BLACK CELL
Protecting critical infrastructures

Industrial Control Systems security feed

2026 February

2026 February, Industrial Control Systems security feed

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

List of Contents

1. ICS good practices, recommendations

CISA introduces POEM framework to strengthen insider threat mitigation across critical infrastructure

Critical infrastructure organizations should establish a formal, multidisciplinary insider threat management team integrated into existing security, HR, legal, and operational functions rather than operating in isolation.

Following CISA’s POEM model, organizations should first plan by identifying critical assets (including ICS/OT systems), defining insider threat scenarios, and aligning the program with organizational risk tolerance. The team should be properly organized with clear roles, legal and privacy safeguards, and secure handling of sensitive information.

Execution should focus on fostering a culture of reporting without fear of retaliation, correlating data from technical logs, access records, and HR sources, and ensuring mandatory training and structured assessment processes. Insider threat programs must address both malicious and unintentional risks, supported by least privilege access, monitoring of high-risk roles, and early intervention mechanisms.

To remain effective, the capability should be continuously maintained through regular reviews, exercises, policy updates, and integration into new technologies and business changes. Strong confidentiality controls and legal oversight are essential, as insider threat programs handle highly sensitive information. A mature, cross-functional approach strengthens organizational resilience, reduces the likelihood and impact of disruption, and improves protection of critical operations, people, and sensitive data.

Source and links and more information:

CISA introduces POEM framework to strengthen insider threat mitigation across critical infrastructure - Industrial Cyber

2. ICS conferences

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

CS4CA 2026

Industrial Defender is thrilled to return to CS4CA this year! The Cyber Security for Critical Assets Summit brings together senior cybersecurity leaders from across US critical infrastructure, for 2-days of in-depth knowledge exchange, strategy planning and insight building.

Be sure to visit our booth to learn how deeper OT asset data enables maturity in cybersecurity for resilience, safety, and performance.

Houston, Texas, USA; 10th – 11th March 2026

More details can be found on the following website:

https://www.industrialdefender.com/events/cs4ca-2026

2026 Pacific Operational Science & Technology (POST) Conference

Industrial Defender is back for the 2026 Pacific Operational Science & Technology (POST) Conference. Our team will be exhibiting at the event with more than 60 industry companies showcasing their cutting-edge technologies and services. Explore the latest advancements, witness groundbreaking demonstrations, and engage in thought-provoking conversations with the brightest minds in the industry.

Stop by our booth or book a meeting with our team. We look forward to connecting with you about OT security.

Honolulu, HI; 9th – 12th March 2026

More details can be found on the following website:

https://www.industrialdefender.com/events/2026-pacific-operational-science-technology-post-conference

Scada Security Conference 2026

The Scada Security Conference, held at the Police Academy in Prague, Czech Republic, serves as a pivotal gathering for experts and leaders in the field of civil security and cyber defense. This event, part of the FUTURE FORCES FORUM, emphasizes global networking and innovation in security solutions. Attendees can expect a range of keynote speeches and presentations from prominent figures, including the President of the Czech Republic, the Prime Minister, and the Minister of the Interior, among other key officials. Their insights will cover critical topics related to national security, cyber resilience, and advancements in defense technologies.

The conference will feature several notable components, including the Future of Civil Security Conference, the Future of Cyber Live Hacking Zone, and the Future Forces Exhibition & Forum. Additionally, the event will recognize cutting-edge developments through the Innovation Awards. Participants can also engage in discussions around Multi Domain Advanced Robotic Systems, Homeland Security and Resilience, and the implications of Defence Interests in Space. With a focus on Disruptive Technologies and Security Innovations, the Scada Security Conference promises to be an integral platform for stakeholders in the security and defense sectors, shaping future strategies and collaborations.

