BLACK CELL
Protecting critical infrastructures

Critical Systems security feed

2026 August

2026 August, Critical Systems security feed

Black Cell is committed for the security of Critical Systems and Critical Infrastructure, therefore we are publishing a monthly security feed. This document gives useful information and good practices to the ICS, OT and critical infrastructure operators and provides information on vulnerabilities, podcasts, trainings, conferences, books, and incidents on the subject of ICS and OT security. Black Cell provides recommendations and solutions to establish a resilient and robust critical systems security organization. If you're interested in critical systems security, feel free to contact our experts at info@blackcell.io.

List of Contents

1. Critical systems security practices, recommendations 2
2. Critical systems security conferences 3
3. Critical systems security incidents 5
4. Book recommendation 9
5. Critical systems security news selection 10
6. Critical systems vulnerabilities 19
7. Critical systems security alerts 27
8. Critical systems security trainings, education 29
9. Critical systems security podcasts 32

1. Critical systems security practices, recommendations

CI Fortify – Advice for isolating vital systems

CISA and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), in collaboration with the Federal Bureau of Investigation and international partners, released joint guidance CI Fortify – Advice for isolating vital systems. This guidance contains practical steps for critical infrastructure (CI) organizations to isolate vital operational technology and enabling systems from all other networks in the event of disruption or crisis and operate in isolation for an extended period. Developed to address escalating cyber threats, the guidance outlines key steps for identifying critical systems, mapping connections, and implementing effective separation points. By following these recommendations, organizations can enhance their resilience, minimize disruption, and maintain essential services during cyber incidents or geopolitical crises.

Pdf: CI Fortify — Advice for isolating vital system

Source and more information:

CI Fortify – Advice for isolating vital systems | CISA

2. Critical systems security conferences

In September 2026, the following ICS/SCADA/OT security conferences and workshops will be organized (not comprehensive):

Industrial AI Summit 2026

The Industrial AI Summit 2026 is a free, two-day virtual conference hosted by IIoT World on September 9-10, 2026. The event features live interactive panels on agentic and physical AI in manufacturing, AI-powered energy management, edge AI and small language models, digital twins, cybersecurity for AI-connected operations, and measurable AI ROI. Speakers include practitioners deploying AI across discrete manufacturing, process industries, automotive, and energy. Registration is free for CDOs, CIOs, CTOs, VPs of IT/OT and automation, plant managers, data engineers, IoT architects, and technology leaders across manufacturing and industrial operations.

Virtual; 9th – 10th September 2026

More details can be found on the following website:

Industrial AI Summit 2026 | IIoT World

Kaspersky Industrial Cybersecurity Conference 2026

Kaspersky Industrial Cybersecurity Conference brings together OT cybersecurity practitioners, vendors and customers from all over the world. We invite you to discuss key ICS/OT cybersecurity issues, share experiences, benefit from unique content and case studies, and learn the cutting-edge approaches to securing industrial automation systems and infrastructures.

Sochi, Russia; 9th – 11th September 2026

More details can be found on the following website:

Kaspersky Industrial Cybersecurity Conference 2026

CS4CA

Europe faces a volatile cyber landscape shaped by intensifying geopolitical tensions and the rapid adoption of AI by attackers. Nevertheless, European organisations are still reluctant to give OT Security the resources necessary, with 44% of European organisations fearing that deploying cyber security tools will negatively impact system performance.

While frameworks like NIS2 set a high bar, many organisations still struggle with complex governance, unmanaged remote access, and the persistent vulnerabilities of legacy systems. From state-sponsored campaigns to ransomware targeting industrial control systems, the risk is escalating, demanding deeper collaboration and stronger industry alignment.

In response, CS4CA Europe 2026 focuses on "Building Intelligence-Driven IT/ OT Resilience in an Era of Increasing Risk" Our meticulously curated programme brings together senior security leaders from across Europe's critical sectors to tackle operational technology challenges head-on.

London, UK; 23rd – 24th September 2026

More details can be found on the following website:

CS4CA Europe: Cyber Security Summit | 23rd - 24th September 2026 | London, UK

3. Critical systems security incidents

Ransomware Attack Puts a Chill on Japanese Frozen-Food Chain

In late July, Nichirei Corporation, a major Japanese frozen-food supplier and logistics powerhouse, fell victim to a severe cyberattack that disrupted its core warehousing and shipping operations. As an enterprise operating 141 logistics centers and managing a fleet of approximately 7.000 refrigerated vehicles, Nichirei's system failure immediately rippled across its vast supply network, directly affecting nearly 5.000 commercial clients. Among the most prominent impacted customers was Kentucky Fried Chicken (KFC) in Japan, which was forced to warn consumers of potential product shortages and reduced operating hours at its nationwide franchises due to curtailed shipments.

To contain the threat, Nichirei took the strategic decision to sever its internal networks - a standard operational response designed to halt active encryption and prevent the lateral movement of malware across subnetworks. Following an emergency response in collaboration with an external cybersecurity firm, the company issued a statement on July 22 confirming that recovery efforts were underway, with all affected logistics and warehousing locations scheduled to return to normal operations within the week.

Responsibility for the attack was claimed by RansomHouse, a relatively new ransomware group known for utilizing double-extortion tactics. The threat actors reportedly exfiltrated sensitive data prior to encrypting systems and subsequently posted a subset of Nichirei's compromised data on the Dark Web. Nichirei officially acknowledged the breach and confirmed that personal data had been stolen, though the company refrained from disclosing deeper technical specifics while investigations remain ongoing alongside the police and relevant regulatory authorities.

This incident highlights the convergence of the top two cyber threats facing Japanese organizations today, as classified by the Information-technology Promotion Agency (IPA): ransomware infections and attacks targeting supply chains and subcontractors. According to survey data from the Japan Institute for the Promotion of Digital Economy and Community (JIPDEC), nearly half of all Japanese companies (46%) have experienced a ransomware attack.

The attack on Nichirei closely mirrors a major ransomware incident in October 2025 involving Japanese beverage titan Asahi. In that event - claimed by the Qilin ransomware group - shipments were disrupted for nearly two weeks, full recovery took months, the personal data of 1,9 million individuals was leaked, and Q4 revenues fell between 10% and 30% across various divisions.

