

OT Cyber Security

Rainer Baeder



Cyberdefense

Typical Customer Journey OT Cyber Security

Step 1

Trigger & Awareness

- Common triggers: Security incidents (in-house or involving competitors), new compliance requirements (NIS2, GDPR), audit results
- Content: Technical articles, threat reports, webinars, SEO-optimized blog posts on current threats

Step 2

Consideration

- Multiple decision-makers involved: IT directors, CISOs, executive management, and often data protection officers as well
- Content: White papers, comparative studies, case studies, analyst reports (Gartner, Forrester)
- Important: technical depth AND business value (risk mitigation, compliance, costs)

Step 3

Strategy

Gap Analysis & Priorization

Step 4

Requirements

Architecture Design and Market Analysis

Step 5

Evaluation

- Highly security-specific: testing phases, sandbox demos, penetration tests, discussions with reference customers
- Trust is the main driver here—certifications (ISO 27001, SOC 2), references, transparency regarding the company's own security architecture

Step 6

Decision & Purchase

- Often a complex procurement process (RFP, security clearance, legal review)
- Clear SLAs, an onboarding plan, and a support structure should already be in place at this stage

Step 7

Implementation

- Critical Phase: A Smooth Deployment Is Key to Customer Satisfaction
- Dedicated Point of Contact, Clear Communication, Training

Step 8

Operation

- Regular security updates, threat intelligence reports, quarterly business reviews
- Satisfied customers become references—which is extremely important in this industry, since trust is a key factor in purchasing decisions

- Very long sales cycles (often 6–18 months)
- Multi-stakeholder decisions (technical, business, and legal)
- Trust signals (certifications, audits, transparency) are more important than pure marketing
- Content must appeal to both groups: technical experts and decision-makers without in-depth technical knowledge

OT Security Attacks

□ Recent and Ongoing Industrial Cyber Incidents (2022–2025)

1. Polish Critical Infrastructure Cyber Operations (2024–2025)
2. Danish Energy Sector Intrusions (2023–2024)
3. United States Water Utilities Cyber Incidents (2023–2024)
4. German Municipal Utilities Cyber Incidents (2023–2024)
5. Jaguar Land Rover Ransomware Attack (2023)
6. Ukraine–Russia Conflict Cyber Operations (2022–2024)
7. Pipedream / Incontroller (2022)

OT Security Attacks

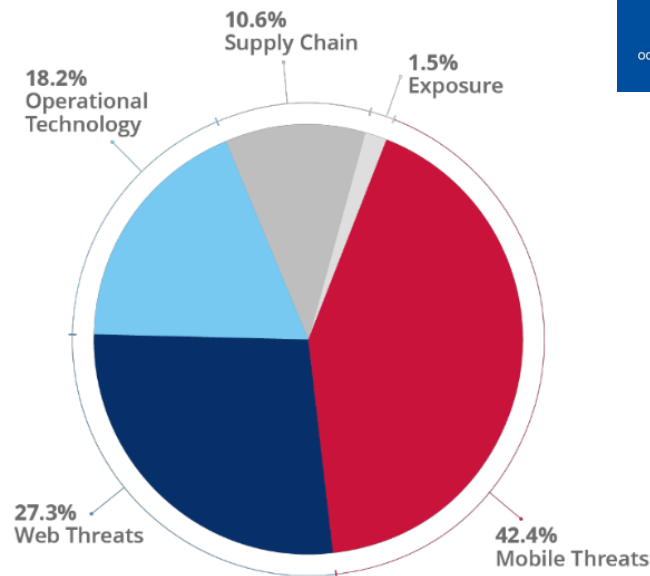
- Foundational and Historical ICS and Industrial Cyber Attacks (2000–2021)
 8. JBS Ransomware Attack (2021)
 9. Colonial Pipeline (2021)
 10. SolarWinds Supply Chain Attack (2020)
 11. EKANS / Snake Ransomware Attacks (2019–2023)
 12. Norsk Hydro Ransomware Attack (2019)
 13. Ryuk Ransomware (2018–2022)
 14. APT33 Campaigns (2017–2020)
 15. WannaCry Ransomware (2017)
 16. NotPetya (2017)
 17. Triton / Trisis (2017)
 18. Industroyer / CrashOverride (2016)
 19. Sandworm Campaigns (2015–2020)
 20. Ukraine Power Grid Attack (2015)
 21. BlackEnergy (2014–2015)
 22. Dragonfly / Energetic Bear (2014)
 23. German Steel Mill Cyber Attack (2014)
 24. Havex (2013)
 25. Shamoon (2012, 2016, 2018)
 26. Stuxnet (2010)
 27. Slammer Worm Impact on Davis-Besse Nuclear Plant (2003)
 28. Maroochy Shire Sewage Spill (2000)