Prague, Czech Republic; 25th March 2026

More details can be found on the following website:

https://10times.com/e1h1-8x0d-p9pf-f-scada-security-conference#google_vignette

3. ICS incidents

Romanian oil pipeline operator Conpet discloses cyberattack

Conpet S.A., Romania's national oil pipeline operator, reported a cyberattack that affected its corporate IT systems and resulted in the temporary unavailability of the company's website. The incident was detected early in February and publicly disclosed the following day. Conpet operates nearly 4,000 kilometers of oil pipelines transporting crude oil and petroleum derivatives to refineries across Romania.

According to the company, the cyberattack impacted only the corporate IT infrastructure. Operational technologies, including the SCADA and telecommunications systems supporting pipeline operations, were not affected. As a result, crude oil and fuel transportation through the National Oil Transport System continued without disruption, and contractual obligations were fulfilled as normal.

Conpet stated that incident response and system restoration activities are ongoing in cooperation with national cybersecurity authorities. The company has also notified the Directorate for Investigating Organized Crime and Terrorism (DIICOT) and filed a criminal complaint. At the time of reporting, the company's official website (www.conpet.ro) remained inaccessible.

Although Conpet has not disclosed the technical nature of the attack, the Qilin ransomware group has claimed responsibility and listed the company on its dark web leak site. The threat actor alleges the exfiltration of nearly 1 TB of data and published a limited set of internal documents as proof of compromise. These claims have not been independently verified by Conpet.

This incident follows a series of ransomware attacks targeting Romanian critical infrastructure and public sector organizations, including energy providers, water management authorities, and healthcare institutions. The Conpet case highlights the continued ransomware threat to corporate IT environments within critical infrastructure operators and the importance of effective IT–OT separation to prevent operational impact.

The source is available at the following link:

https://www.bleepingcomputer.com/news/security/romanian-oil-pipeline-operator-conpet-discloses-cyberattack-qilin-ransomware/

4. Book recommendation

Industrial Internet of Things Security

The industrial landscape is changing rapidly, and so is global society. This change is driven by the growing adoption of the Industrial Internet of Things (IIoT) and artificial intelligence (AI) technologies. IIoT and AI are transforming the way industrial engineering is done, enabling new levels of automation, productivity, and efficiency. However, as IIoT and AI become more pervasive in the industrial world, they also offer new security risks that must be addressed to ensure the reliability and safety of critical systems.

Industrial Internet of Things Security: Protecting AI-Enabled Engineering Systems in Cloud and Edge Environments provides a comprehensive guide to IIoT security, covering topics such as network architecture, risk management, data security, and compliance. It addresses the unique security challenges that the cloud and edge environments pose, providing practical guidance for securing IIoT networks in these contexts. It includes numerous real-world case studies and examples, providing readers with practical insights into how IIoT security and AI-enabled industrial engineering are being implemented in various industries. Best practices are emphasized for the readers to ensure the reliability, safety, and security of their systems while also learning the latest developments in IIoT security for AI-enabled industrial engineering systems in this rapidly evolving field.

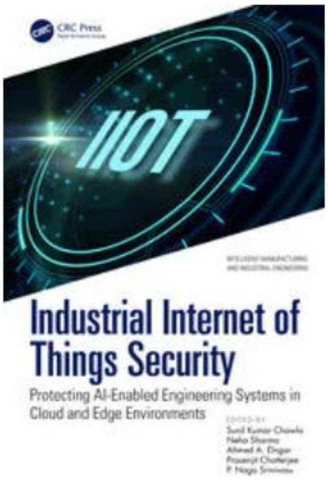
By offering step-by-step guidance for the implantation process along with best practices, this book becomes a valuable resource for practitioners and engineers in the areas of industrial engineering, IT, computer engineering, and anyone looking to secure their IIoT network against cyber threats.