Cybersecurity experts emphasize that the Nichirei incident exposes the inherent vulnerabilities of Japan's hyper-efficient, "just-in-time" procurement and delivery model. Because logistics ecosystems operate with minimal buffer inventory, even a brief 48-hour network freeze can instantly trigger empty retail shelves and stock-outs at major food chains.

Furthermore, security analysts stress that while regulatory frameworks - such as Japan’s Active Cyber Defense Actm - mandate incident reporting and grant government authority to assist in server shutdowns, organizations cannot rely solely on policy compliance. True resilience requires routine ransomware recovery exercises and the ability to maintain manual

workarounds or air-gapped operational setups when primary IT infrastructure must be isolated.

The source is available at the following link:

Ransomware Attack Puts a Chill on Japanese Frozen-Food Chain

4. Book recommendation

ICS & SCADA Protection

ICS & SCADA Protection is a complete awareness and implementation guide that demystifies the world of industrial OT security.

Covering frameworks, ICS/SCADA risk management, manufacturing protection, and real-world case studies, this book empowers readers to secure critical infrastructure with confidence.

In today's connected world, power plants, transportation networks, and manufacturing systems face unprecedented digital challenges.

From factory floors to control rooms, every operation depends on reliable and protected OT environments.

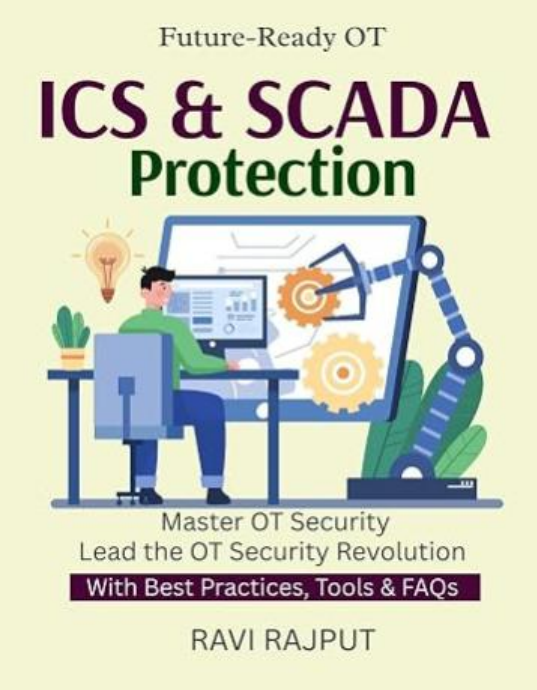
This book reveals why securing OT is not optional anymore but a necessity for resilience and growth.

Author/Editor: RAVI RAJPUT (Author)

Year of issue: 2025

The book is available at the following link:

[ICS & SCADA Protection: OT Security Frameworks | ICS/SCADA Risk Management | Protecting Manufacturing Systems | OT Cyber Incidents Explained | Real-World ... Security Cases | operational technology sec eBook : RAJPUT, RAVI: Amazon.in: Kindle Store]



5. Critical systems security news selection

Important articles dealing with critical infrastructure protection and industrial cybersecurity in August:

1. **Water Sector Cyberattacks Reportedly Hit at Least 12 States**
2. **New York Pours $9M Into Water Cyber Defense Amid Attacks**
3. **Congressional report warns Chinese telecoms remain embedded in US networks despite FCC restrictions**
4. **BitSight reports 56% decline in US internet-exposed ATG systems following critical infrastructure security warnings**
5. **Multistate Water System Attacks Widen, Iran Suspected**
6. **Ransomware gangs don't need control system access to disrupt industrial production**
7. **Why Critical Infrastructure Needs OT-Focused AI Security**
8. **Post-Quantum Deadlines Collide With OT Reality**
9. **CERT Polska exposes multi-stage cyberattack on energy infrastructure involving VPN, private APN, OT network tunnelling**
10. **Bridewell reports infostealer threat to UK critical infrastructure sector, as manufacturing takes 40% of victims**
11. **Acronis exposes Patchcord cyber espionage campaign targeting telecom and critical infrastructure in South Asia**
12. **Critical Infrastructure Needs a Unified Cyber Defense**
13. **New Jersey, Alabama Join States Targeted in Water Cyberattacks**
14. **Rush to Build Data Centers Leaves OT Security Behind**
15. **A Baffling Case of Inept Iranian Strikes on Water Utilities**
16. **Hackers Using AI to Target Siemens PLCs in Critical US Sectors**
17. **Senators introduce bipartisan Quantum-GUARD Act to boost US electric grid against emerging quantum cyber threats**
18. **How an Emerging Industrial Protocol Family Could Put OT at Risk**
19. **UK Government Reticent Over Power Plant Hack**
20. **ARI urges Trump to designate AI as 'critical infrastructure' amid growing cyber risks across critical sectors**

21. **You Need Cyber Deception for OT**
22. **OpenAI-backed initiative targets critical infrastructure cyber gaps with AI-powered defenses, coordinated global response**

Water Sector Cyberattacks Reportedly Hit at Least 12 States

The number of US states affected by the recent hacking campaign targeting water and wastewater facilities continues to grow.

At least 12 states have been hit, according to ABC News, but the names of only a handful of the affected states are currently known

Minnesota was the first to report attacks, with more than 30 community water systems targeted on July 26 and 27. Michigan has also officially confirmed that a "small number" of communities have seen malicious cyber activity. …

Source and more information:

Water Sector Cyberattacks Reportedly Hit at Least 12 States - SecurityWeek

New York Pours $9M Into Water Cyber Defense Amid Attacks

New York is fast-tracking more than $9 million in cyber grants to its water utilities as hackers target and disrupt systems in a string of attacks across the country.

Gov. Kathy Hochul's office said Monday it was set to administer a series of statewide cybersecurity grants amid a series of targeted attacks (see: Hackers Disrupt Controls at Minnesota Water Utilities).