ENISA THREAT LANDSCAPE 2025

The distribution of threat categories shows a clear concentration in a few areas. Mobile threats account for the largest share at 42.4%, highlighting how mobile devices continue to be a primary attack surface. Web threats follow with 27.3%, underlining the persistent exploitation of online services and applications. Operational technology threats represent 18.2%, reflecting the growing exposure of industrial and critical systems as they continue being increasingly connected and targeted. Supply chain risks make up 10.6%, showing that attackers are actively leveraging indirect pathways through third-party providers and dependencies.

Fig. 5 - Distribution of threats.

Source: ENISA dataset



Hugging Face Incident Initial Post-Mortem

Expedited Strategy Briefing

By the CSA CISO Community, SANS, [un]prompted, RSAC, Knostic, FIRST, and the wider community.

Angriffe auf Wasserversorger in Minnesota decken Cyberrisiken der Branche auf (31. Juli 2026)



Hackers targeted operational technology (OT) systems at two private water utilities in Colorado in late August, apparently attempting to cause disruptions...

CISA urged the water sector to secure OT in light of these attacks. **The cybersecurity agency said it is aware of 100 internet-exposed water systems** targeted in cyberattacks in July.

What is confirmed

Between Sunday, July 26 and Monday, July 27, more than 30 community water and wastewater systems across Minnesota were targeted in what Minnesota IT Services has described as a coordinated cyberattack. MNIT activated statewide incident response.



New Jersey, Alabama Join States Targeted in Water Cyberattacks

ARTIFICIAL INTELLIGENCE

Hackers Using AI to Target Siemens PLCs in Critical US Sectors

A cybersecurity advisory with technical details and recommendations has been written by the NSA, CISA and other agencies.

By Edward Kovacs | August 20, 2026 (3:02 AM ET)



securityweek.com

Several government agencies in the United States have issued a joint cybersecurity advisory warning critical infrastructure organizations about hacker attacks targeting Siemens programmable logic controllers (PLCs).

TRENDING

- 1 Banking Trojans Maric, Grandoreiro, ToxicPanda 2.0 in the Spotlight
- 2 Rust Supply Chain Attack Linked to North Korean Hackers
- 3 New Phishing Toolkit Uses Passkeys to Maintain Access After Password Resets
- 4 Encrypted Prompts Bypass AI Safety Guards in GPT and Gemini
- 5 Anthropic Expands Mythos 5 Access to More Defenders, Unwells \$35M Open Source Fund
- 6 Iran-Linked Hackers Shut Down UK Power Plant for Four Days
- 7 Hackers Using AI to Target Siemens PLCs in Critical US Sectors
- 8 Microsoft Patches Exploited Entra ID Vulnerability

CYBERSECURITY ADVISORY

Defending Against an Active Threat to Siemens S7 Series PLCs

Release Date: August 19, 2026

Alert Code: AA26-231A

DEFENDING AGAINST AN ACTIVE THREAT TO SIEMENS S7 SERIES PLCs →

RELATED TOPICS: [CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE](#), [INDUSTRIAL CONTROL SYSTEMS](#), [CYBER THREATS AND RESPONSE](#)

Executive summary

Note: This advisory relates to an active threat to Siemens S7 Series programmable logic controllers (PLCs). However, ongoing PLC targeting activity is broader than Siemens PLCs. All PLC owners and operators should apply relevant mitigations to reduce the risk to their devices and systems. The Siemens-specific content in this advisory should be understood and applied as one subset of the wider threat landscape.