Author/Editor: Sunil Kumar Chawla, Neha Sharma, Ahmed Elngar, Prasenjit Chatterjee, P. Naga Srinivasu

Year of issue: 2025

The book is available at the following link:

[Industrial Internet of Things Security: Protecting AI-Enabled Engineer]


CRC Press
IIOT
Industrial Internet of Things Security
Protecting AI-Enabled Engineering Systems in Cloud and Edge Environments
Sunil Kumar Chawla
Neha Sharma
Ahmed A. Elngar
Prasenjit Chatterjee
P. Naga Srinivasu

5. ICS security news selection

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

1. **AI accelerates industrial cyber threats, transforms OT attack landscape to challenge traditional defenses**
2. **MITRE expands Caldera for OT with Modbus, BACnet simulators for industrial process security testing**
3. **Cyber resilience becomes governance priority for healthcare systems amid rising attack costs**
4. **OT Attacks Get Scary With 'Living-off-the-Plant' Techniques**
5. **5 Bills to Boost Energy Sector Cyber Defenses Clear House Panel**
6. **New NCSC-Led OT Security Guidance for Nuclear Reactors**
7. **Ransomware surge in 2025 exposes mounting OT risk as industrial impacts outpace IT narratives**
8. **Connected and Compromised: When IoT Devices Turn Into Threats**
9. **The hidden security cost of treating labs like data centers**
10. **Beyond the honeypot: How OT deception is reshaping active defense in ICS networks**
11. **The Danger of IT, OT, Medical Device Cyber Turf Wars**
12. **NVIDIA partners with Akamai, Forescout, Palo Alto Networks and Siemens to target real-time OT threat detection**
13. **Maritime cyber incidents jump 103%, as CYTUR warns smart ships under fire; urges secure by design overhaul**
14. **S4x26: New OTI Impact Score debuts to rate real-world damage from industrial cyberattacks**

AI accelerates industrial cyber threats, transforms OT attack landscape to challenge traditional defenses

When it comes to cyberattacks across industrial environments, the role of AI (artificial intelligence) falls between real escalation and inflated alarm. Most alleged AI-enabled threats are not stand-alone systems running in isolation within OT networks. Rather, the bad guys are leveraging AI to speed up human-driven activity, such as automating reconnaissance, generating targeted phishing, and crafting functional exploit code within minutes. What previously took specialized teams and long development cycles can now be done in a matter of minutes across connected OT environments. This shift is not theoretical. …

Source and more information:

https://industrialcyber.co/features/ai-accelerates-industrial-cyber-threats-transforms-ot-attack-landscape-to-challenge-traditional-defenses/

MITRE expands Caldera for OT with Modbus, BACnet simulators for industrial process security testing

MITRE Caldera announced the release of the Wildcat Dam simulator, which helped lower that barrier by introducing an open-source software-based Modbus simulation that can be used as a virtual OT (operational technology) protocol sandbox. The Aloha Water Treatment Plant builds upon that work by adding a simple water treatment process, supporting Modbus and BACnet control protocols, and includes a web-based human-machine interface (HMI). …

Source and more information:

https://industrialcyber.co/ics-security-framework/mitre-expands-caldera-for-ot-with-modbus-bacnet-simulators-for-industrial-process-security-testing/

Cyber resilience becomes governance priority for healthcare systems amid rising attack costs

Healthcare systems are increasingly targeted by cyberattacks that can disrupt care delivery, expose sensitive patient information, and erode trust, yet many providers struggle to balance investments in patient care with strengthening cyber resilience. A World Economic Forum (WEF) report argues that embedding cyber resilience into strategic decision-making is essential to protect patient safety, sustain trust, and support innovation in an increasingly connected healthcare ecosystem, and points to tools such as strategic digital twin simulations as ways for leaders to anticipate cyber risk impacts across clinical, operational, and financial functions.

Source and more information:

https://industrialcyber.co/medical/cyber-resilience-becomes-governance-priority-for-healthcare-systems-amid-rising-attack-costs/

OT Attacks Get Scary With 'Living-off-the-Plant' Techniques

Operational technology (OT) cyberattacks in recent years have been relatively tame, thanks to attackers' ignorance of bespoke and legacy systems. But there are early indications that attackers are growing more interested in and accustomed to dealing with industrial machines, and that they might be on the precipice of causing much more serious damage to them.