U.S. officials have not publicly attributed the campaign to any country or hacking group, though the series of water systems attacks has coincided with renewed U.S. and Iranian military strikes in the Middle East. …

Source and more information:

New York Pours $9M Into Water Cyber Defense Amid Attacks

Congressional report warns Chinese telecoms remain embedded in US networks despite FCC restrictions

Members of the Select Committee on China concluded that Chinese state-owned telecommunications carriers remain deeply embedded in the U.S. internet ecosystem despite federal actions restricting their operations, raising concerns that their continued presence could support future cyber activities linked to the Chinese Communist Party (CCP). The bipartisan investigation found that although the Federal Communications Commission (FCC) denied or revoked the Section 214 telecommunications licenses of China Mobile, China

Unicom, and China Telecom, the companies continue to maintain extensive, largely unregulated infrastructure and network relationships within the United States. …

Source and more information:

Congressional report warns Chinese telecoms remain embedded in US networks despite FCC restrictions - Industrial Cyber

BitSight reports 56% decline in US internet-exposed ATG systems following critical infrastructure security warnings

New research from Bitsight researchers found that internet-exposed automatic tank gauge (ATG) systems in the U.S. fell by more than half between March and June 2026, with exposed IP addresses dropping 56% from the March peak. The cybersecurity company said the decline followed a year of relatively stable exposure levels and coincided with industry advisories about attacks targeting internet-connected ATGs. Bitsight said its analysis indicates the reduction was largely genuine rather than the result of Internet scanning noise or changing IP addresses. …

Source and more information:

BitSight reports 56% decline in US internet-exposed ATG systems following critical infrastructure security warnings - Industrial Cyber

Multistate Water System Attacks Widen, Iran Suspected

Cyberattacks against water and wastewater systems reportedly have reached at least a dozen states, with threat actors exploiting low-complexity attacks against industrial controllers. The intrusions, possibly linked to the Iranian government, prove the US's water infrastructure remains dangerously exposed.

In recent weeks, water and wastewater organizations associated several US states have disclosed cyberattacks against their systems. Minnesota was the first to confirm such attacks late last month, saying that cyberattackers targeted operational technology (OT) systems for more than 30 water systems. Around the same time on July 30, the Cybersecurity and Infrastructure Security Agency (CISA) updated an earlier advisory warning of "a significant increase in cyber-threat actors targeting programmable logic controllers (PLCs) in the Water and Wastewater Systems (WWS) Sector." …

Source and more information:

Multistate Water System Attacks Widen, Iran Suspected

Ransomware gangs don't need control system access to disrupt industrial production

Disrupting IT systems that support industrial environments can be enough to interrupt production, even when ransomware operators do not gain direct access to industrial control systems (ICS), according to Dragos.

The company identified 1,140 ransomware incidents involving industrial organizations in the second quarter of 2026, up 12% from 1,020 in Q1. The figures come from publicly disclosed victim data and posts made by ransomware groups on their data leak sites. Manufacturing accounted for 747 incidents, or 65% of the total. ...

Source and more information:

Ransomware gangs don't need control system access to disrupt industrial production - Help Net Security

Why Critical Infrastructure Needs OT-Focused AI Security

Nation-state attackers are exploiting outdated operational technology and converged IT/OT infrastructure faster than operators can defend them. Claroty is countering this by launching a dedicated public sector arm and an artificial intelligence-native security agent built to protect OT environments.

Yaniv Vardi, CEO of Claroty, said recent attacks on water utilities, along with nation-state activity linked to Volt Typhoon and Salt Typhoon, underscore the lack of dedicated OT security services for the U.S. public sector, pushing the company to launch a dedicated public sector business focused on OT security. Public-sector environments carry different risk priorities, he said. ...

Source and more information:

Why Critical Infrastructure Needs OT-Focused AI Security

Post-Quantum Deadlines Collide With OT Reality

Quantum-safe algorithms are here, but OT isn't ready to run them.

Post-quantum cryptography standards were released in August 2024 by the National Institute of Standards and Technology, and governments worldwide have followed with hard deadlines for critical infrastructure operators to adopt them - mostly between 2028 and 2030. Nearly all critical infrastructure - power grids, water systems and transportation networks - rely on operational technology systems and outdated remote terminal units such as SCADA platforms and PLCs, and that legacy infrastructure could be a problem. ...

Source and more information:

Post-Quantum Deadlines Collide With OT Reality

CERT Polska exposes multi-stage cyberattack on energy infrastructure involving VPN, private APN, OT network tunneling

CERT Polska has disclosed the first purely destructive cyberattack on Poland's energy sector and revealed it was far more complex than initially understood. A newly published report supplement details a second, previously undisclosed assault on a combined heat and power (CHP) plant that occurred in the same campaign. The three-month investigation uncovered a novel attack vector involving a private APN, marking an escalation in the sophistication of threats to the country's critical infrastructure. …

Source and more information:

CERT Polska exposes multi-stage cyberattack on energy infrastructure involving VPN, private APN, OT network tunneling - Industrial Cyber

Bridewell reports infostealer threat to UK critical infrastructure sector, as manufacturing takes 40% of victims

New data from Bridewell's BCON Collective identified confirmed infostealer exposure at 10 U.K. critical national infrastructure (CNI) organizations across five sectors during the second quarter of 2026, with 13 distinct stealer families recorded. The analysis found about 1,400 credential-set detections, with Unknown Stealer accounting for 20.5% of detections. Only two of the 10 victims had a specific stealer family attributed, while the remaining eight were classified as having confirmed exposure without a published family breakdown. Manufacturing was the hardest-hit CNI sector, accounting for 40% of victims. …

Source and more information:

Bridewell reports infostealer threat to UK critical infrastructure sector, as manufacturing takes 40% of victims - Industrial Cyber

Acronis exposes Patchcord cyber espionage campaign targeting telecom and critical infrastructure in South Asia

New data from Acronis Threat Research Unit identified an ongoing campaign targeting Afghan telecommunications providers and critical infrastructure organizations in South Asia with a previously undocumented custom backdoor tracked as Patchcord. The malware is delivered through sector-specific lures, including fake VPN installers impersonating Afghan Telecom and telecom management tools. …

Source and more information:

Acronis exposes Patchcord cyber espionage campaign targeting telecom and critical infrastructure in South Asia - Industrial Cyber

Critical Infrastructure Needs a Unified Cyber Defense

Critical infrastructure operators face cyberthreats that cross sector boundaries, making isolated defense strategies less effective, said Tom Fanning, chair of the executive committee for the Alliance for Critical Infrastructure and former CEO and executive chairman at Southern Company.

