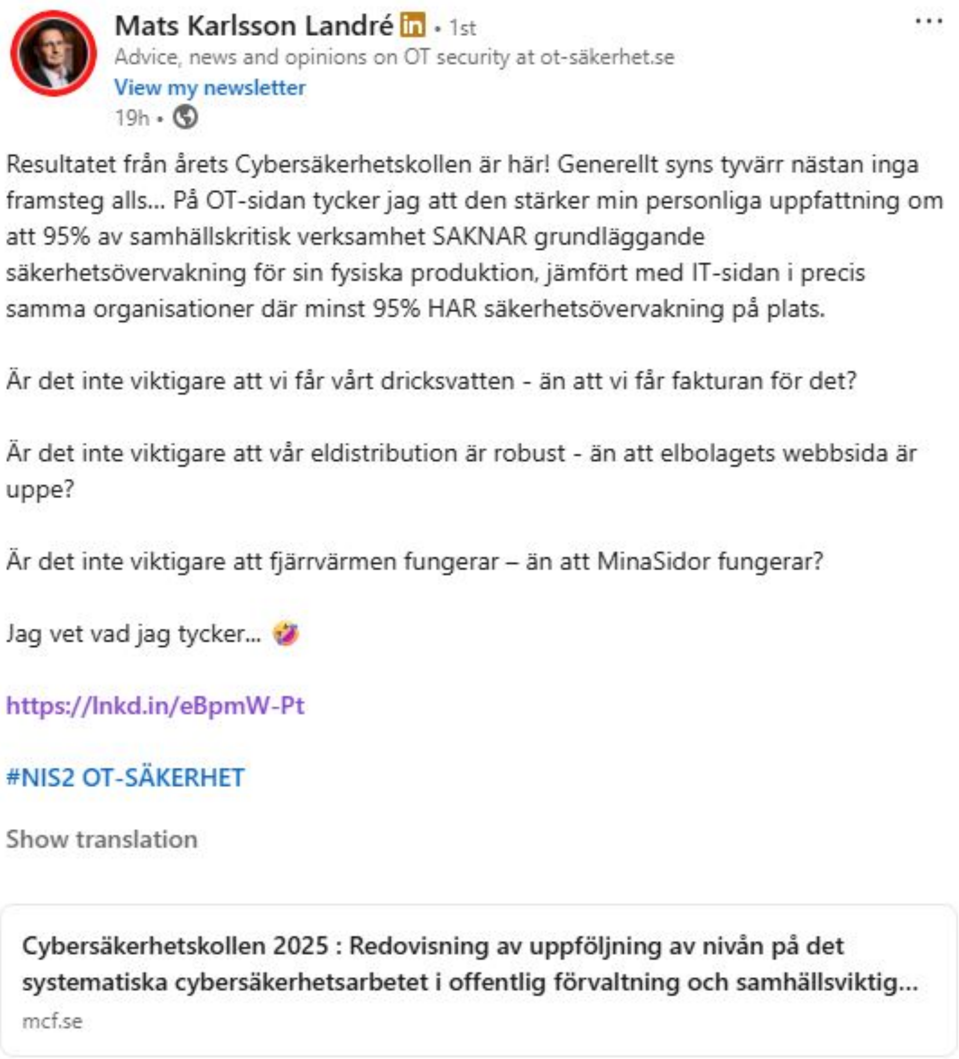
Operational Technology (OT) systems serve as the backbone of critical infrastructure. They drive essential processes in systems that must function continuously to ensure safety, reliability, and uninterrupted delivery of vital services such as energy, transportation, and water.

Recent reports and case studies have revealed a troubling trend – opportunistic attackers are targeting internet-exposed OT devices, often without needing sophisticated techniques or advanced exploits. These opportunistic intrusions leverage basic vulnerabilities, such as default credentials or misconfigured network access, to get

https://communications.sectra.com/resources/identifying-and-mitigating-internet-exposed-systems/

How detection engineering helps

- Not all steps could be explained due to missing logs
- Detection Engineering
  - Making sure we get visibility and detection capability
- Identify relevant logs to collect in advance
  - Export to a centralized storage
- Collect several examples of attacks towards systems like yours
  - Use this to know the most likely attack techniques for prioritization



Mats Karlsson Landré • 1st

Advice, news and opinions on OT security at ot-säkerhet.se

View my newsletter

19h •

Resultatet från årets Cybersäkerhetskollen är här! Generellt syns tyvärr nästan inga framsteg alls... På OT-sidan tycker jag att den stärker min personliga uppfattning om att 95% av samhällskritisk verksamhet SAKNAR grundläggande säkerhetsövervakning för sin fysiska produktion, jämfört med IT-sidan i precis samma organisationer där minst 95% HAR säkerhetsövervakning på plats.

