WEBINAR

POWERED BY
pv magazine

pv magazine
WEBINARS

29 April 2026

2:00 pm – 3:30 pm BST, London
3:00 pm – 4:30 pm CEST, Berlin
9:00 am – 10:30 am EDT, New York City

Decoding the first massive cyberattack on Europe’s solar energy infrastructure - The Poland case and lessons learned

Emiliano Bellini

News Director

pv magazine

pv magazine WEBINARS

Do you have any questions? ❓ 🙋
Ask them via the Q&A tab. 👉 We will try to answer as many as possible!

Who else is here?
Use the open chat to discuss with other participants.

We are recording this webinar today. 📹
We will email you where to find the recording and slides, so you can watch them again at your leisure. 👀 💡

WEBINAR

POWERED BY
pv magazine

pv magazine
WEBINARS

Decoding the first massive cyberattack on Europe’s solar energy infrastructure - The Poland case and lessons learned

29 April 2026

2:00 pm – 3:30 pm BST, London
3:00 pm – 4:30 pm CEST, Berlin
9:00 am – 10:30 am EDT, New York City

Emiliano Bellini
News Director
pv magazine

Marian Willuhn
Senior Editor
pv magazine

WEBINAR

POWERED BY
pv magazine

pv magazine
WEBINARS

Decoding the first massive cyberattack on Europe’s solar energy infrastructure - The Poland case and lessons learned

29 April 2026

2:00 pm – 3:30 pm BST, London
3:00 pm – 4:30 pm CEST, Berlin
9:00 am – 10:30 am EDT, New York City

Emiliano Bellini
News Director
pv magazine

Daniel dos Santos
VP Research
Forescout Technologies

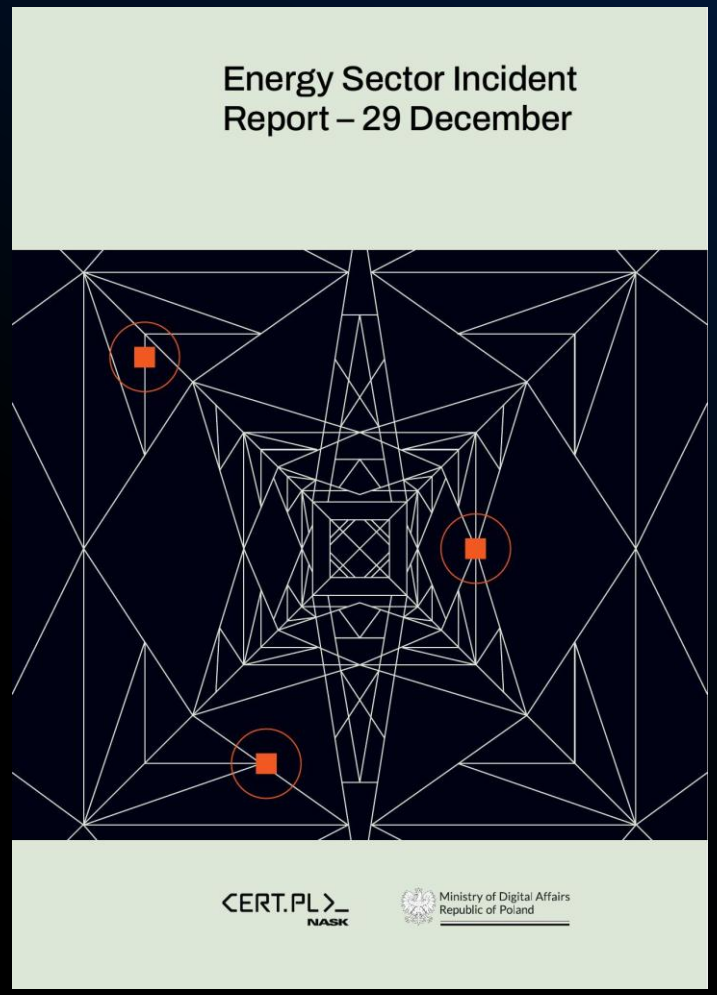
FORESCOUT

THREAT LANDSCAPE FOR SOLAR ENERGY

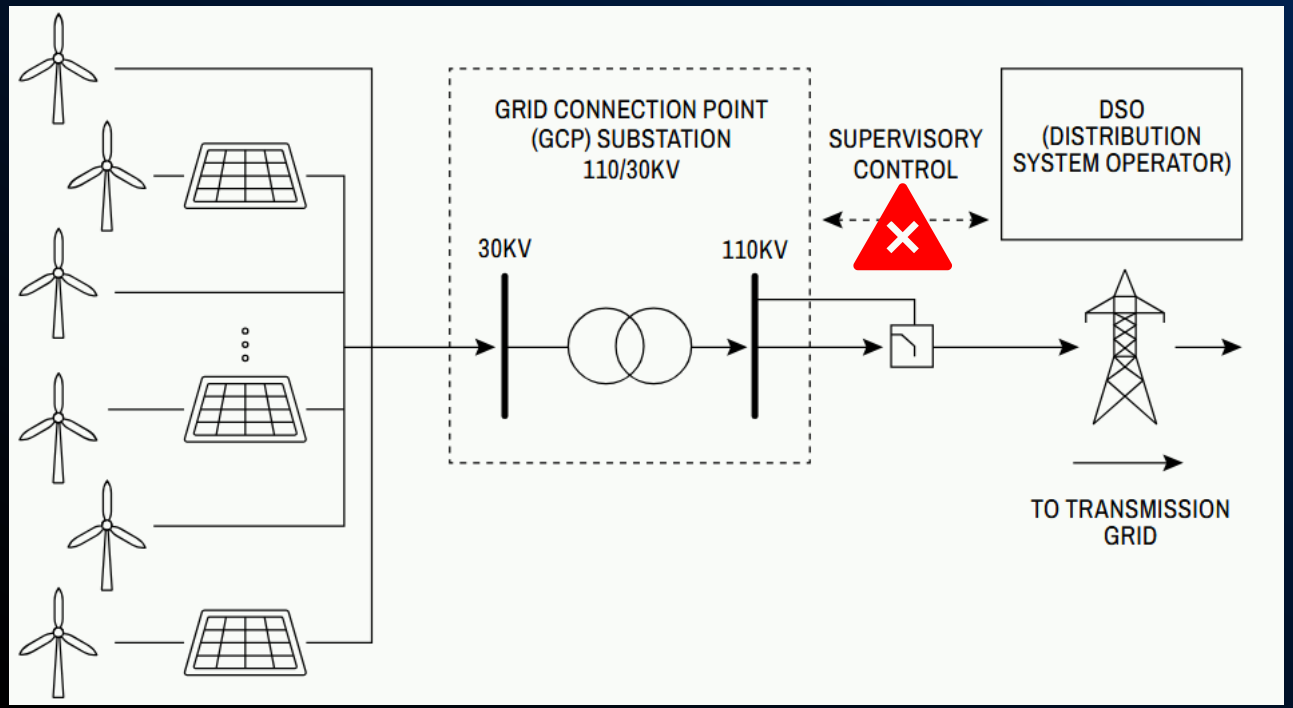
Poland Cyber Incident and Beyond

Daniel dos Santos, PhD
VP, Research

Cyber Incident in Poland



- Attack attributed to Russia's Berserk Bear against Polish Distributed Energy Resources (DER) at the end of 2025
- Goal: cut the communication between substations and supervisory control