Energy, finance, communications, transportation and water systems need a common operating picture and shared accountability for national security. Fanning says the key to success will be "getting the sectors to talk with each other as a private sector, and then collaborating - not coordinating, not cooperating, not sharing - but collaborating." ...

Source and more information:

Critical Infrastructure Needs a Unified Cyber Defense

New Jersey, Alabama Join States Targeted in Water Cyberattacks

New Jersey and Alabama have joined the list of US states that confirmed their water and wastewater facilities have been targeted in a hacking campaign that started in late July.

At least 12 states have reportedly been hit, but not all have been identified. Minnesota was the first to confirm that over 30 water systems had their operational technology (OT) systems targeted.

Michigan, South Dakota, and Georgia later also confirmed being targeted.

The latest to join the list are New Jersey and Alabama. In New Jersey, Cape May and Woodbine water systems were targeted in cyberattacks on July 27, but officials said only phone systems were disrupted, according to Fox29. ...

Source and more information:

New Jersey, Alabama Join States Targeted in Water Cyberattacks - SecurityWeek

Rush to Build Data Centers Leaves OT Security Behind

In the rush to get servers on the ground, and new compute up and running, especially to cater to the artificial intelligence boom, data center owners have neglected security and left vulnerable operational technology devices dangerously close to the public internet, according to experts and recent research.

Total U.S. capital expenditure on data centers is expected to top $700 billion this year, according to Moody's Investor Services, as tech giants and their smaller rivals race to power ever larger and more complex large language models and meet the predicted mushrooming demand from business. Over the next five years, predicts market intelligence firm Industrial Info Resources, data center developers and big tech firms plan to start construction on 2,913 data centers at a cost of about $2.4 trillion by 2030. ...

Source and more information:

Rush to Build Data Centers Leaves OT Security Behind

A Baffling Case of Inept Iranian Strikes on Water Utilities

More than three weeks after a wave of cyberattacks struck dozens of rural and small town water and wastewater utilities in at least 12 states, experts are still trying to figure out what exactly the attackers thought they were doing.

The hackers, widely believed to be from a group aligned with Iran's Islamic Revolutionary Guard Corps, had the keys to the kingdom for those utilities, said Josh Corman. An executive in residence for public safety and resilience at the Institute for Security and Technology, Corman is the founder of I Am The Cavalry, one of the earliest cybersecurity community activities aimed at helping secure America's vital facilities. …

Source and more information:

A Baffling Case of Inept Iranian Strikes on Water Utilities

Hackers Using AI to Target Siemens PLCs in Critical US Sectors

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).

According to the NSA, CISA, FBI, EPA, and DOE, the hackers are scanning the internet to identify exposed PLCs and developing exploits that could cause serious disruption to industrial processes. Other potential impacts include equipment damage, safety incidents affecting workers, compromise of sensitive data, and cascading effects on supply chains, associated facilities, and business operations. …

Source and more information:

Hackers Using AI to Target Siemens PLCs in Critical US Sectors - SecurityWeek

Senators introduce bipartisan Quantum-GUARD Act to boost US electric grid against emerging quantum cyber threats

Two U.S. Senators introduced bipartisan legislation aimed at strengthening the electric grid against cybersecurity threats from advancing quantum computing. The Quantum Grid Utility Assurance and Resilient Defense Act of 2026, or Quantum-GUARD Act, would direct federal agencies to assess quantum-related cybersecurity vulnerabilities, help electric utilities transition to post-quantum cryptography and improve coordination among grid operators, cybersecurity experts and government partners. …

Source and more information:

Senators introduce bipartisan Quantum-GUARD Act to boost US electric grid against emerging quantum cyber threats - Industrial Cyber

How an Emerging Industrial Protocol Family Could Put OT at Risk

In operational technology (OT) networking, the reliability and availability of industrial processes trumps everything, even cybersecurity. But what happens when an OT networking protocol designed to ensure speedy availability of safety-critical communications also embeds a security weakness into the architecture?

Without a full slate of cyber controls folded in, that reliability mechanism could itself become a vehicle for the kinds of industrial failures it's supposed to help prevent. ...

Source and more information:

How an Emerging Industrial Protocol Family Could Put OT at Risk

UK Government Reticent Over Power Plant Hack

Operational technology security leaders are calling on the British government to release technical details of a cyberattack last month that took a small power plant offline for four days.

So far, the government's public statements have "been very limited, and hopefully, we'll find out more soon," Markus Mueller, field CISO at operational technology security company Nozomi Networks, told ISMG.

The British government should follow the example of the Polish national Computer Emergency Response Team, which published a comprehensive technical breakdown of last year's three-pronged attack on the Polish energy grid, attributed to Russian hackers. ...

Source and more information:

UK Government Reticent Over Power Plant Hack - OTToday

ARI urges Trump to designate AI as 'critical infrastructure' amid growing cyber risks across critical sectors

Americans for Responsible Innovation (ARI) released a report warning that the growing integration of artificial intelligence across health care, finance and manufacturing creates infrastructure vulnerabilities that could have sector-wide consequences if attacked. It identifies that voluntary corporate security measures are insufficient as reliance on AI expands across private and public sectors. Furthermore, the report recommends that U.S. President Donald Trump designate AI as critical infrastructure, subjecting the sector to incident reporting requirements. It also calls for the Cybersecurity and Infrastructure Security Agency (CISA) and the Center for AI Standards and Innovation (CAISI) to coordinate on security standards covering the AI infrastructure stack. ...

Source and more information:

ARI urges Trump to designate AI as 'critical infrastructure' amid growing cyber risks across critical sectors - Industrial Cyber

You Need Cyber Deception for OT

There are three statements that sum up the frustrating reality for defenders responding to a cyberattack on operational technology (OT) systems: The attack data is not there. There is no trail to follow. There is no history to sort through.