Är det inte viktigare att vi får vårt dricksvatten - än att vi får fakturan för det?

Är det inte viktigare att vår eldistribution är robust - än att elbolagets webbsida är uppe?

Är det inte viktigare att fjärrvärmen fungerar – än att MinaSidor fungerar?

Jag vet vad jag tycker...

https://lnkd.in/eBpmW-Pt

#NIS2 OT-SÄKERHET

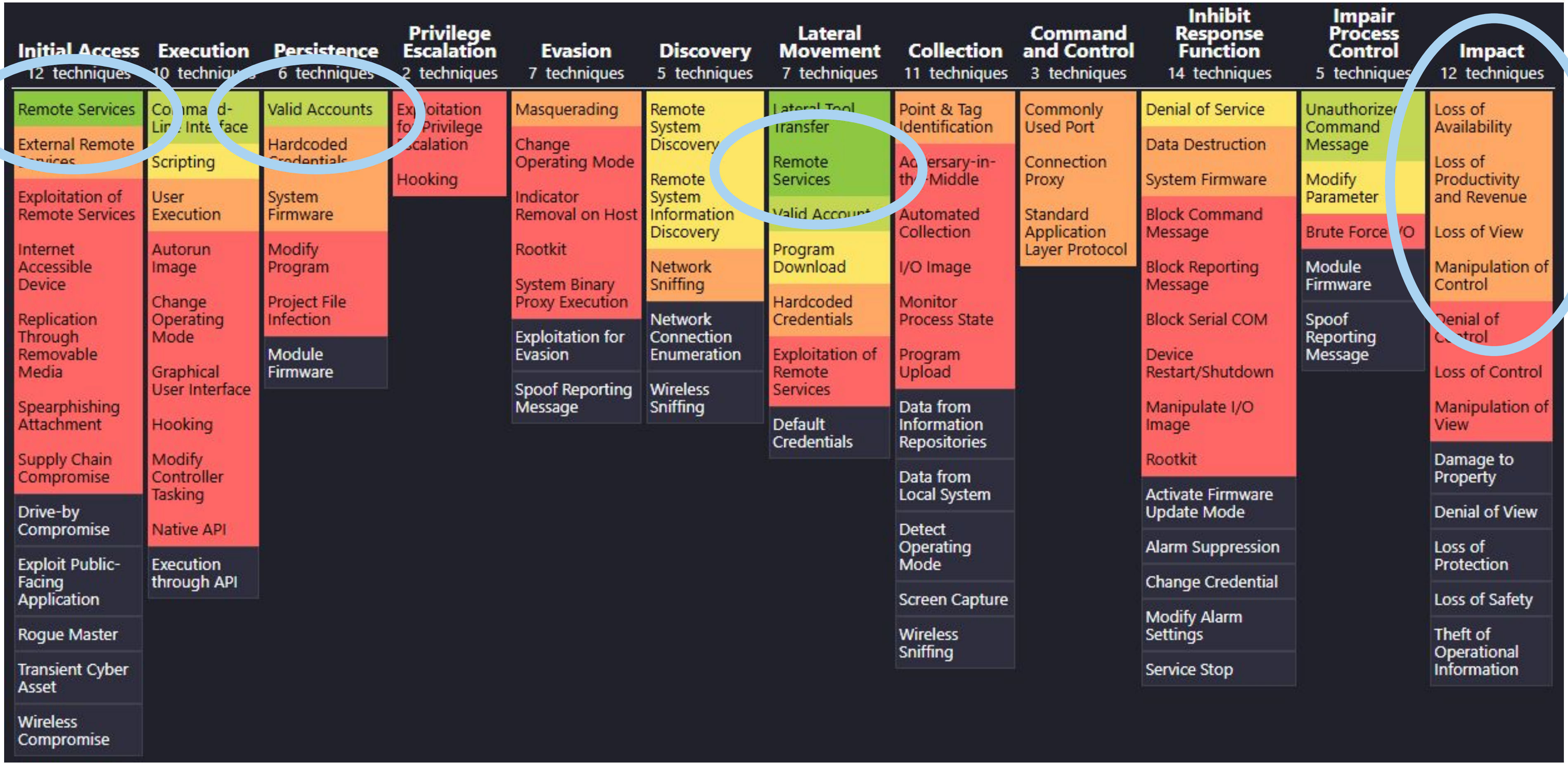
Show translation

Cybersäkerhetskollen 2025 : Redovisning av uppföljning av nivån på det systematiska cybersäkerhetsarbetet i offentlig förvaltning och samhällsviktig...