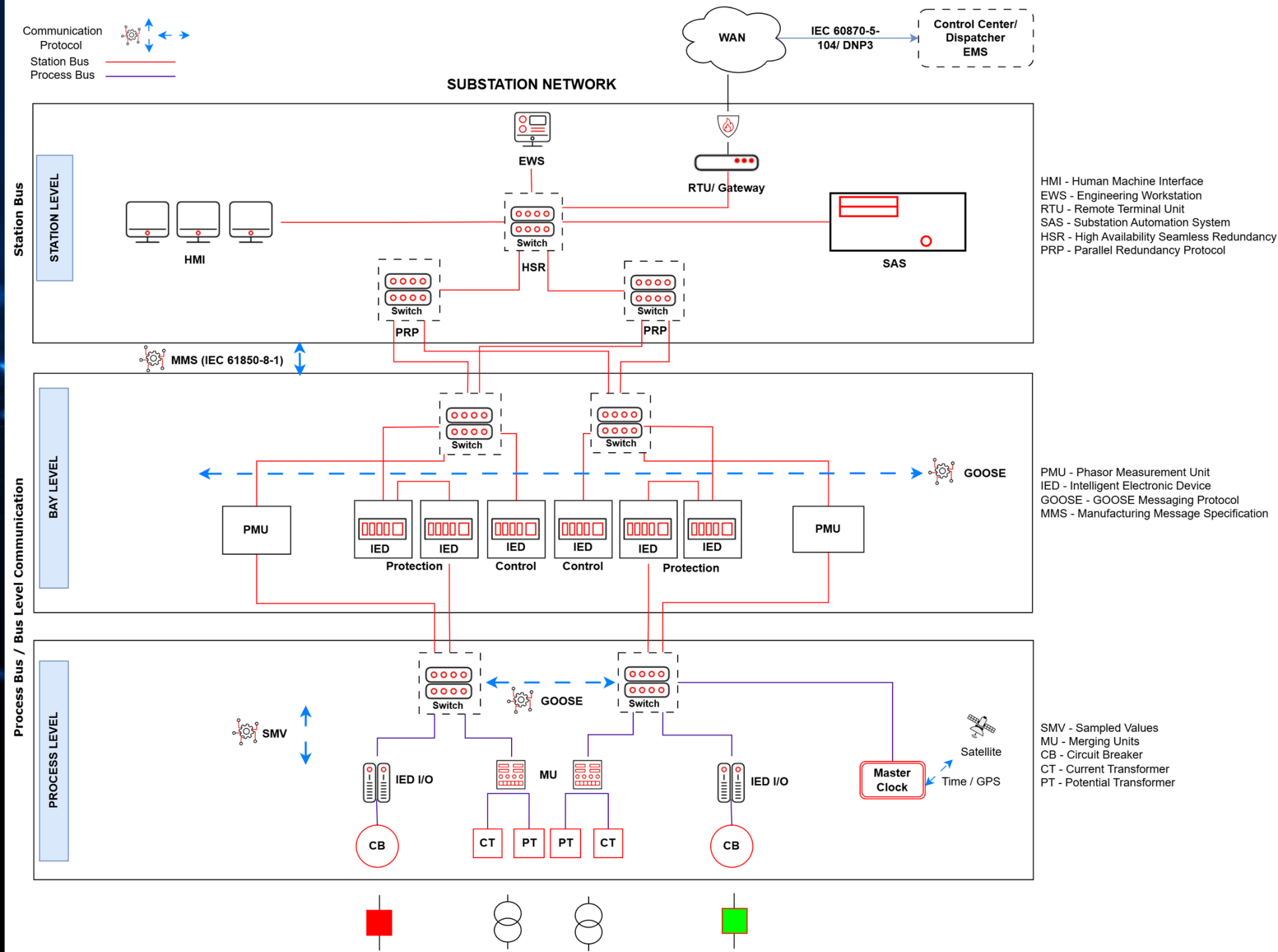
What a substation looks like

It's not simple…

… lots of devices

… lots of protocols

… lots of entry points

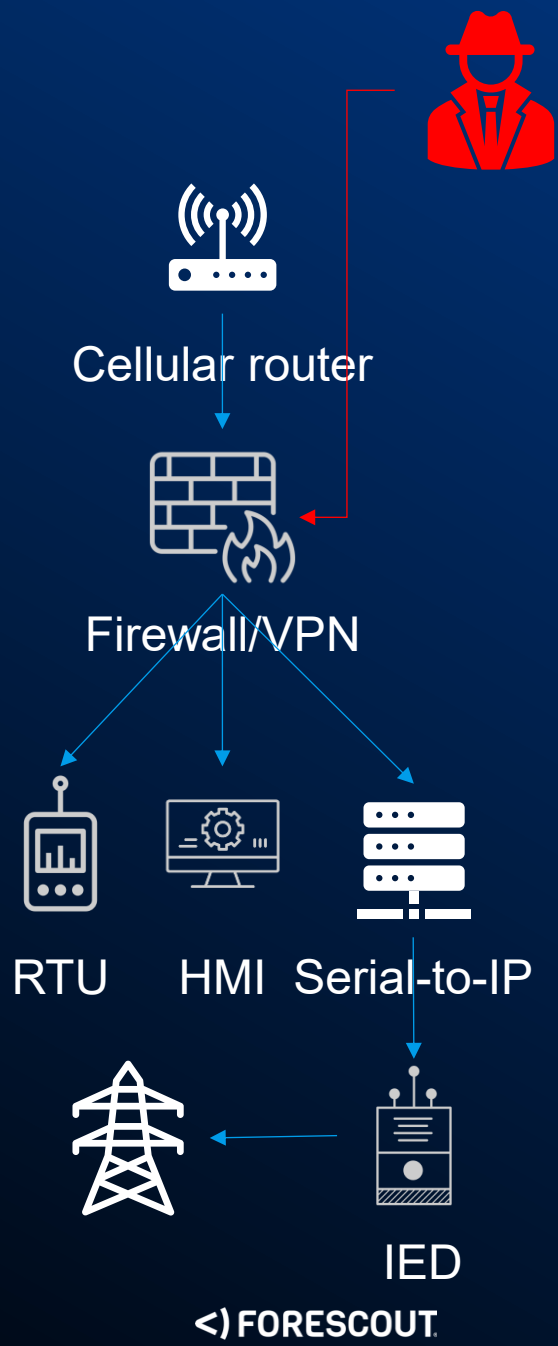


Source: https://cloud.google.com/blog/topics/threat-intelligence/securing-protection-relays-modern-substations

Assets Involved In This Attack

- The attacker just needs to find one way in and attack the devices of interest

Asset	Description
Cellular router	Connect to central SCADA via DNP3 or IEC-101
VPN/firewall edge device	Provide remote access and network segmentation
Remote Terminal Units (RTUs)	Remote monitoring and control for substation
Local Human Machine Interface (HMI)	View operational data based on RTU input data
Serial-to-IP converters (“device servers”)	Connect RS-232/485 devices to IP network
Protection relays / IEDs	Physical protection functions such as fault detection and isolation

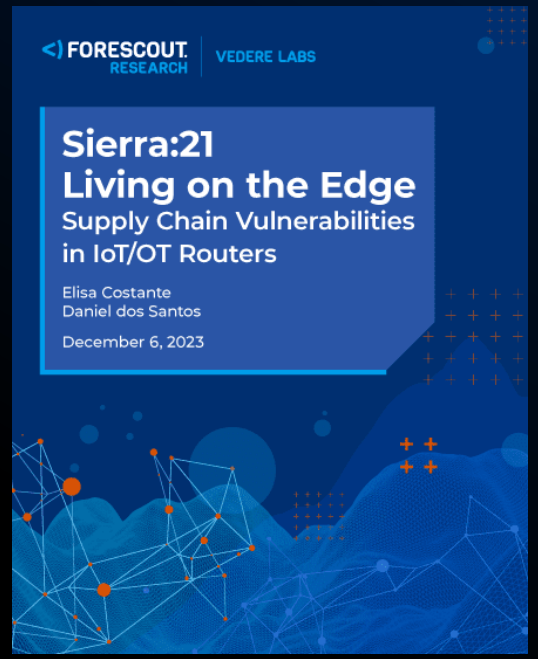


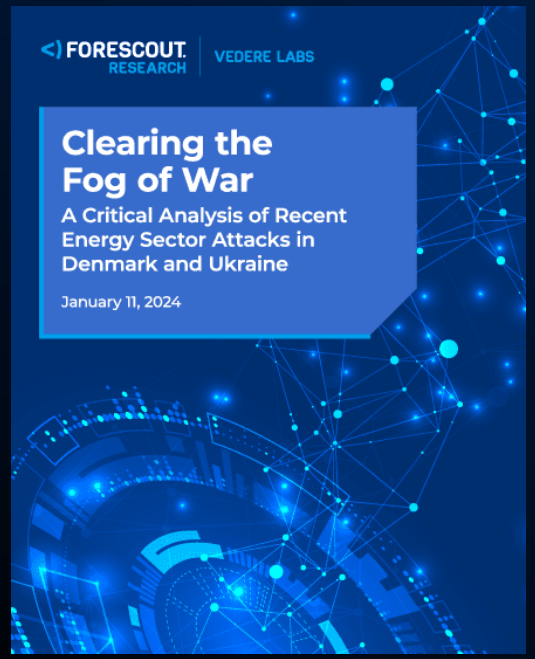
Attack Details

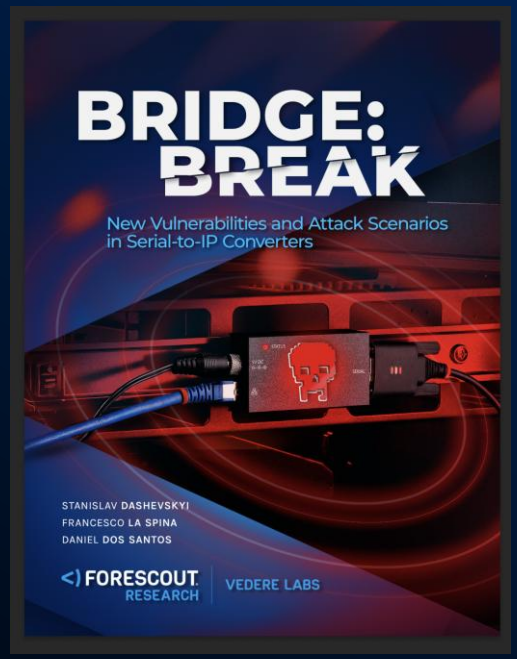
Asset	Entry point	Action
FortiGate VPN/firewall	Uncertain: known credentials or vulnerability exploit	• Recon via configuration files • Configuration changes for persistence • Lateral movement to rest of the network • Destruction: Factory reset
Hitachi RTUs	Default credentials (HTTP)	• Destruction: Upload corrupted firmware
Mikronika RTUs	Default credentials (SSH)	• Destruction: Delete all files on system
Hitachi IED relays	Default credentials (FTP)	• Destruction: Delete essential files
Mikronika HMIs	Valid credentials (Windows/RDP)	• Configuration changes • Network recon • Destruction: Deploy wiper
Moxa Nport serial-to-IP	Default credentials (HTTP)	• Destruction: Factory reset