While these dynamics will always be true for OT, defenders are getting help from cyber deception as it matures beyond honeypots to a more sophisticated, proactive cyber-defense tool. …

Source and more information:

You Need Cyber Deception for OT

OpenAI-backed initiative targets critical infrastructure cyber gaps with AI-powered defenses, coordinated global response

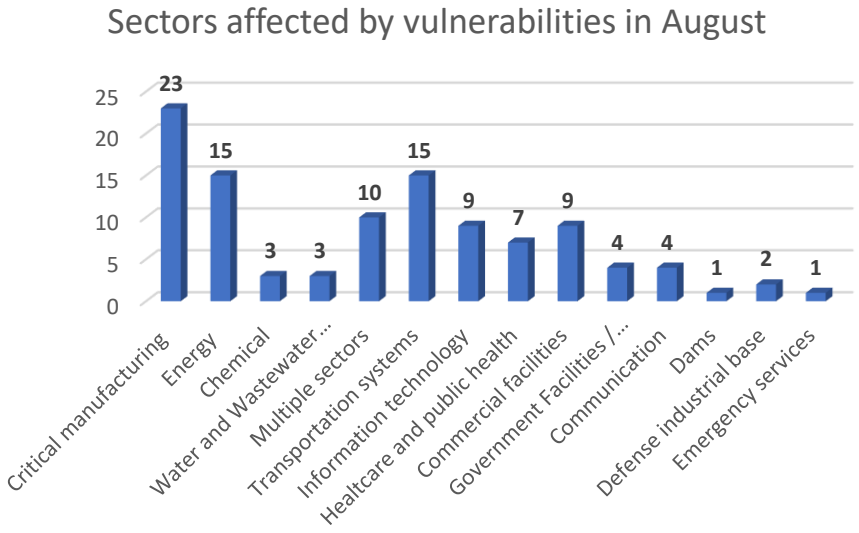
OpenAI and a broad group of technology and cybersecurity organizations are launching a collective cyber defense initiative calling for coordinated global efforts to protect essential services, including hospitals, water treatment plants, and internet infrastructure, against increasingly sophisticated AI-enabled attacks. While these organizations face growing risks, longstanding vulnerabilities such as unpatched software, misconfigurations, weak authentication, and legacy technical debt continue to leave systems exposed. …

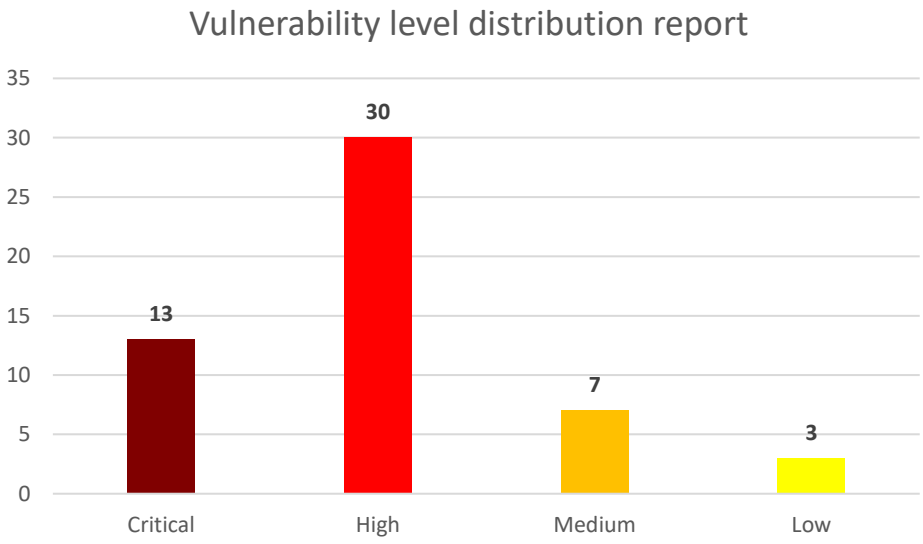
Source and more information:

OpenAI-backed initiative targets critical infrastructure cyber gaps with AI-powered defenses, coordinated global response - Industrial Cyber

6. Critical systems vulnerabilities

In August 2026, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT and Siemens ProductCERT and Siemens CERT:





ICSA-25-128-03: **Mitsubishi Electric Multiple FA Products (Update D)**

High level vulnerability: Improper Validation of Specified Quantity in Input.

Mitsubishi Electric Multiple FA Products (Update D) | CISA

ICSA-26-078-05: **Mitsubishi Electric CNC Series (Update A)**

Medium level vulnerabilities: Improper Validation of Specified Index, Position, or Offset in Input.

Mitsubishi Electric CNC Series (Update A) | CISA

ICSA-26-239-01: **Xiiaozet LK100W**

Critical level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Missing Authentication for Critical Function, Authentication Bypass Using an Alternate Path or Channel.

Xiiaozet LK100W | CISA

ICSA-26-239-02: **All-Line Equipment Company Fuel-Boss**

High level vulnerabilities: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection'), Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').

All-Line Equipment Company Fuel-Boss | CISA

ICSA-26-239-03: **Rockwell Automation OTTO Fleet Manager**

Medium level vulnerability: Use of Password Hash With Insufficient Computational Effort.

Rockwell Automation OTTO Fleet Manager | CISA

ICSA-26-239-04: **Applied Systems Engineering ASE2000 V2 Communications Test Set**

Critical level vulnerabilities: Improper Restriction of XML External Entity Reference, Improper Certificate Validation.

Applied Systems Engineering ASE2000 V2 Communications Test Set | CISA

ICSA-26-239-05: **Ebyte NA111-M**

Critical level vulnerabilities: Missing Authentication for Critical Function, Use of GET Request Method With Sensitive Query Strings, Cross-Site Request Forgery (CSRF), Improper Restriction of Excessive Authentication Attempts, Missing Authorization, Cleartext Transmission of Sensitive Information, Use of Client-Side Authentication, Improper Restriction of Rendered UI Layers or Frames, Use of a Broken or Risky Cryptographic Algorithm, Weak Authentication, Cleartext Storage of Sensitive Information.

Ebyte NA111-M | CISA

ICSA-25-070-02: **Optigo Networks Visual BACnet Capture Tool/Optigo Visual Networks Capture Tool (Update A)**

Critical level vulnerabilities: Use of Hard-coded, Security-relevant Constants, Authentication Bypass Using an Alternate Path or Channel.

Optigo Networks Visual BACnet Capture Tool/Optigo Visual Networks Capture Tool (Update A) | CISA

ICSA-26-069-02: **Lantronix EDS3000PS and EDS5000 (Update A)**

Critical level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Authentication Bypass Using an Alternate Path or Channel, Unverified Password Change.