Top Mitigations

- **Inventory** all Siemens S7 Series programmable logic controllers (PLCs)
- **Apply** critical security patches
- **Ensure** PLCs are **not** accessible from the Internet
- **Strengthen** access controls
- **Monitor** for unauthorized activity
- **Harden** PLC services, protocols, and ladder logic integrity
- **Hunt** for anomalies that may indicate a compromise

cisa.gov



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

AI-Generated Exploit Scripts Target Siemens S7 PLCs in U.S. Critical Infrastructure



The U.S. government on Wednesday **warned** of an "active threat" targeting critical infrastructure organizations in the country using artificial intelligence (AI)-generated exploit scripts.

The activity is targeting Siemens S7 Series Programmable Logic Controllers (PLCs) to conduct reconnaissance and capability development using AI-generated scripts disguised as legitimate monitoring tools. That said, the ongoing PLC targeting activity is assessed to be broader in scope than Siemens PLCs.

Dragos details AI-assisted intrusion targeting Mexican water utility as Claude, OpenAI models used to pursue OT access

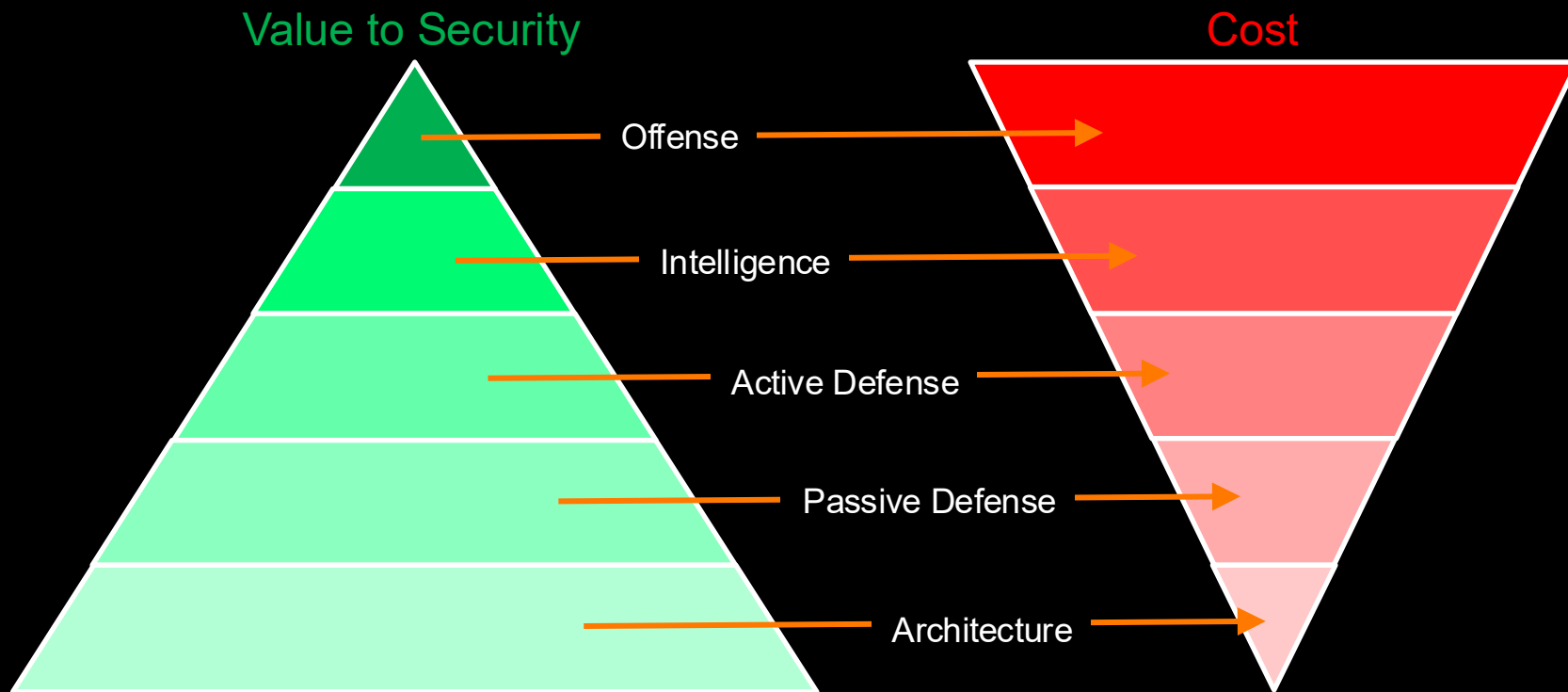


- Dragos analysis of materials associated with the compromise of a municipal water and drainage utility's IT environment indicates an unknown adversary leveraged commercial AI tools to target OT infrastructure.
- Dragos assesses with high confidence that the intrusion was primarily enabled by Anthropic's Claude, which supported the development and technical execution of core intrusion activity.
- The AI correctly identified an internally accessible vNode Supervisory Control and Data Acquisition (SCADA) / Industrial Internet of Things (IIoT) management interface as a critical infrastructure-related asset and generated a targeted password spray attack to breach the IT-OT boundary.
- Extensive AI-developed tooling demonstrated how an adversary's use of AI as an aid materially accelerated the intrusion by operationalizing capabilities against IT systems adjacent to OT through the rapid application of publicly available tradecraft.

New Jersey, Alabama Join States Targeted in Water Cyberattacks

What is remarkable is not that programmable logic controllers are being targeted—that is well known. **What is remarkable is how. According to the authorities, the attackers use AI-generated exploit scripts, disguised as legitimate OT monitoring tools, to identify exposed S7 controllers.** Using search services such as Censys and ZoomEye, they locate devices that are accessible from the internet—preferably those with outdated firmware or lacking basic network segmentation. The entire product line, from the S7-200 to the S7-1500, is affected.

OT Security Best Practice – Sliding Scale of Cyber Security (SANS)