Beyond Poland

Other relevant assets and what could have happened







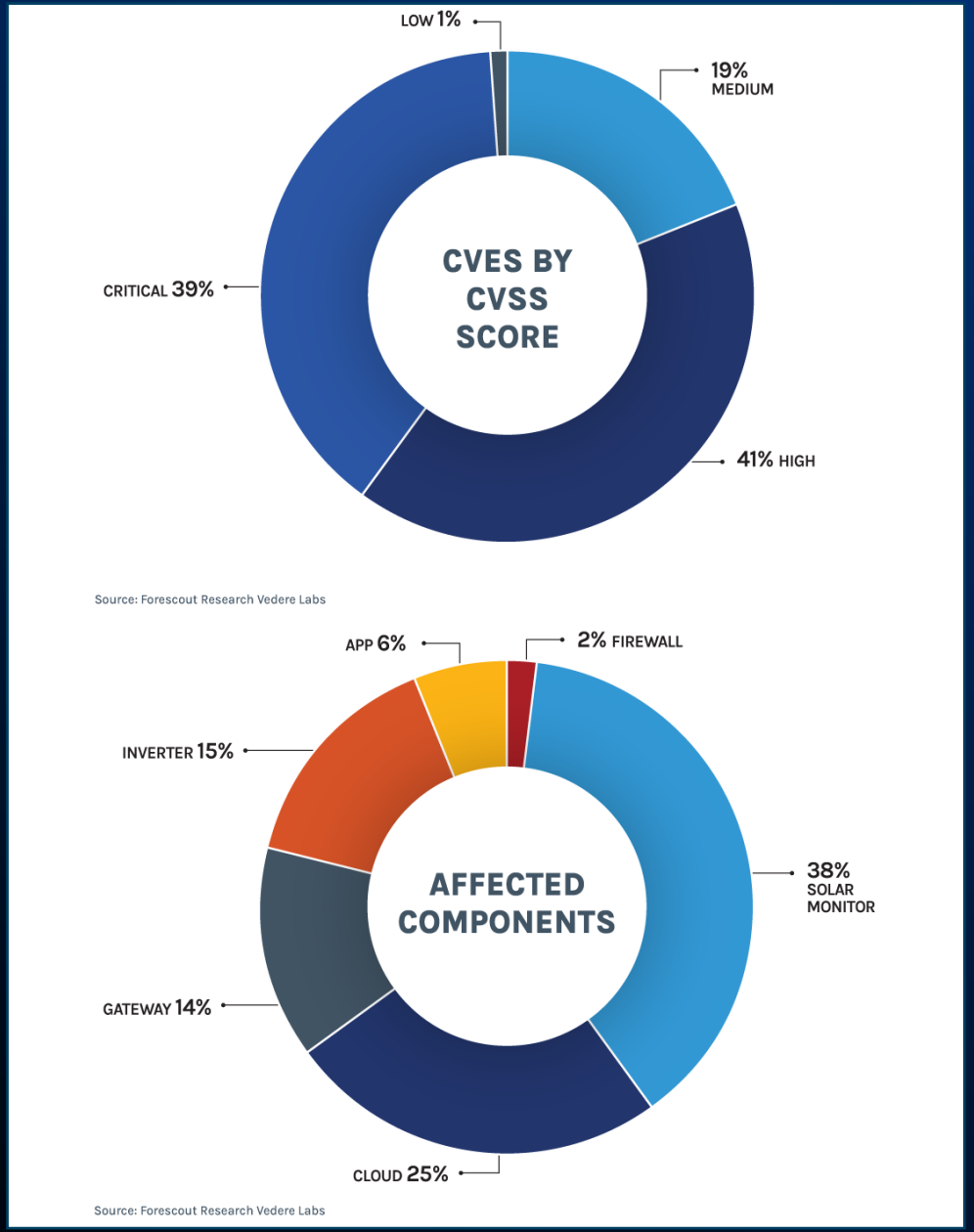
- 2023: Cellular routers have multiple vulnerabilities and are often unpatched
- 2024: Firewalls in substations can be quickly exploited by botnets once a vulnerability is published
- **2025: Solar inverters are notoriously weak and orchestrated exploits can lead to grid disruption**
- **2026: Serial-to-IP converters are critical in substations and have been attacked multiple times**

Solar Inverters: Vulnerabilities

- Cataloged **93 previous vulnerabilities affecting 34 vendors**
  - CVEs since 2012, average of 10/year for the past 3 years
  - 80% high or critical CVSS
  - Most cases affected solar monitoring/cloud products
  - Relatively few issues found directly on the inverters
- Six vulnerabilities **regularly exploited by botnets since 2022**

Product	CVEs
CONTEC SolarView	CVE-2022-29303 CVE-2022-40881 CVE-2023-23333 CVE-2023-29919
APsytems	CVE-2023-28343
Altenergy	CVE-2024-11305