Lantronix EDS3000PS and EDS5000 (Update A) | CISA

ICSA-26-237-01: **Rently Smart Home**

High level vulnerability: Insufficiently Protected Credentials.

Rently Smart Home | CISA

ICSA-26-237-02: **Zoneminder**

High level vulnerability: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').

Zoneminder | CISA

ICSA-26-237-03: **Siemens SIMATIC IoT2050 Advanced**

Critical level vulnerability: Missing Authentication for Critical Function.

Siemens SIMATIC IoT2050 Advanced | CISA

ICSA-26-237-04: **PayRange API**

High level vulnerability: Missing Authorization.

PayRange API | CISA

ICSA-26-237-05: **Bendix EC80 Brake ECU**

High level vulnerabilities: Stack-based Buffer Overflow, Out-of-bounds Write, Use of Hard-coded Credentials.

Bendix EC80 Brake ECU | CISA

ICSA-26-237-06: **Ebyte NE2-D11**

Critical level vulnerabilities: Missing Authentication for Critical Function, Cleartext Transmission of Sensitive Information, Insufficiently Protected Credentials, Use of Client-Side Authentication, Use of GET Request Method With Sensitive Query Strings, Cross-Site Request Forgery (CSRF), Improper Restriction of Excessive Authentication Attempts, Improper Restriction of Rendered UI Layers or Frames, Missing Authorization.

Ebyte NE2-D11 | CISA

ICSA-26-237-07: **Furuno FA-50 Class B AIS Transponder**

Critical level vulnerability: Use of Hard-coded Credentials, Missing Authentication for Critical Function.

FURUNO FA-50 Class B AIS Transponder | CISA

ICSA-26-232-01: **Johnson Controls Simplex Incident Manager**

Medium level vulnerability: Cleartext Storage of Sensitive Information in Memory.

Johnson Controls Simplex Incident Manager | CISA

ICSA-26-230-01: **CISA Malcolm**

High level vulnerabilities: Allocation of Resources Without Limits or Throttling, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Unrestricted Upload of File with Dangerous Type, Incorrect Authorization, Improper Handling of Highly Compressed Data (Data Amplification).

CISA Malcolm | CISA

ICSA-26-230-02: **Siemens Simcenter Nastran**

High level vulnerability: Stack-based Buffer Overflow.

Siemens Simcenter Nastran | CISA

SSA-069220: **Stack Overflow Vulnerability in Simcenter Nastran Before V2606 (Update: 1.1.)** **High** level vulnerability: Stack-based Buffer Overflow.

SSA-069220

SSA-864900: **Multiple Vulnerabilities in Fortigate NGFW on RUGGEDCOM APE1808 Devices (Update: 2.0.)**

High level vulnerabilities: Multiple.

SSA-864900

SSA-827968: **Vulnerability in Nozomi Guardian/CMC Before V26.2.0 on RUGGEDCOM APE1808 Devices (Update: 1.4.)**

High level vulnerabilities: Multiple.

SSA-827968

SSA-686975: **IPU 2022.3 Vulnerabilities in Siemens Industrial Products using Intel CPUs (Update: 1.7.)**

High level vulnerability: Time-of-check Time-of-use (TOCTOU) Race Condition.

SSA-686975

SSA-628843: **Out of Bound Read Vulnerability in TPM 2.0 (Update: 1.1.)**

Medium level vulnerability: Out-of-bounds Read.

SSA-628843

SSA-434797: **Buffer Overflow Vulnerability in OpenSSL affecting Siemens Products (Update: 1.2.)**

High level vulnerability: Out-of-bounds Write.

SSA-434797

SSA-392349: **Denial of Service Vulnerability in Industrial Devices (Update: 1.2.)**

High level vulnerability: NULL Pointer Dereference.

SSA-392349

SSA-306654: **Insyde BIOS Vulnerabilities in Siemens Industrial Products (Update: 2.0.)**

High level vulnerabilities: Multiple.

SSA-306654

SSA-282044: **DLL Hijacking Vulnerability in Siemens Web Installer used by the Online Software Delivery (Update: 1.8.)**

High level vulnerability: Uncontrolled Search Path Element.

SSA-282044

SSA-104023: **Multiple Vulnerabilities in Palo Alto Networks PAN-OS on RUGGEDCOM APE1808 Devices (Update: 1.1.)**

Critical level vulnerability: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Missing Authorization, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Incorrect Calculation of Buffer Size, Use of Cache Containing Sensitive Information, Improper Input Validation, Missing Authentication for Critical Function, Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Server-Side Request Forgery (SSRF), Improper Check for Unusual or Exceptional Conditions, Out-of-bounds Write.

SSA-104023

ICSA-26-225-01: **AVEVA Enterprise SCADA**

High level vulnerability: Deserialization of Untrusted Data.

AVEVA Enterprise SCADA | CISA

ICSA-26-225-02: **Haiwell IoT Cloud HMI Gateway**

Critical level vulnerability: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').

Haiwell IoT Cloud HMI Gateway | CISA

ICSA-26-225-03: **Johnson Controls Inc. Airwall**

Medium level vulnerabilities: Use of Hard-coded Cryptographic Key, External Control of File Name or Path.

Johnson Controls Inc. Airwall | CISA

ICSA-26-225-04: **Hitachi Energy APM Edge Product**

High level vulnerabilities: Write-what-where Condition, Out-of-bounds Write.

Hitachi Energy APM Edge Product | CISA

ICSA-26-225-05: **ANDRITZ HIPASE-250 and 250 SCALA**

High level vulnerabilities: Storing Passwords in a Recoverable Format, Missing Authentication for Critical Function, Use of Hard-coded Credentials.

ANDRITZ HIPASE-250 and 250 SCALA | CISA

ICSA-26-225-06: **Siemens RUGGEDCOM APE1808**

Medium level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

Siemens RUGGEDCOM APE1808 | CISA

ICSA-26-225-07: **Siemens License Server (SLS)**

High level vulnerability: Incorrect Permission Assignment for Critical Resource, Path Traversal: '.../...//'.

Siemens License Server (SLS) | CISA

ICSA-26-225-08: **Siemens Desigo DXR and PXC Controllers**

Low level vulnerability: Improper Check for Unusual or Exceptional Conditions.