A decade ago, it might have seemed like the world was entering a new, more dangerous era of cyberattacks. Russia hacked Ukraine's power grid. Israel and the United States sabotaged an Iranian nuclear facility. Attackers were targeting dams, and manufacturing plants. This was cyberactivity with real-world, sometimes life-threatening consequences. …

Source and more information:

https://www.darkreading.com/ics-ot-security/ot-attacks-living-off-the-plant

5 Bills to Boost Energy Sector Cyber Defenses Clear House Panel

The House Subcommittee on Energy this week advanced five recently introduced bills aimed at boosting the physical and cyber security of the United States' electric grid and other energy infrastructure.

The bills collectively aim to update Department of Energy (DOE) programs, enhance grid and pipeline protections, and prioritize cybersecurity for vulnerable sectors amid rising threats.

One of the bills is H.R. 7258, named the Energy Emergency Leadership Act, which bolsters the Department of Energy's capabilities to perform its energy emergency functions and respond to risks and incidents. …

Source and more information:

https://www.securityweek.com/5-bills-to-boost-energy-sector-cyber-defenses-clear-house-panel/

New NCSC-Led OT Security Guidance for Nuclear Reactors

Last month, the U.K. National Cyber Security Centre in partnership with the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation and other international partners released a new guidance, titled "Secure Connectivity Principles for Operational Technology."

Highlighting eight foundational security principles, the guidance has been designed to help organizations "mitigate exposed and insecure connectivity and protect networks from highly capable and opportunistic cyberthreat actors, including nation state-sponsored actors," according to a CISA press release. …

Source and more information:

https://www.ot.today/blogs/new-ncsc-led-ot-security-guidance-for-nuclear-reactors-p-4044

Ransomware surge in 2025 exposes mounting OT risk as industrial impacts outpace IT narratives

New research from Dragos observed that persistent mischaracterization of ransomware as solely an IT problem obscures growing risks to OT (operational technology) environments.

While adversaries increasingly target industrial organizations, as attacks become more frequent and disruptive, they rely on basic tactics that exploit weak security practices rather than sophisticated techniques. Ransomware groups targeting industrial organizations surged 49% year-over-year, impacting 3,300 organizations globally and disrupting operations.

Additionally, Dragos has observed numerous instances in which a ransomware case was classified as IT only because the victim company or its security firm misclassified OT devices, such as engineering workstations and HMIs (Human-Machine Interface), as IT devices since they ran on Windows operating systems. While exact numbers are difficult to obtain, there are a considerable number of OT-specific ransomware incidents that are mischaracterized. …

Source and more information:

https://industrialcyber.co/ransomware/ransomware-surge-in-2025-exposes-mounting-ot-risk-as-industrial-impacts-outpace-it-narratives/

Connected and Compromised: When IoT Devices Turn Into Threats

The number of Internet of Things (IoT) devices operating in a home or office continues to balloon, but security awareness is lagging despite the considerable risks the technologies pose, from credential theft to network access.

IoT security is a long-standing topic that evolves as an influx of devices emerges onto the landscape. Devices require internet connectivity, yet many lack sufficient passcode and encryption features and ship with insecure default settings, placing much of the responsibility on the user. …

Source and more information:

https://www.darkreading.com/iot/connected-compromised-iot-devices-turn-threats

The hidden security cost of treating labs like data centers

In this Help Net Security interview, Rich Kellen, VP, CISO at IFF, explains why security teams should not treat OT labs like IT environments. He discusses how compromise can damage scientific integrity and create safety risks that backups cannot fix.

Kellen also outlines what “good enough” OT visibility looks like, why compensating controls can backfire, and how partnering with scientists improves security outcomes. …

Source, the link and more information:

https://www.helpnetsecurity.com/2026/02/23/rich-kellen-iff-ot-lab-cybersecurity/

Beyond the honeypot: How OT deception is reshaping active defense in ICS networks

Across industrial and critical infrastructure environments, OT deception has evolved from simple honeypots into a strategic pillar of active defense. Because industrial control systems often lack robust native security, adapting deception for these environments requires emulating specialized protocols, such as Modbus or OPC UA, to create high-fidelity decoys that mirror real PLCs (programmable logic controllers), HMIs (human-machine interface), and SCADA (supervisory control and data acquisition) servers.