- **Our own research identified 46 new vulnerabilities**

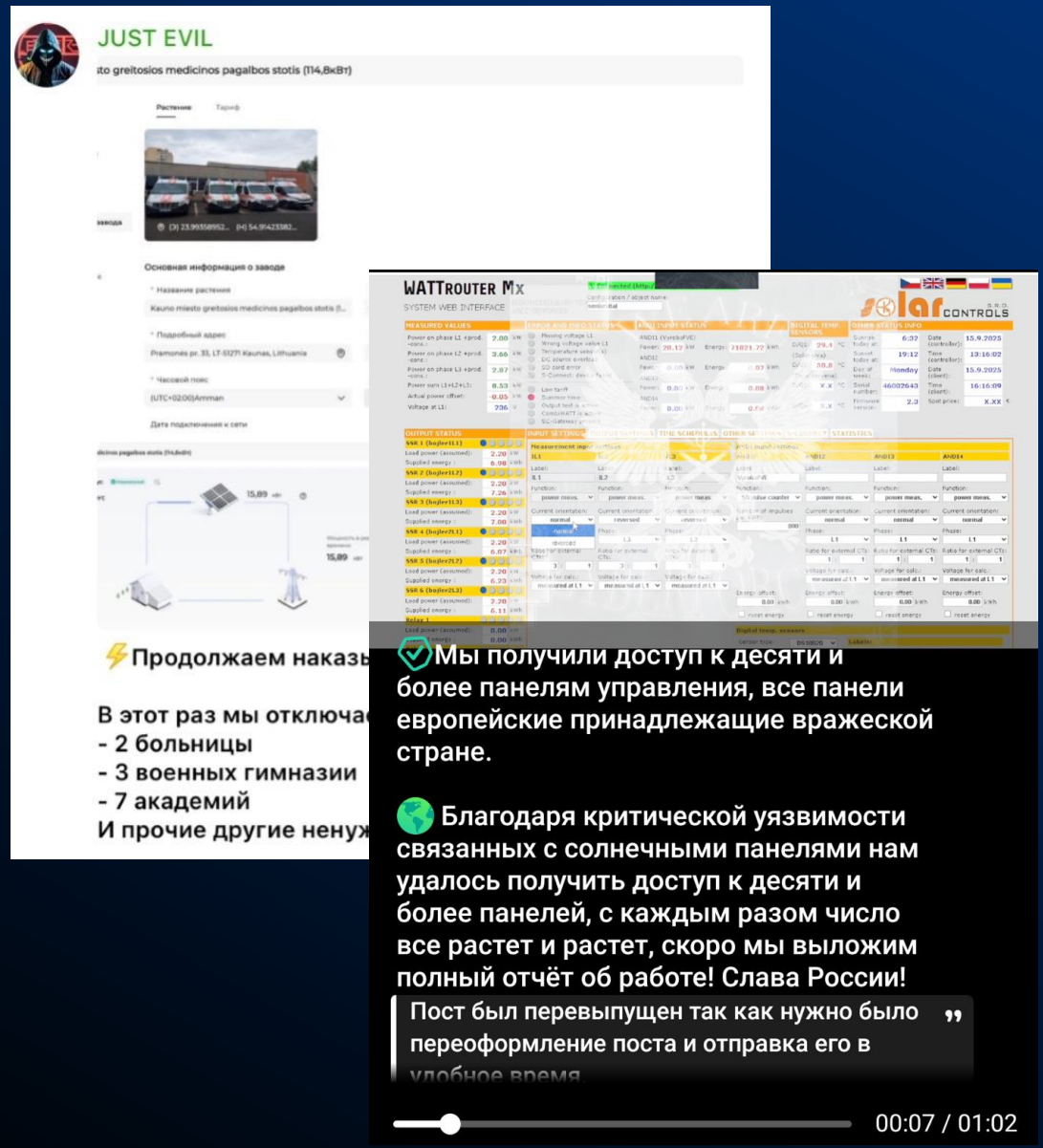


Solar Inverters: Incidents

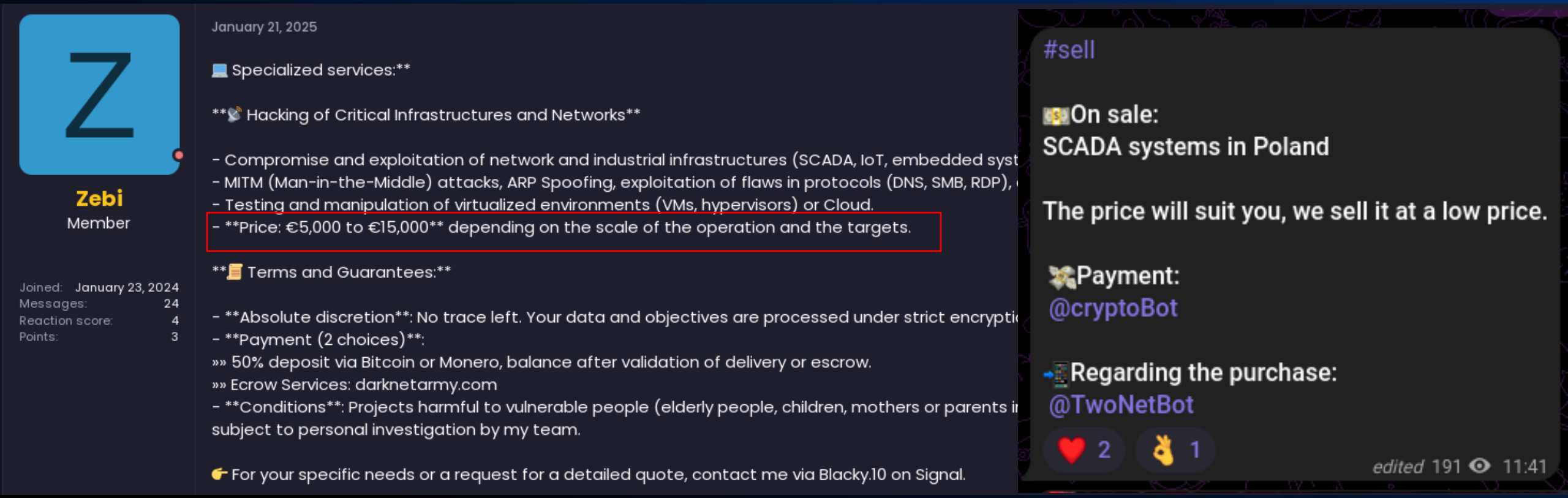
- **Poland was the first state-sponsored attack against DER, but…**

- **Three relevant incidents in 2024**
  - **Lithuania**: Pro-Russian hacktivists hijacked inverters in 22 organizations, including 2 hospitals via iSolarCloud management
  - **Japan**: 800 SolarView Compact monitoring devices hijacked by botnets
  - **US**: Flax Typhoon APT building botnets used to proxy further attacks. Exploited CVEs include two on SolarView Compact

- **Lots of hacktivist activity in 2025 and 2026**
  - More to come…



Looking Ahead:
Hack For Hire And IABs for Critical Infrastructure



Z

Zebi
Member

Joined: January 23, 2024
Messages: 24
Reaction score: 4
Points: 3

January 21, 2025

💻 Specialized services:**

🛰️ Hacking of Critical Infrastructures and Networks

- Compromise and exploitation of network and industrial infrastructures (SCADA, IoT, embedded syst
- MITM (Man-in-the-Middle) attacks, ARP Spoofing, exploitation of flaws in protocols (DNS, SMB, RDP),
- Testing and manipulation of virtualized environments (VMs, hypervisors) or Cloud.
- **Price: €5,000 to €15,000** depending on the scale of the operation and the targets.

📜 Terms and Guarantees:

- **Absolute discretion**: No trace left. Your data and objectives are processed under strict encrypti
- **Payment (2 choices)**:
»» 50% deposit via Bitcoin or Monero, balance after validation of delivery or escrow.
»» Ecrow Services: darknetarmy.com
- **Conditions**: Projects harmful to vulnerable people (elderly people, children, mothers or parents i
subject to personal investigation by my team.

👉 For your specific needs or a request for a detailed quote, contact me via Blacky.10 on Signal.

#sell

💸On sale:
SCADA systems in Poland

The price will suit you, we sell it at a low price.

💸Payment:
@cryptoBot

📲Regarding the purchase:
@TwoNetBot

❤️ 2 👌 1

edited 191 👁 11:41

Attacks on critical infrastructure are not so “special” anymore and they will likely only become more common!

Three Pillars for Risk Mitigation

Risk & Exposure Management

Identify, Quantify, and Prioritize cybersecurity risk and compliance

Network Security

Assess, Segment, and Enforce with proactive and reactive controls

Threat Detection & Response

Detect, Investigate, and Respond to true threats and incidents

Threat Intelligence

Understand how threat actors behave and use this for informed defense

FORESCOUT RESEARCH | VEDERE LABS


Thank you.
FORESCOUT

WEBINAR

POWERED BY
pv magazine

pv magazine
WEBINARS

Decoding the first massive cyberattack on Europe’s solar energy infrastructure - The Poland case and lessons learned

29 April 2026

2:00 pm – 3:30 pm BST, London
3:00 pm – 4:30 pm CEST, Berlin
9:00 am – 10:30 am EDT, New York City

Emiliano Bellini
News Director
pv magazine

Uri Sadot
CEO
SolarDefend

Decoding the first massive cyberattack on Europe's solar Infrastructure

Premium content webinar

29 of April, 2026

SolarDefend introduction

"On a mission to secure the digital grid"

- I work with:
  - Solar Investors
  - Power Producers
  - OEMs
  - Academics

- Held positions:
  - Chair, SolarPower Europe
  - Contributing expert – European Commission Smart Energy Group
  - European Stakeholder Committee on Electricity

- Columnist & Podcaster

Uri Sadot

Industry impact of the attack

Reported after two weeks

LIGA.net

"Digital tanks are here". Poland says it was on the verge of blackouts due to Russian cyberattacks

Poland's Vice Prime Minister says the country almost suffered a large-scale power outage due to Russia's attack on energy infrastructure.

14 Jan 2026

Euronews.com

Poland's PM praises cyber defences after attack on heating grid foiled

Tusk blamed Russia and urged Parliament to swiftly pass new cybersecurity legislation to strengthen protection against foreign interference.

15 Jan 2026

Українська правда

Poland came "very close" to blackout in December due to Russian cyberattack – deputy PM

Krzysztof Gawkowski, Polish Deputy Prime Minister and Minister of Digital Affairs, has said that the country came "very close" to a blackout...

13 Jan 2026

- Dec 29 – attack
- Jan 13 – Publication by Polish PM
- Jan 23 – ESET report
- Jan 29 – Dragos Report
- Jan 30 – Cert.pl report

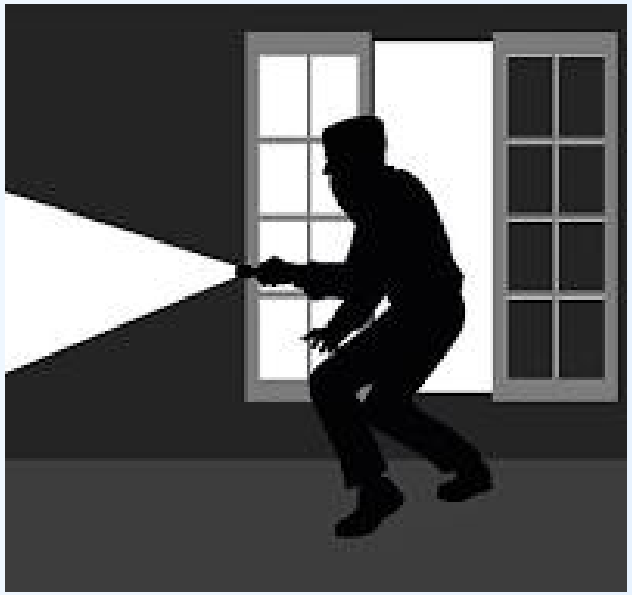
SOLAR DEFEND

Immediate impact

Financial

- 3 weeks of manual operations & partial downtime: **1,000-10,000 EUR per plant**
- Damaged equipment **1,000-10,000 EUR**

- Multiplied by 30 solar plants: **30,000-300,000 EUR**



SOLAR DEFEND

Source: interview with an investor \ institution of a plants affected

Potential impact

Financial estimates

- Inverter damages: **10,000-100,000 EUR** (per site), totalling **300,000-3,000,000 EUR**
- Power manipulation: Blackouts, grid damage – **Billions & casualties (e.g. Iberian blackout)**