Siemens Desigo DXR and PXC Controllers | CISA

ICSA-26-225-09: **Siemens Siveillance Video**

Critical level vulnerability: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').

Siemens Siveillance Video | CISA

ICSA-26-225-10: **Siemens Parasolid**

High level vulnerability: Out-of-bounds Read.

Siemens Parasolid | CISA

ICSA-26-225-11: **Siemens Simcenter Femap**

High level vulnerability: Out-of-bounds Read.

Siemens Simcenter Femap | CISA

ICSA-26-225-12: **Siemens Solid Edge**

High level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write, Use After Free.

Siemens Solid Edge | CISA

ICSA-26-225-13: **Siemens LOGO! Soft Comfort**

Medium level vulnerabilities: Use of Hard-coded Cryptographic Key, Use of a One-Way Hash without a Salt.

Siemens LOGO! Soft Comfort | CISA

ICSA-26-225-14: **Johnson Controls Metasys**

High level vulnerability: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

Johnson Controls Metasys | CISA

ICSMA-26-223-01: **Mira Hormone Monitor, Mira Android App**

Critical level vulnerabilities: Missing Authentication for Critical Function, Authentication Bypass by Spoofing, Use of Hard-coded Credentials, Weak Authentication, Improper Restriction of Excessive Authentication Attempts, Reliance on Untrusted Inputs in a Security Decision, Use of GET Request Method With Sensitive Query Strings.

Mira Hormone Monitor, Mira Android App | CISA

ICSMA-26-223-02: **Pulsetto Vagus Nerve Stimulator**

High level vulnerability: Hidden Functionality.

Pulsetto Vagus Nerve Stimulator | CISA

ICSA-26-204-01: **Johnson Controls C-CURE 9000 and Victor application server (Update A)** **Critical** level vulnerabilities: Server-Side Request Forgery (SSRF), Execution with Unnecessary Privileges.

Johnson Controls C-CURE 9000 and Victor application server (Update A) | CISA

ICSA-26-219-01: **CPDLC over ATN-B1 Vulnerabilities**

High level vulnerabilities: Missing Authentication for Critical Function, Allocation of Resources Without Limits or Throttling, Improper Check for Unusual or Exceptional Conditions.

CPDLC over ATN-B1 Vulnerabilities | CISA

ICSMA-26-218-01: **Medixant RadiAnt DICOM Viewer**

Low level vulnerability: Out-of-bounds Write.

Medixant RadiAnt DICOM | CISA

ICSA-26-218-01: **ABB Ability Zenon**

High level vulnerabilities: Improper Handling of Length Parameter Inconsistency, Improper Neutralization of Null Byte or NUL Character, Collapse of Data into Unsafe Value,

Undefined Behavior for Input to API, Incorrect Regular Expression, Uncaught Exception, Reachable Assertion, Allocation of Resources Without Limits or Throttling, Out-of-bounds Write, Improper Output Neutralization for Logs, Improper Certificate Validation, Execution with Unnecessary Privileges.

ABB Ability Zenon | CISA

ICSA-26-218-02: **Johnson Controls TLS280**

Low level vulnerability: Use of a Broken or Risky Cryptographic Algorithm.

Johnson Controls Inc. TL280 | CISA

ICSA-26-216-01: **Acrisure Karr Anti-theft**

High level vulnerability: Use of Hard-coded Cryptographic Key.

Acrisure KARR BT and DR-100 | CISA

ICSMA-26-216-01: **Thermo Fisher Applied Biosystems 3100 and 3500 Series Genetic Analyzers**

High level vulnerability: Missing Support for Integrity Check.

Thermo Fisher Applied Biosystems Genetic Analyzers | CISA

The vulnerability reports contain more detailed information, which can be found on the following websites:

ICS Advisories | CISA

Cybersecurity Alerts & Advisories | CISA

CERT Services | Services | Siemens Siemens global website

Continuous monitoring of vulnerabilities is recommended, because relevant information on how to address vulnerabilities, patch vulnerabilities and mitigate risks are also included in the detailed descriptions.

7. Critical systems security alerts

CISA has published alerts in 2026 August:

CISA Adds Known Exploited Vulnerabilities to Catalog

CVE-2026-18577 N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability;
CVE-2026-9198 IBM Langflow Code Injection Vulnerability;
CVE-2026-18556 N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability;
CVE-2026-34486 Apache Tomcat Missing Encryption of Sensitive Data Vulnerability;
CVE-2026-63077 JetBrains TeamCity Deserialization of Untrusted Data Vulnerability;
CVE-2026-8037 Progress LoadMaster Command Injection Vulnerability;
CVE-2026-20349 Cisco Secure Firewall Adaptive Security Appliance (ASA) and Firewall Threat Defense (FTD) Heap Inspection Vulnerability;
CVE-2026-68820 Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability;
CVE-2026-72898 Metabase SQL Injection Vulnerability;
CVE-2025-62593 Ray-Project Ray Code Injection Vulnerability;
CVE-2026-33824 Microsoft Internet Key Exchange (IKE) Service Extensions Double Free Vulnerability;
CVE-2026-55040 Microsoft SharePoint Weak Authentication Vulnerability;
CVE-2026-59310 Broadcom VMware vCenter Path Traversal Vulnerability;
CVE-2026-65400 Apple macOS Improper Authentication Vulnerability;
CVE-2026-64849 MLflow Server-Side Request Forgery Vulnerability;
CVE-2026-72529 TrueConf Server Missing Authentication for Critical Function Vulnerability;
CVE-2026-72530 TrueConf Server Code Injection Vulnerability;
CVE-2026-73570 Zimbra Collaboration Suite (ZCS) OS Command Injection Vulnerability;
CVE-2026-21962 Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in Improper Access Control Vulnerability;
CVE-2026-60004 Gitea Code Injection Vulnerability;
CVE-2015-3246 Red Hat Libuser Race Condition Vulnerability;
CVE-2015-5287 Red Hat Automatic Bug Reporting Tool Privilege Escalation Vulnerability;
CVE-2019-1068 Microsoft SQL Server Remote Code Execution Vulnerability;
CVE-2021-23758 Ajax.NET Professional Deserialization of Untrusted Data Vulnerability;
CVE-2022-0995 Linux Kernel Out-of-Bounds Write Vulnerability;
CVE-2026-8452 Citrix NetScaler ADC and NetScaler Gateway Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability;
CVE-2023-49105 ownCloud Improper Authentication Vulnerability;
CVE-2026-53362 Linux Kernel Unspecified Vulnerability;