According to CounterCraft, these assets must operate without introducing safety risks or 'noise' that could disrupt deterministic processes. …

Source and more information:

https://industrialcyber.co/features/beyond-the-honeypot-how-ot-deception-is-reshaping-active-defense-in-ics-networks/

The Danger of IT, OT, Medical Device Cyber Turf Wars

What often appears to be turf wars between healthcare technology management, facilities OT staff, IT departments and security teams are often just the result of unclear ownership and accountability of device security. And that presents a safety risk to patients, said Mohamed Waqas, chief technology officer at Armis.

As more medical gear, facilities and operational technologies become network-connected, devices are frequently deployed outside the visibility of cybersecurity teams, with the expectation that IT or security - or perhaps a vendor - will intervene only when something goes wrong, he said. …

Source and more information:

https://www.ot.today/interviews/danger-it-ot-medical-device-cyber-turf-wars-i-5526

NVIDIA partners with Akamai, Forescout, Palo Alto Networks and Siemens to target real-time OT threat detection

NVIDIA is collaborating with industry leaders like Akamai, Forescout, Palo Alto Networks, and industrial automation vendor Siemens to integrate accelerated computing and AI into the protection of the world's critical infrastructure. As global industrial systems become more connected through cloud and enterprise networks, traditional OT (operational technology) and ICS (industrial control systems) face a heightened risk of cyber threats. By leveraging NVIDIA's AI capabilities, these companies aim to secure high-stakes environments, such as energy, manufacturing, and transportation, where a digital breach can lead to immediate, real-world consequences for public safety and operational continuity. …

Source and more information:

https://industrialcyber.co/ai/nvidia-partners-with-akamai-forescout-palo-alto-networks-and-siemens-to-target-real-time-ot-threat-detection/

Maritime cyber incidents jump 103%, as CYTUR warns smart ships under fire; urges secure by design overhaul

Amid rising cyber risks targeting smart shipping operations, CYTUR released a white paper examining security blind spots in the maritime sector's digital transformation and outlining how a Secure by Design approach can close those gaps. Drawing on real-world intelligence from CYTUR-TI, the report details emerging threat patterns and sets out proactive response strategies to safeguard connected vessels and sustain operational continuity at sea.

Titled '2026 Maritime Cyber Threat White Paper,' CYTUR reported that maritime cyber incidents in 2025 surged by 103% compared to 2024, emerging as a critical threat to maritime safety. DDoS (Distributed Denial of Service), ransomware, and malware infections account for most of these attacks, with their growth rate more than doubling over the past year. …

Source and more information:

https://industrialcyber.co/reports/maritime-cyber-incidents-jump-103-as-cytur-warns-smart-ships-under-fire-urges-secure-by-design-overhaul/

S4x26: New OTI Impact Score debuts to rate real-world damage from industrial cyberattacks