SOLAR DEFEND

Longer term impact

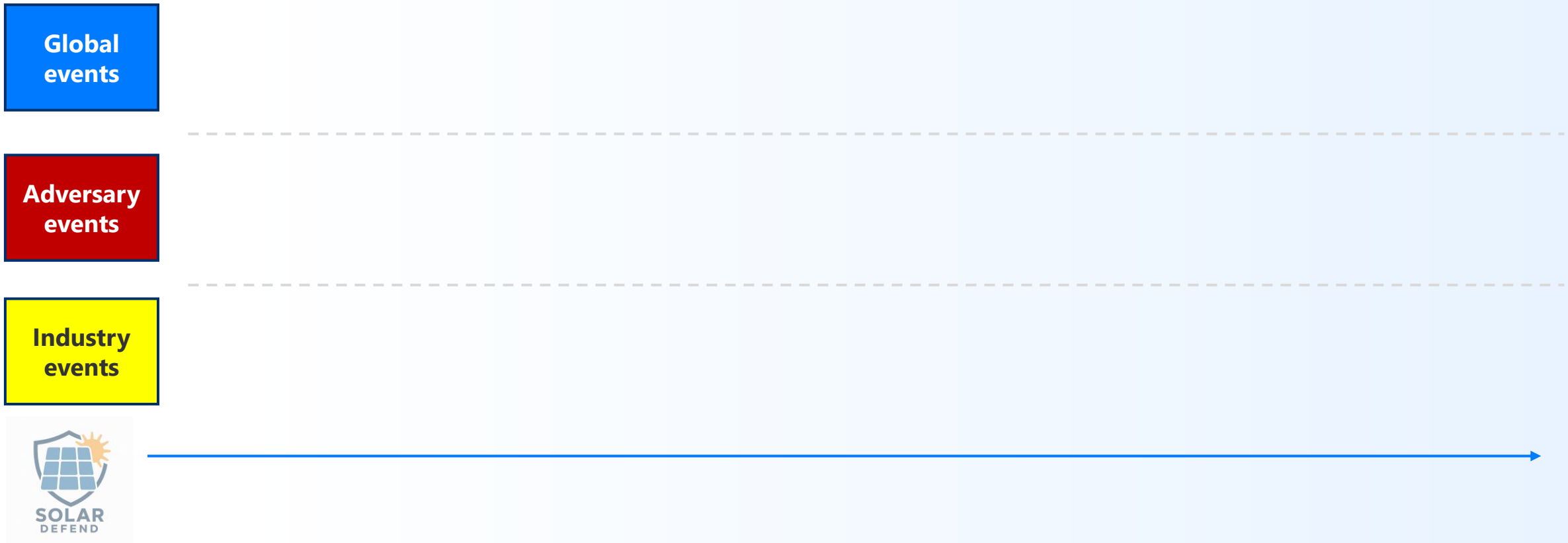
Speculative

- Heightened risk feeds into regulatory discussions
- Feeds into financing and insurance (NIS 2 exposure)
- Publicity may attract more attacks

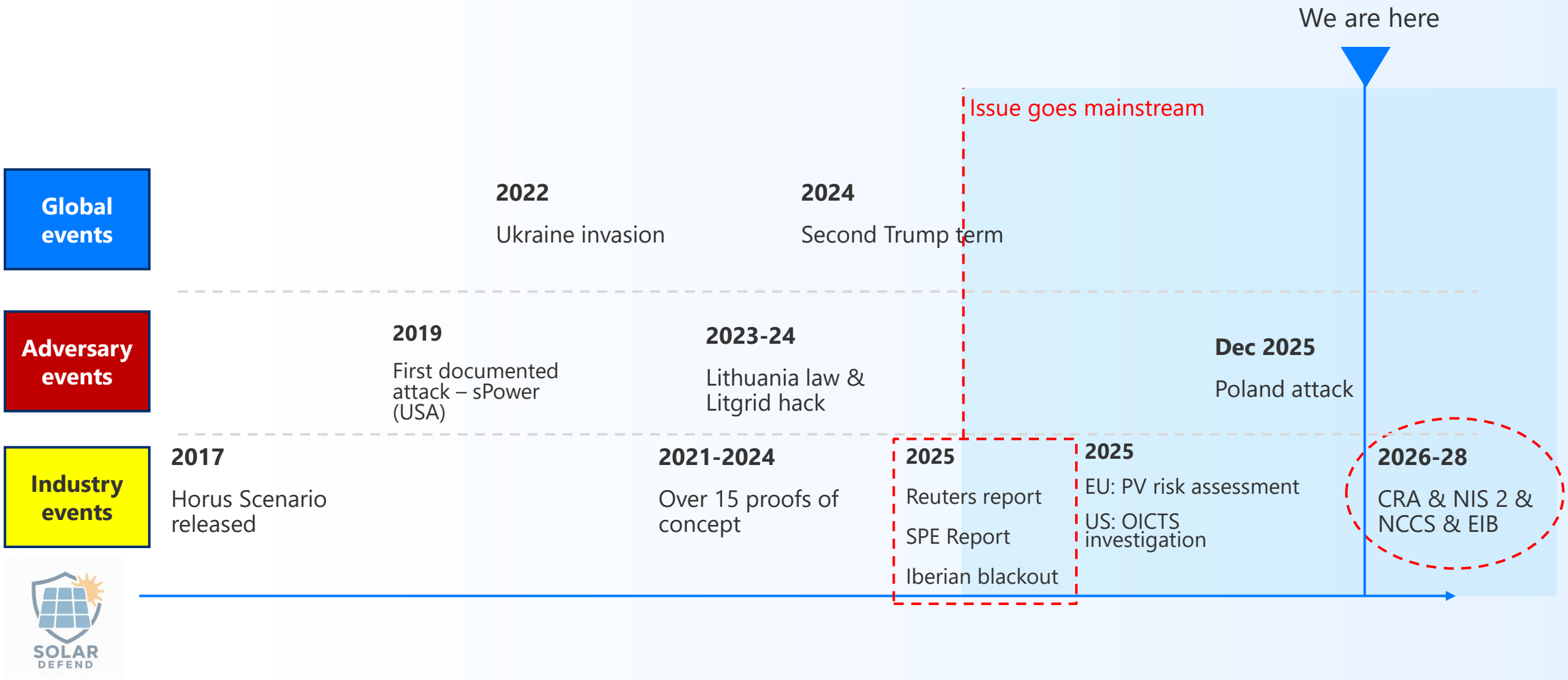
The attack hadn’t come from nowhere

SOLAR
DEFEND

Cyber in Solar: Past, Present, Future

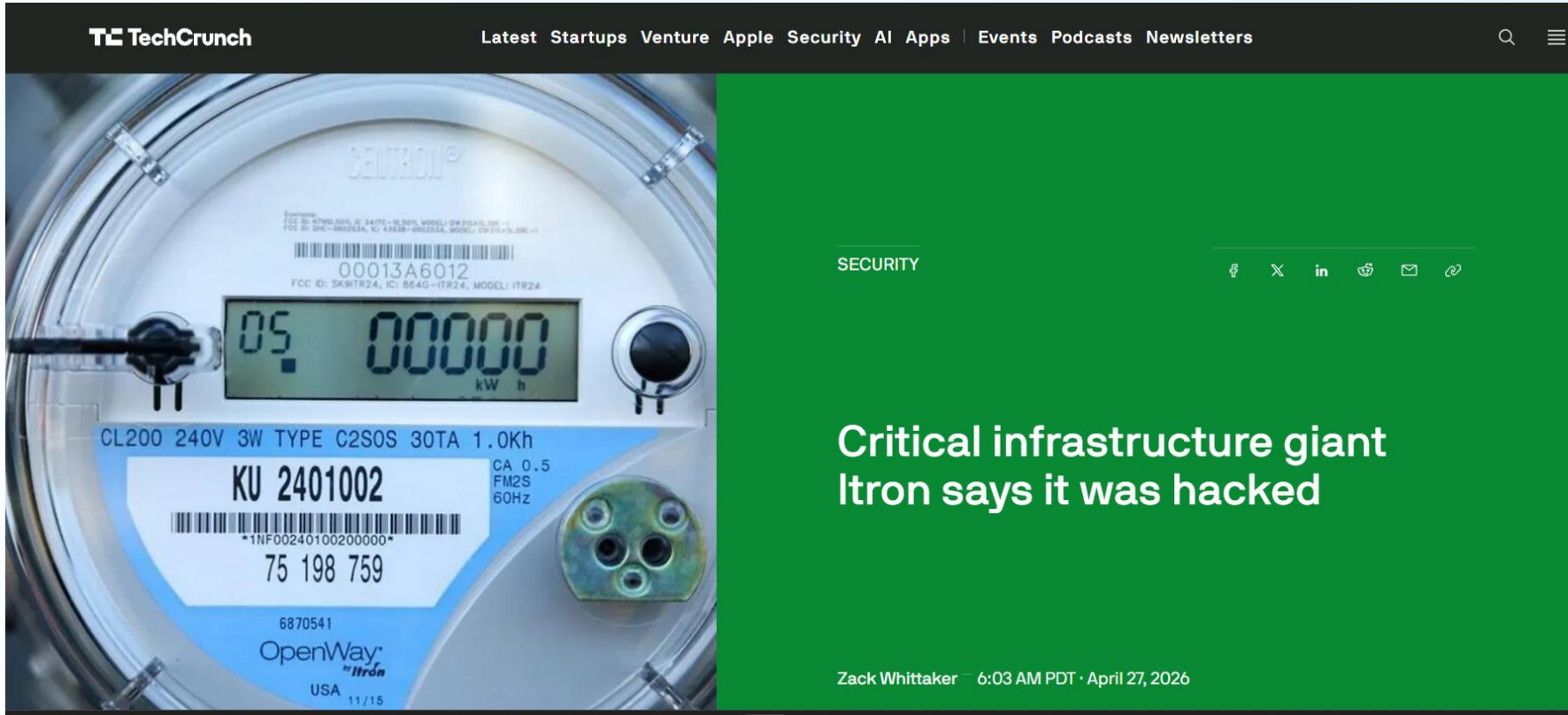


Cyber in Solar: Past, Present, Future



Events keep on happening

- **Two weeks ago**: Itron breach – smart meters (13th of April)