CVE-2026-66384 JFrog Artifactory Improper Limitation of a Pathname to a Restricted Directory Vulnerability;

Links and more information:

CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Six Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA

8. Critical systems security trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in September 2026:

- Internet of Things (IoT) Practitioner (Exam ITP-110)
- Internet of Things (IoT) Security (Exam ITS-110)

Coursera | Online Courses From Top Universities. Join for Free

- Industrial Control Systems Cybersecurity (Virtual)(ICS300)
- Industrial Control Systems Evaluation (Virtual)(401V)
- ICS Cybersecurity & RED-BLUE Exercise (In-Person)(ICS301)
- Industrial Control Systems Evaluation (In-Person)(401L)
- Introduction to Control Systems Cybersecurity (In-Person)(101)
- Intermediate Cybersecurity for Industrial Control Systems (201), (202)

ICS Training Available Through CISA | CISA

- Operational Security (OPSEC) for Control Systems (100W)
- Differences in Deployments of ICS (210W-1)
- Influence of Common IT Components on ICS (210W-2)
- Common ICS Components (210W-3)
- Cybersecurity within IT & ICS Domains (210W-4)
- Cybersecurity Risk (210W-5)
- Current Trends (Threat) (210W-6)
- Current Trends (Vulnerabilities) (210W-7)
- Determining the Impacts of a Cybersecurity Incident (210W-8)
- Attack Methodologies in IT & ICS (210W-9)
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10)
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11)
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115)
- ICS410: ICS/SCADA Security Essentials
- ICS515: ICS Active Defense and Incident Response

ICS410: ICS/SCADA Security Essentials | SANS Institute

- ICS/SCADA Cyber Security
- Fundamentals of OT Cybersecurity (ICS/SCADA)
- An Introduction to the DNP3 SCADA Communications Protocol
- Learn SCADA from Scratch - Design, Program and Interface

ICS/SCADA Cyber Security

- SCADA security training

SCADA Security Training | SCADA Security Training Course

- Fundamentals of Industrial Control System Cyber Security
- Ethical Hacking for Industrial Control Systems

https://scadahacker.com/training.html

- INFOSEC-Flex SCADA/ICS Security Training Boot Camp

ICSP Training Boot Camp (OT/ICS Certified Security Professional) | Infosec

- Industrial Control System (ICS) & SCADA Cyber Security Training

Industrial Control System and SCADA Cybersecurity Training - Tonex Training

- Bsigroup: Certified Lead SCADA Security Professional training course

ISA/IEC 62443 Training for Product and System Manufacturers | UL Solutions

- The Industrial Cyber Security Certification Course

Certified Industrial Cybersecurity Professional Certification | CICP Course

- Secure IACS by ISA-IEC 62443 Standard

Secure IACS by ISA-IEC 62443 Standard

- Dragos Academy ICS/OT Cybersecurity Training

https://www.dragos.com/dragos-academy/#on-demand-courses

- ISA/IEC 62443 Training for Product and System Manufacturers

ISA/IEC 62443 Training for Product and System Manufacturers | UL Solutions

- ICS/SCADA/OT Protocol Traffic Analysis: IEC 60870-5-104

ICS/SCADA/OT Protocol Traffic Analysis: IEC 60870-5-104

- ICS/OT Cyber ICS/OT Cybersecurity as per NIST 800-82 Updated - Part1

ICS/OT Cybersecurity as per NIST 800-82 Updated - Part1

- Lead SCADA Security Manager

Lead SCADA Security Manager | PECB

- OT/IT Security Training

https://www.infosectrain.com/operational-technology-ot-training-courses/#courses

- OT Railway Cybersecurity (OTCS)

OT Railway Cybersecurity (OTCS) Training - Informa Academy

- OT Security Expert (*Master OT/ICS security essentials for protecting critical infrastructure in the digital era*)

OT Security Expert - OPSWAT Academy

- CTR-008 - OT-Security Awareness E-Learning Course

CTR-008 - OT-Security Awareness E-Learning Course | Yokogawa Europe

- Comprehensive Guide to Industrial Cybersecurity with IEC 62443-3 Standards

Comprehensive Guide to Industrial Cybersecurity with IEC 62443-3 Standards | EC-Council Learning

- Cybersecurity for Industrial Automation (ICS/SCADA) and OT

https://www.imfacademy.com/security-management/ot-cybersecurity.php

- Operational Technology (OT) Security Learning Path

Infosec's Operational Technology (OT) Security Learning Path

9. Critical systems security podcasts

People listen more and more podcasts nowadays. Whether it's for our personal interests or for our professional development, the world of podcasts is a great possibility to be well informed. In this section, we bring together the ICS security podcasts from the previous month.

Dale Peterson

This podcast is named after and made by one of the most famous ICS security expert, Dale Peterson. It's made on Wednesdays on every week and the usual structure contains an opening monologue, interviews with guests and listener questions on topics that are on the leading, or even bleeding edge of OT and ICS security. The podcast is also interactive, so the listeners could ask question from Dale and the guests.

You can find all of Peterson's podcasts on the below URL.

Link: https://dale-peterson.com/podcast-2/

Industrial Cybersecurity Pulse

This podcast is discussing major industrial cybersecurity topics and features industry experts covering everything from ransomware through critical infrastructure to supply chain attacks. Tune in to stay on top of the latest cybersecurity trends, threats and tactics. Hosted by Gary Cohen and Tyler Wall.

Link: https://www.industrialcybersecuritypulse.com/ics-podcast/

BEERISAC: OT/ICS Security Podcast Playlist

A curated playlist of Operational Technology and ICS Cyber Security related podcast episodes by ICS Security enthusiasts.

At this link, you can find numerous podcasts on the topic of ICS (Industrial Control Systems) created by various content producers. It's worth browsing through and listening to podcasts that are of interest to the organization or the readers of this newsletter themselves.

Link: https://www.iheart.com/podcast/256-beerisac-ot-ics-security-p-43087446/