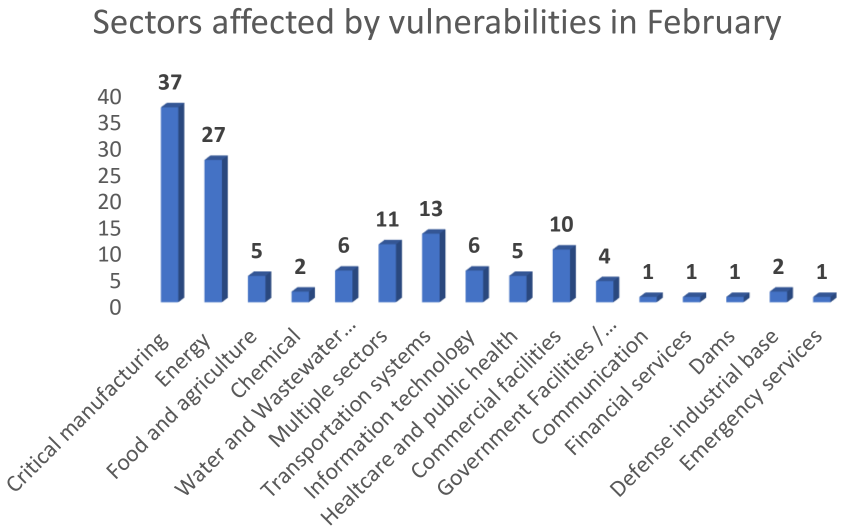
A new metric for measuring real-world consequences of industrial cyberattacks has been unveiled at the ongoing S4x26 conference, aiming to provide a standardized way for the public and policymakers to understand cyber incident severity. Known as the Operations Technology Incident (OTI) Impact Score, this 'Richter Scale for OT cyber incidents' translates complex technical disruptions into a simple score between 0.0 and 10.0. The initiative addresses a growing problem where minor incidents are often over-sensationalized, leading to unnecessary hysteria and misallocation of critical security resources. …

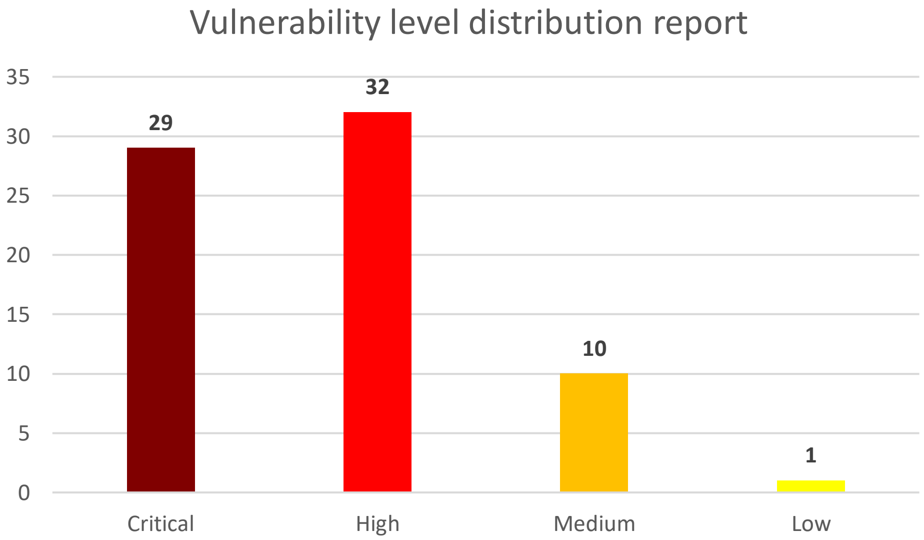
Source and more information:

https://industrialcyber.co/industrial-cyber-attacks/s4x26-new-oti-impact-score-debuts-to-rate-real-world-damage-from-industrial-cyberattacks/

6. ICS vulnerabilities

In February 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-26-057-01: **Johnson Controls, Inc. Frick Controls Quantum HD**

Critical level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Control of Generation of Code ('Code Injection'), Relative Path Traversal, Plaintext Storage of a Password.

Johnson Controls, Inc. Frick Controls Quantum HD | CISA

ICSA-26-057-02: **Pelco, Inc. Sarix Pro 3 Series IP Cameras**

High level vulnerability: Authentication Bypass Using an Alternate Path or Channel.

Pelco, Inc. Sarix Pro 3 Series IP Cameras | CISA

ICSA-26-057-03: **CloudCharge cloudcharge.se**

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Restriction of Excessive Authentication Attempts, Insufficient Session Expiration, Insufficiently Protected Credentials.

CloudCharge cloudcharge.se | CISA

ICSA-26-057-04: **EV2GO ev2go.io**

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Restriction of Excessive Authentication Attempts, Insufficient Session Expiration, Insufficiently Protected Credentials.