SOLAR DEFEND

Not just a “Solar” problem

- Wind
  - Vestas, 2021
  - Viasat, 2023
- Data Centers
  - Cyrus1
  - Equinix
- Water
- Many more

pv magazine International

Satellite cyber attack paralyzes 11GW of German wind turbines

German wind turbine operators have reportedly been confronted with a fault in the satellite connection of their systems.

1 Mar 2022

Page **1** of **2**

Vestas

News release from
Vestas Wind Systems A/S

Aarhus, 06 December 2021

Third update on cyber incident

On 19 November 2021, Vestas discovered a cyber security incident which involved external attackers gaining unauthorised access to some of Vestas' IT systems. Following extensive investigations, forensics, restoration activities and hardening of our IT systems and IT infrastructure together with external partners and experts, all systems are, with very few exceptions, up and running. The work and investigations are still ongoing, and Vestas still has no indication that the event has impacted customer and supply chain operations, a view which is supported by third-party experts.

BLEEPINGCOMPUTER

NEWS ▾ TUTORIALS ▾ WEBINARS DOWNLOADS ▾

Home > News > Security > Equinix data center giant hit by Netwalker Ransomware, $4.5M ransom

Equinix data center giant hit by Netwalker Ransomware, $4.5M ransom

By Lawrence Abrams September 10, 2020 11:32 AM 0

SOLAR DEFEND

Don’t worry – good news ahead

- But first, let’s hear our other two speakers
  - Florian – on NIS 2 exposure
  - Fabian – on practical cyber risk management

SOLAR DEFEND

WEBINAR

POWERED BY
pv magazine

pv magazine
WEBINARS

Decoding the first massive cyberattack on Europe’s solar energy infrastructure - The Poland case and lessons learned

29 April 2026

2:00 pm – 3:30 pm BST, London
3:00 pm – 4:30 pm CEST, Berlin
9:00 am – 10:30 am EDT, New York City

Emiliano Bellini
News Director
pv magazine

Florian Eisenmenger
Specialist IT Lawyer
Osborne Clarke

pv magazine Webinar+

The Poland case from a NIS2 legal perspective

29 April 2026

NIS2 – Background: The EU Cybersecurity Strategy (December 2020)

Cybersecurity

NIS2 Directive + **CER Directive**

Cyber Resilience Act | **Cybersecurity Act**

- **Geopolitical tensions also threaten the virtual space**
- **Attacks on critical infrastructures as a major global risk**
- **Cross-sector interdependencies and industry's dependence on IT systems**
- Crime investigation has increasingly digital components
- Digital services and financial services are among most frequent targets of cyberattacks
- Security concerns as major disincentive to use online services
- Major shortage of cybersecurity skills in the workforce, too few cyber security experts on the market
- EU lacks collective awareness of cyber threats

➢ **Cybersecurity is essential for prosperity in Europe and the protection of European fundamental rights**

Europe's Digital Decade 2020 – 2030

See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018 for more details

NIS2 – Recap (including Germany)

Entities providing services or carry out activities within the EU

Important Entity

at least medium-sized public or private entities[1] in **sectors** listed in **Annex I or II** (critical sectors)

50+ employees (*annual work units*) **and** EUR 10m+ turnover **or** EUR 10m+ balance sheet

Essential Entity

>medium-sized public or private entities[1] in **sectors** listed in **Annex I** (high criticality sectors)

250+ employees (*annual work units*) **and** EUR 50m+ turnover **or** EUR 43m+ balance sheet

Important & Essential Entities regardless of size

- Providers of public electronic communications networks or services
- Trust service providers
- Domain registries or certain DNS services
- Sole providers of critical societal or economically important activities
- Disruption of the service could have significant effects on public order or security
- Particular importance at national or regional level for the respective sector
- Certain public administration entities
- **Critical entities under the CER Directive**[2] (e.g., energy sector)

[1]Recommendation 2003/361/EC: Consider numbers of partner & linked enterprises (upstream & downstream)

SPVs?

Germany: Critical Facilities Operator

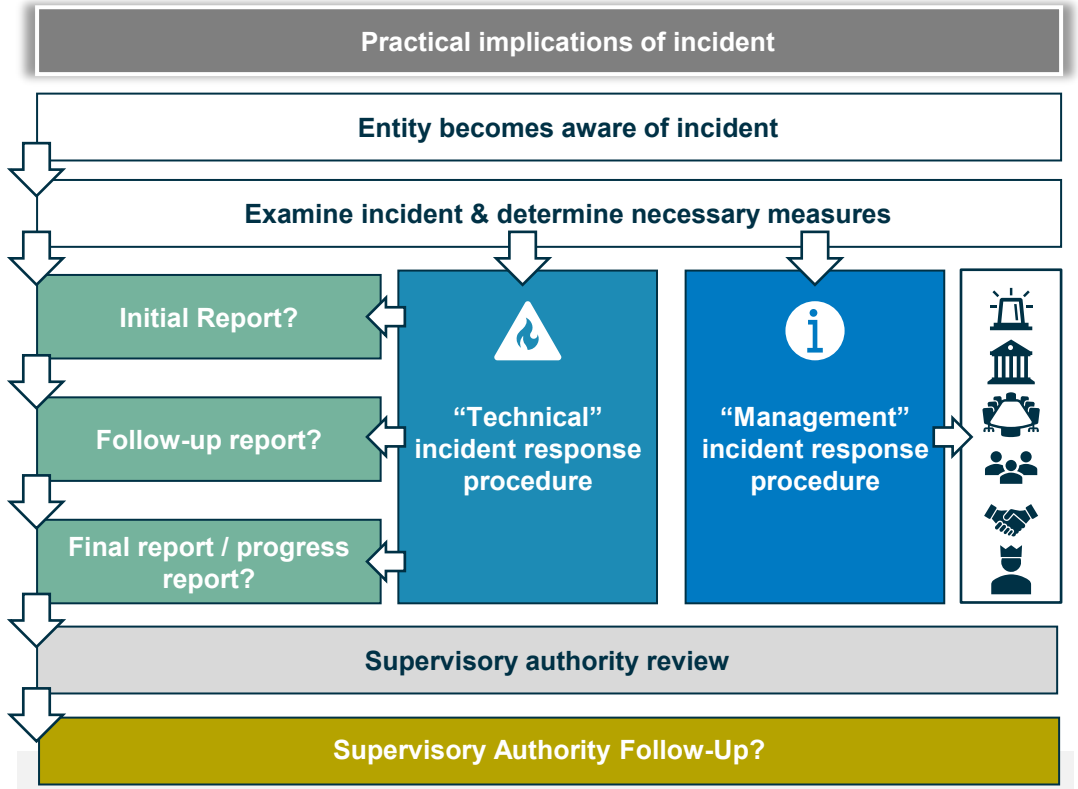
Entities qualifying as **operator** of critical facilities under the German BSI-KritisV

Sector and facility specific thresholds under the BSI-KritisV apply

[2] **Directive (EU) 2022/2557**

NIS2 – Overview Key Obligations and Sanctions (Germany)

Cybersecurity Risk Management	Implement cybersecurity risk-management measures; additional obligations for critical facilities operators, but sector-specific rules apply (e.g., entities in the energy sector regulated under the energy industry law, EnWG).
Supply Chain Security	Cybersecurity-related aspects of relationships between each entity and its direct suppliers or service providers must be taken into account
Registration	Regulated entities must register with the BSI (sector-specific provisions apply); critical facilities operators must provide additional information upon registration
Providing evidence of compliance	Critical facilities operators must regularly provide evidence of implementation of cybersecurity risk-management measures (sector-specific obligations for energy sector)
Reporting	Three-stage incident-reporting: initial report within 24 hours, follow-up report within 72 hours, final/progress report after one month; where applicable, notification of status updates at the request of the supervisory authority (BSI, unless sector-specific rules)
Management	Management to approve, implement and monitor implementation of cybersecurity risk-management measures; continuous training obligation, management may be held personally liable for certain compliance violations (in line with corporate law provisions)
Administrative Fines	Up to EUR 10 million or up to 2% of the total worldwide turnover of the preceding financial year, whichever is higher (depending on entity turnover).