mcf.se

SECTRA

Summarize relevant attack scenarios with MITRE ATT&CK

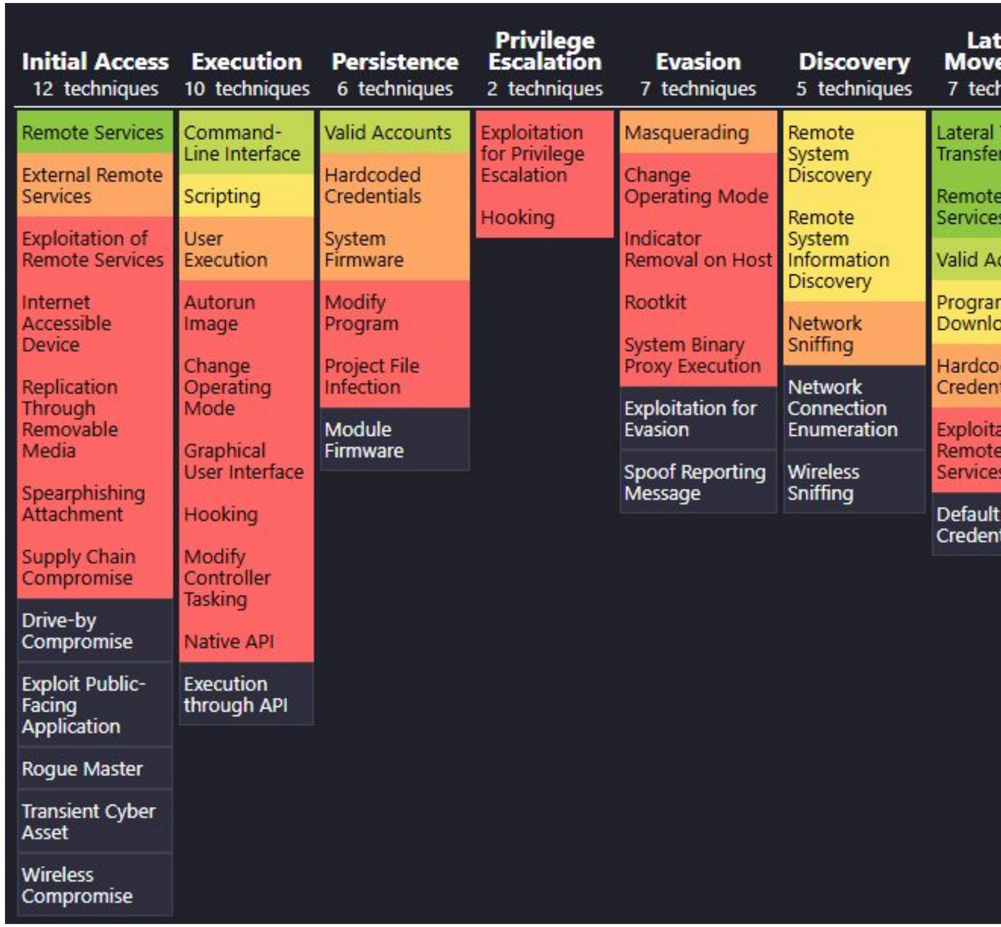


Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14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

Continuous security work is important

- We can identify which logs are most important to collect right now
  - Also make sure to have detection methods doing something useful with them!

- Continuous work with improving security makes it harder for attackers
  - They need to try and succeed with more attack techniques to reach their goals
  - We get more opportunities to discover them in time



Initial Access 12 techniques	Execution 10 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 7 techniques	Discovery 5 techniques	Lat Move 7 tech
Remote Services	Command-Line Interface	Valid Accounts	Exploitation for Privilege Escalation	Masquerading	Remote System Discovery	Lateral Transfe
External Remote Services	Scripting	Hardcoded Credentials	Hooking	Change Operating Mode	Remote System Information Discovery	Remote Services
Exploitation of Remote Services	User Execution	System Firmware		Indicator Removal on Host	Network Sniffing	Valid Ac
Internet Accessible Device	Autorun Image	Modify Program		Rootkit	Network Connection Enumeration	Progra Downlo
Replication Through Removable Media	Change Operating Mode	Project File Infection		System Binary Proxy Execution	Wireless Sniffing	Hardco Creden
Spearphishing Attachment	Graphical User Interface	Module Firmware		Exploitation for Evasion		Exploita Remote Service
Supply Chain Compromise	Hooking			Spoof Reporting Message		Default Creden
Drive-by Compromise	Modify Controller Tasking					
Exploit Public-Facing Application	Native API					
Rogue Master	Execution through API					
Transient Cyber Asset						
Wireless Compromise						

Summary

- OT systems can be thought of as several layers
  - From IT enterprise systems at the top, to industrial controllers steering physical processes at the lowest level
- The Poland Energy Systems attack
  - Where advanced attackers took advantage of critical infrastructure with lower security measures
- We can get very far with “basic” security recommendations
  - Make sure to understand what your network look like,
  - And look at different attack scenarios to help prioritize how to protect your systems!

SECTRA

Knowledge and passion