EV2GO ev2go.io | CISA

ICSA-26-057-05: **Chargemap chargemap.com**

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Restriction of Excessive Authentication Attempts, Insufficient Session Expiration, Insufficiently Protected Credentials.

Chargemap chargemap.com | CISA

ICSA-26-057-06: **SWITCH EV swtchenergy.com**

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Restriction of Excessive Authentication Attempts, Insufficient Session Expiration, Insufficiently Protected Credentials.

SWITCH EV swtchenergy.com | CISA

ICSA-26-057-07: **EV Energy ev.energy**

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Restriction of Excessive Authentication Attempts, Insufficient Session Expiration, Insufficiently Protected Credentials.

EV Energy ev.energy | CISA

ICSA-26-057-08: **Mobility46 mobility46.se**

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Restriction of Excessive Authentication Attempts, Insufficient Session Expiration, Insufficiently Protected Credentials.

Mobility46 mobility46.se | CISA

ICSA-26-057-10: **Copeland XWEB and XWEB Pro**

Critical level vulnerabilities: Unexpected Status Code or Return Value, Use of a Broken or Risky Cryptographic Algorithm, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Stack-based Buffer Overflow.

Copeland XWEB and XWEB Pro | CISA

ICSA-25-133-02: **Hitachi Energy Relion 670/650/SAM600-IO Series (Update B)**

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

Hitachi Energy Relion 670/650/SAM600-IO Series (Update C) | CISA

ICSA-25-203-04: **Schneider Electric EcoStruxure Power Operation (Update A)**

High level vulnerabilities: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection'), Integer Overflow to Buffer Overflow, Improper Handling of Highly Compressed Data (Data Amplification), Out-of-bounds Write, Uncontrolled Resource Consumption.

Schneider Electric EcoStruxure Power Operation (Update A) | CISA

ICSA-26-048-04: **Honeywell HIB2PI and HDZ Series CCTV Cameras (Update A)**

Critical level vulnerability: Missing Authentication for Critical Function.

Honeywell HIB2PI and HDZ Series CCTV Cameras (Update A) | CISA

ICSA-26-055-01: **InSAT MasterSCADA BUK-TS**

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

InSAT MasterSCADA BUK-TS | CISA

ICSA-26-055-02: **Schneider Electric EcoStruxure Building Operation Workstation**

High level vulnerabilities: Improper Restriction of XML External Entity Reference, Improper Control of Generation of Code ('Code Injection').

Schneider Electric EcoStruxure Building Operation Workstation | CISA

ICSA-26-055-03: **Gardyn Home Kit IoT Device**

Critical level vulnerabilities: Cleartext Transmission of Sensitive Information, Use of Default Credentials, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Use of Hard-coded Credentials.

Gardyn Home Kit | CISA

ICSA-22-202-04: **ICONICS Suite and Mitsubishi Electric MC Works64 Products (Update C)**

Critical level vulnerabilities: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Deserialization of Untrusted Data, Inclusion of Functionality from Untrusted Control Sphere, Out-of-bounds Read.

ICONICS Suite and Mitsubishi Electric MC Works64 Products (Update C) | CISA

ICSA-24-296-01: **Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update C)**

High level vulnerability: Incorrect Default Permissions.

Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update C) | CISA

ICSA-26-050-01: **EnOcean SmartServer IoT**

High level vulnerabilities: Improper Neutralization of Special Elements used in a Command ('Command Injection'), Out-of-bounds Read.

EnOcean SmartServer IoT | CISA

ICSA-26-050-02: **Valmet DNA Engineering Web Tools**

High level vulnerability: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

Valmet DNA Engineering Web Tools | CISA

ICSA-26-050-03: **Jinan USR IOT Technology Limited (PUSR) USR-W610**

Critical level vulnerabilities: Weak Password Requirements, Cleartext Transmission of Sensitive Information, Insufficiently Protected Credentials, Missing Authentication for Critical Function.