- Authority may follow up on incident with various measures, e.g., requiring notification of public/customers, order third-party audits, request deficiency mitigation plan, temporarily suspend authorisations granted under sectoral legislation, temporarily prohibit unreliable management from carrying out the activities for which they are appointed
- **Conflict of interest for management: Risk liability?**

NIS2 – Key Obligations

Cybersecurity Risk Management	Implement cybersecurity risk-management measures; additional obligations for critical facilities operators, but sector-specific rules apply (e.g., entities in the energy sector regulated under the energy industry law, EnWG).
Supply Chain Security	Cybersecurity-related aspects of relationships between each entity and its direct suppliers or service providers must be taken into account
Registration	Regulated entities must register with the BSI (sector-specific provisions apply); critical facilities operators must provide additional information upon registration
Providing evidence of compliance	Critical facilities operators must regularly provide evidence of implementation of cybersecurity risk-management measures (sector-specific obligations for energy sector)
Reporting	Three-stage incident-reporting: initial report within 24 hours, follow-up report within 72 hours, final/progress report after one month; where applicable, notification of status updates at the request of the supervisory authority (BSI, unless sector-specific rules)
Management	Management to approve, implement and monitor implementation of cybersecurity risk-management measures; continuous training obligation, management may be held personally liable for certain compliance violations (in line with corporate law provisions)
Administrative Fines	Up to EUR 10 million or up to 2% of the total worldwide turnover of the preceding financial year, whichever is higher (depending on entity turnover).

Cybersecurity risk-management measures pursuant to Art. 21 NIS2:

a. policies on risk analysis and information system security;
b. incident handling;
c. business continuity, such as backup management and disaster recovery, and crisis management;
d. supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
e. security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
f. policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
g. basic cyber hygiene practices and cybersecurity training;
h. policies and procedures regarding the use of cryptography and, where appropriate, encryption;
i. human resources security, access control policies and asset management;
j. the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Additional Cybersecurity risk-management measures pursuant to Sec. 5c EnwG:

k. Use of intrusion detection systems pursuant to Sec. 2 (41) of the German BSIG
l. Only use ICT products certified in accordance with European cybersecurity schemes pursuant to Article 49 Cybersecurity Act

NIS2 – Transposition in selected EU Countries (high-level)*

	Netherlands	Italy	Spain	Poland
Transposition NIS2	• **No local NIS2 law**; transposition likely completed in Q2/2026 • Transposition CER part of NIS2 package	• **Completed**, local NIS2 law in force since October 2024	• **No local NIS2 law**; draft bill published in 2025 (status unclear)	• **Completed**, local NIS2 law in force since March 2026
Registration	• Portal operated by National Cyber Security Centre	• Portal operated by National Cybersecurity Agency, registration annually by end of February	• Within three months of qualification as regulated entity, registration portal not active yet	• Within six months of qualification as regulated entity, portal operated by Ministry of Digital Affairs
Significant Deviations	• Draft transposition law closely follows NIS2	• Yes, e.g., annual registration obligation starting in January	• Likely not	• Yes, e.g., high-risk vendor provisions (subject to debate)
Additional Sectors in Scope	• No, but broadened scope within sectors, e.g., higher education institutions, local and regional governments	• Yes, e.g., central, regional, local public administrations; local transport services, entities carrying out activities of cultural interest	• No, but broadened scope within sectors, e.g., including nuclear industry, private security, universities, municipalities >20,000 inhabitants, entities with impact on national defence	• No, but broadened scope within sectors, e.g., including nuclear industry, healthcare
Fines (only deviations from NIS2)	• Fines in case of "other" infringements limited to EUR 1 million	• Fines for certain infringements under local NIS2 law up to EUR 50.000 • Fines of up to EUR 125,000 for public administration entities	• Fines of up to EUR 2 million for very serious infringements • Fines for minor infringements of up to EUR 100.000	• Fines of up to approx. EUR 24 million for entities violating local NIS2 law and thereby causing direct and serious cybersecurity threat to national defence, state security, public safety and order, human life and health

Local NIS2 transpositions laws & registration requirements must be considered for each EU Member State

* Based on publicly available information, as of 23 April 2026.

Thank you

Your Contact

Dr. Florian Eisenmenger
Counsel
Germany

Dr. Florian Eisenmenger
Counsel | Specialist Lawyer for IT Law
CIPP/E | CIPM | FIP
Dr. Florian Eisenmenger | Osborne Clarke

E florian.eisenmenger@osborneclarke.com
M +49 163 518 4737
Osborne Clarke GmbH & Co. KG
Lilli-Palmer-Straße 2 | 80636 Munich | Germany

WEBINAR

POWERED BY
pv magazine

pv magazine
WEBINARS

Decoding the first massive cyberattack on Europe’s solar energy infrastructure - The Poland case and lessons learned

29 April 2026

2:00 pm – 3:30 pm BST, London
3:00 pm – 4:30 pm CEST, Berlin
9:00 am – 10:30 am EDT, New York City

Emiliano Bellini
News Director
pv magazine

Fabian Michel
Head of Cyber Security & Operational Technology (OT)
BELECTRIC

Official Partner of the Sun

BELECTRIC® | MEMBER OF ELEVION GROUP

25 Official Partner of the Sun

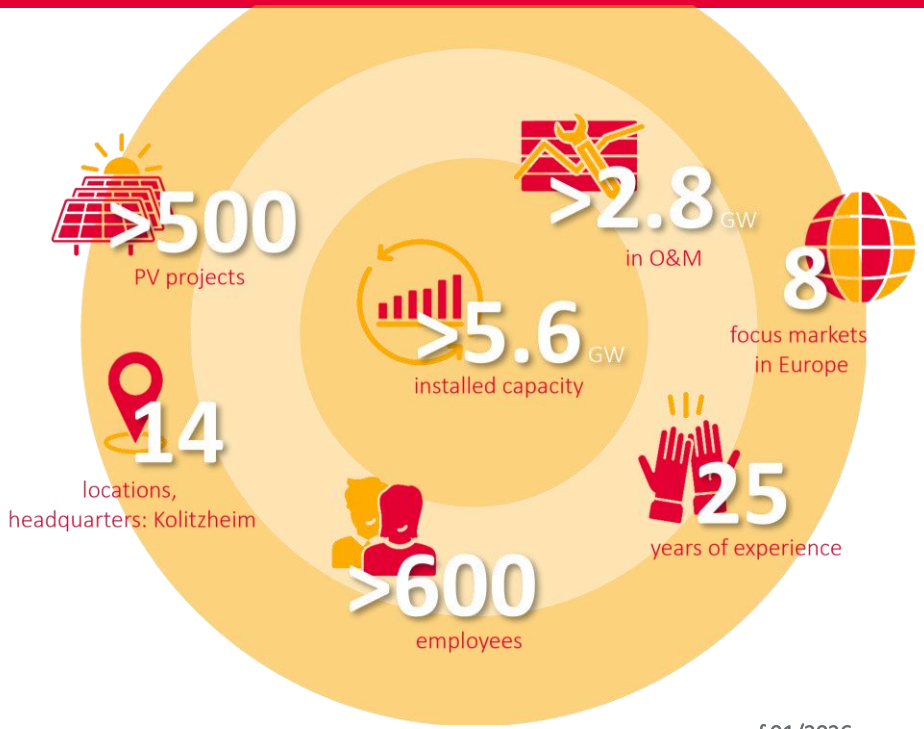
Innovation & System Design

Project Development

Engineering, Procurement & Construction (EPC)

Operations & Maintenance (O&M)

of solar & battery storage systems



as of 01/2026

EPC & O&M Operational View – Poland Cyberattack

Lessons from the Poland Cyberattack

EPC Phase – What we build becomes the attack surface of tomorrow

- Standardized designs = standardized cyber risk = Standardized Mgmt.
- designs depends also on customer requirements
- Clearly defined cyber roles and responsibilities (EPC, O&M, manufacturer, supplier, asset owner). **Main responsibility is on the IPP / owner**.
- Supply chain security begins even before the nonbinding offer, with the selection of the right components and manufacturers.
- Follow IEC 62443 design principles and implement network zones
- EPC decisions directly shape O&M cyber risk and recoverability

O&M Phase – Availability depends also on Cyber hygiene

- Ongoing asset and risk management
- Vulnerability and patch management are mandatory
- **Visibility is the key**
- Patch internet-connected devices asap after vulnerabilities are discovered
- Regularly changing the passwords for all devices
- Identity management & access control
- Loss of view / control halts operations even if generation continues
- Recovery time, not outage, is the real business impact

What happens next?