73% of CISOs admit security incidents due to unknown or unmanaged assets

News

May 12, 2025 • 2 mins

As IT infrastructures become increasingly complex, so do the attack surfaces. Many companies are doing too little to contain the risks.



Credit: ozalpashid - shutterstock.com

Only those who know their attack surfaces can defend against them effectively. What seems like a truism, however, appears to be causing problems for many companies.

According to a **survey of more than 2,000 cybersecurity executives by security provider Trend Micro**, nearly three-quarters (73%) of security leaders say they have experienced a security incident because assets in their IT infrastructure were not managed or simply unknown.

Approximately nine out of 10 managers surveyed stated that **attack surface management** directly impacts their company's business risk. A large proportion of respondents also admitted that a lack of **risk management** for exposed assets could have significant negative consequences. Negative consequences are feared for the following areas, among others:

- Business continuity (42% of respondents)
- Competitiveness (39%)
- Customer trust and brand reputation (39%)
- Supplier relationships (39%)
- Employee productivity (38%)
- Financial performance (38%)

https://www.csoonline.com/article/3980431/more-assets-more-attack-surface-more-risk.html?utm_date=20250514035709&utm_campaign=CSO%20US%20First%20Look&utm_content=sloho-3-tile-73%25%20of%20CISOs%20admit%20security%20incidents%20due%20to%20unknown%20or%20unmanaged%20assets&utm_term=CSO%20US%20Editorial%20Newsletters&utm_medium=email&utm_source=Adestra&aid=16065171&huid=204be216-8511-4f41-b3ed-d4e8-ba33db35

Cyberangriff auf 470.000 PV-Anlagen - Eine Sicherheitslücke hätte die Abschaltung von 17 GW ermöglicht!



Wie die **ARD Tagesschau** berichtet, hat ein **23-jähriger Hacker** eine kritische **#Sicherheitslücke** in der Cloud-Plattform des chinesischen Herstellers Sungrow entdeckt und dabei weitreichende Administratorrechte erlangt.

Das erschreckende Ausmass:

- Zugriff auf rund 470.000 PV-Anlagen, davon 250.000 in Deutschland.
- Potenziell 17 GW Solarleistung, die laut dem Sicherheitsforscher gleichzeitig hätten abgeschaltet werden können.
- Ein mögliches Szenario mit gravierenden Folgen für die Stabilität unseres europäischen Stromnetzes.

<https://www.tagesschau.de/inland/regional/hessen/hr-sicherheitsluecke-bei-solaranlagen-hacker-entdeckt-kritische-sungrow-schwachstelle-100.html>

OT Security 5 Critical Controls (SANS) for ICS/OT cyber defense

- 1) ICS-specific incident response
- 2) Defensible architecture
- 3) ICS network visibility
- 4) Secure remote access
- 5) Risk-based vulnerability management

**Und :
Gesunder
Menschen-
Verstand**