Quick recap

- An unprecedented, widescale cyber attack on our sector
- Part of a broader Infrastructure security problem
- NIS 2 sets high penalties on top
- Most solar plants require investment

SOLAR DEFEND

A regulatory wave is coming (Europe)

Legislative initiatives:

- Limitation on funding allocation (EIB, EBRD, InvestEU, etc) ~20B EUR/year – 15% of market
- Warning CSA may expand ban to 100%
- Stricter NIS 2 enforcement, regardless of OEM Provenance
- Cyber Resilience Act legislation process
- Network Code on Cybersecurity revision

(Deeper dive possible in the Q&A)

Bottom line: big focus on Solar Inverters

SOLAR DEFEND

Key open questions

Enforcement level

- How strictly will the rules be enforced?
  - Penalty size
  - Treatment of “loopholes” – (e.g. onshoring of manufacturing, cloud infra)
  - Exceptions
  - Extensions
  - Member state uniformity

So far

- Criticism on lax enforcement in Germany, Spain
- Seemingly harsh enforcement in Italy and Central Europe

SOLAR DEFEND

Future attacks?

- Hard to say, but trendline is worrying
- Move to BESS increases sector risk

- Points to watch out for:

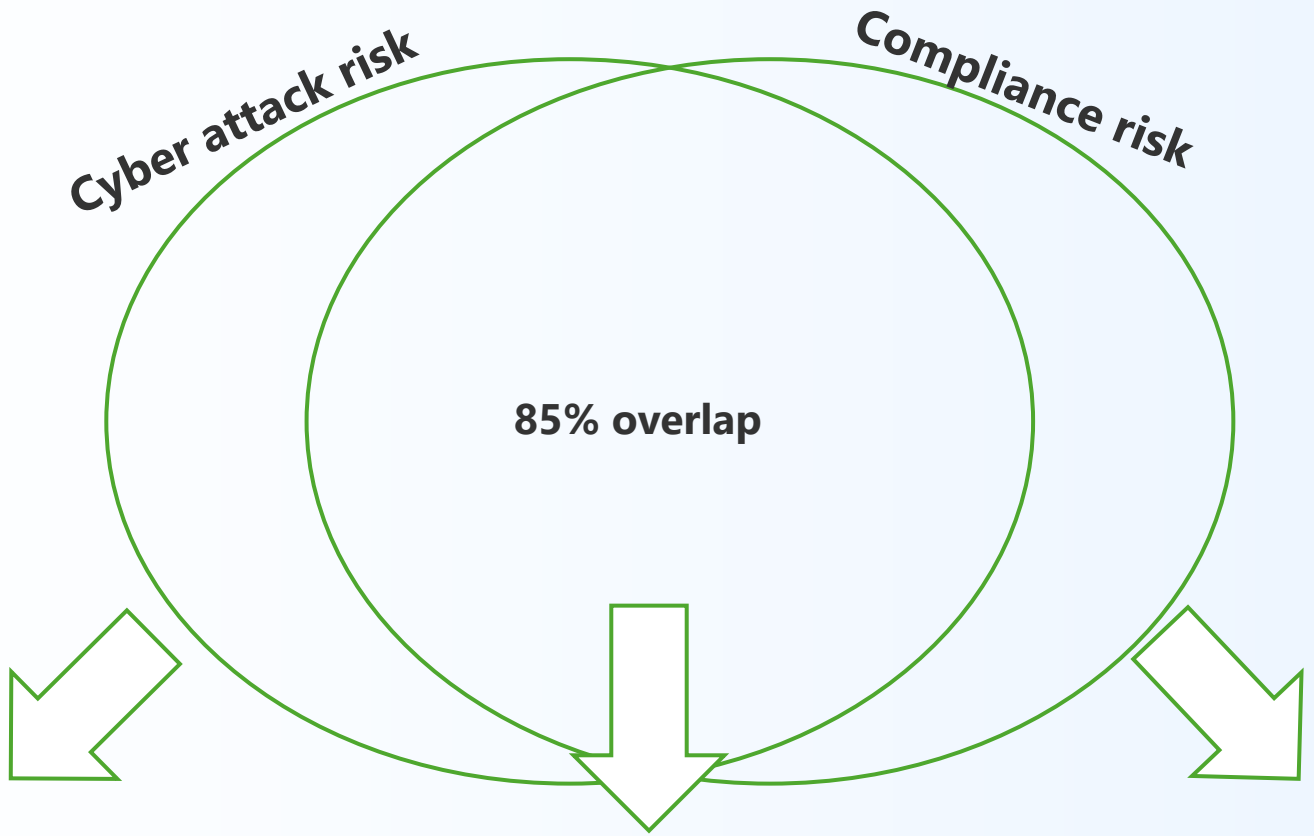
    - Ransom attacks?
    - Hybrid warfare attacks?

    - Local site attacks?
    - Aggregated grid attacks?

SOLAR DEFEND

What you can do tomorrow?

Two risks to reduce



Even compliant companies get hacked

IEC 62443 Certification
ISO 27001
Penetration testing
etc

Reporting
Documentation
Registration
...

SOLAR DEFEND

How to reduce compliance risk

Onboard expertise

- In house
- Consultants

IEC 62443 is the key

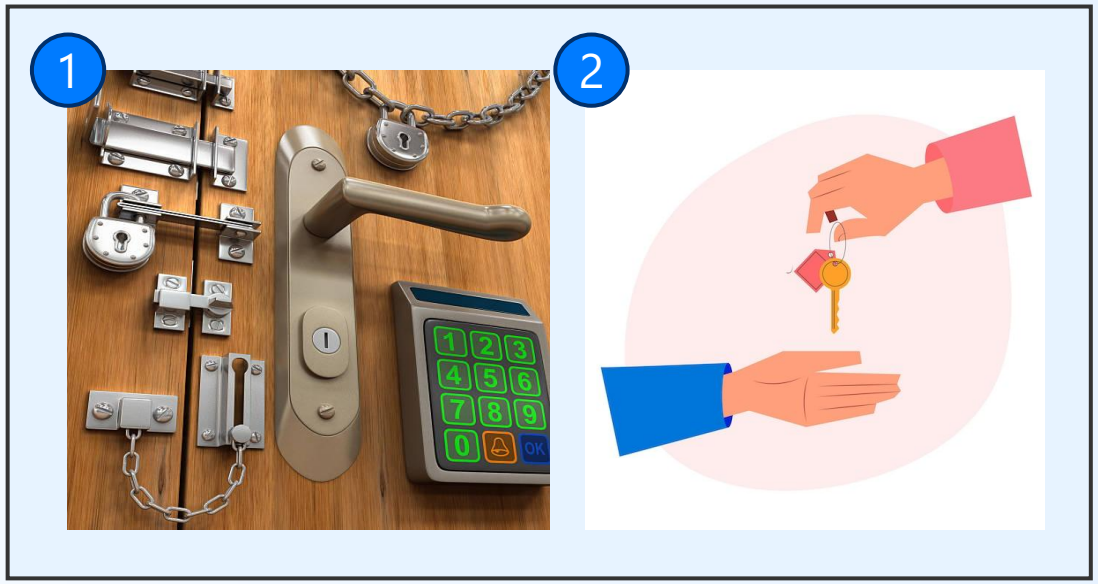
SOLAR DEFEND

How to reduce “cyber attack risk”

Onboard expertise
- Preferably in-house
- Include in O&M RFP

Invest in infrastructure
- HQ to sites communications
- Secure plants

Get the right tools
- Secure remote connections
- Next Gen Firewalls and managed switches
- Intrusion detection systems
- SOC monitoring services



And if you need to remember ONE THING

The Lion

&

The Dentist

SOLAR DEFEND

Thank you!

SOLAR DEFEND

WEBINAR

POWERED BY
pv magazine

pv magazine
WEBINARS

29 April 2026

2:00 pm – 3:30 pm BST, London
3:00 pm – 4:30 pm CEST, Berlin
9:00 am – 10:30 am EDT, New York City

Decoding the first massive cyberattack on Europe’s solar energy infrastructure - The Poland case and lessons learned

Q&A

Emiliano Bellini

News Director

pv magazine

pv magazine WEBINARS

The latest news print & online

Most-read online!

UK solar generation hits record 15 GW as gas falls to historic low

by Matthew Lynas

Developing El Niño points to stronger solar conditions across Australasia and South Asia

by Solcast

pv magazine WEBINARS

Coming up next…

Tuesday, 5 May 2026

10:00 am – 11:00 pm CEST, Berlin

1:30 pm – 2:30 pm IST, Delhi

SolaX Trene 261: Liquid-cooled C&I ESS cabinet for fast deployment

Wednesday, 6 May 2026

3:00 pm – 4:00 pm CEST, Berlin

9:00 am – 10:00 am EDT, New York City

Holistic design: Ending the relay race in utility-scale PV projects

Many more to come!

In the next weeks, we will continuously add further webinars with innovative partners and the latest topics.

Check out our pv magazine Webinar program at:

www.pv-magazine.com/webinars

Registration, downloads & recordings can also be found there.

WEBINAR

POWERED BY
pv magazine

pv magazine
WEBINARS

Thank you for joining today!

Emiliano Bellini
News Director
pv magazine