Jinan USR IOT Technology Limited (PUSR) USR-W610 | CISA

ICSA-26-050-04: **Welker OdorEyes EcoSystem Pulse Bypass System with XL4 Controller**

High level vulnerability: Missing Authentication for Critical Function.

Welker OdorEyes EcoSystem Pulse Bypass System with XL4 Controller | CISA

ICSA-26-048-01: **Siemens Simcenter Femap and Nastran**

High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Heap-based Buffer Overflow.

Siemens Simcenter Femap and Nastran | CISA

ICSA-26-048-02: **Delta Electronics ASDA-Soft**

High level vulnerability: Stack-based Buffer Overflow.

Delta Electronics ASDA-Soft | CISA

ICSA-26-048-03: **GE Vernova Enervista UR Setup**

High level vulnerability: Uncontrolled Search Path Element, Path Traversal: '.../...//'

GE Vernova Enervista UR Setup | CISA

ICSA-26-048-04: **Honeywell CCTV Products**

Critical level vulnerability: Missing Authentication for Critical Function.

Honeywell CCTV Products | CISA

SSA-613116: **Multiple Vulnerabilities in Third-Party Components in SINEC OS before V3.1 (Update: 1.1.)**

Critical level vulnerabilities: Multiple.

SSA-613116

SSA-355557: **Multiple Vulnerabilities in Third-Party Components in SINEC OS before V3.2 (Update: 1.1.)**

Medium level vulnerabilities: Multiple.

SSA-355557

SSA-864900: **Multiple Vulnerabilities in Fortigate NGFW on RUGGEDCOM APE1808 Devices (Update: 1.7.)**

High level vulnerabilities: Multiple.

SSA-864900

SSA-674753: **Denial-of-Service Vulnerability in ET 200 Devices (Update: 1.1.)**

High level vulnerability: Uncontrolled Resource Consumption.

SSA-674753

SSA-599451: **Multiple Vulnerabilities in SiPass integrated (Update: 1.1.)**

High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Authorization Bypass Through User-Controlled Key, Storing Passwords in a Recoverable Format.

SSA-599451

SSA-513708: **Multiple Vulnerabilities in Palo Alto Networks Virtual NGFW on RUGGEDCOM APE1808 Devices (Update: 1.3.)**

High level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Exposure of Sensitive System Information to an

Unauthorized Control Sphere, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Neutralization of Script in Attributes in a Web Page, Improper Check for Unusual or Exceptional Conditions.

SSA-513708

SSA-282044: **DLL Hijacking Vulnerability in Siemens Web Installer used by the Online Software Delivery (Update: 1.6.)**

High level vulnerability: Uncontrolled Search Path Element.

SSA-282044

SSA-265688: **Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 TM MFP V1.1 (Update: 2.1.)**

High level vulnerabilities: Multiple.

SSA-265688

SSA-216014: **Vulnerabilities in EFI variable of SIMATIC IPCs, SIMATIC Tablet PCs, and SIMATIC Field PGs (Update: 1.3.)**

High level vulnerability: Protection Mechanism Failure.

SSA-216014

SSA-212953: **Multiple Vulnerabilities in COMOS (Update: 1.2.)**

Critical level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Input Validation, Generation of Predictable Numbers or Identifiers, Improper Certificate Validation.

SSA-212953

SSA-082556: **Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1.5 (Update: 1.3.)**

High level vulnerabilities: Multiple.

SSA-082556

ICSA-26-043-01: **Siemens SINEC NMS**

High level vulnerability: Uncontrolled Search Path Element.

Siemens SINEC NMS | CISA

ICSA-26-043-02: **Siemens Polarion**

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

Siemens Polarion | CISA

ICSA-26-043-03: **Siemens COMOS**

Critical level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Input Validation, Generation of Predictable Numbers or Identifiers, Improper Certificate Validation.

Siemens COMOS | CISA

ICSA-26-043-04: **Siemens Desigo CC Product Family and SENTRON Powermanager**

High level vulnerability: Heap-based Buffer Overflow.

Siemens Desigo CC Product Family and SENTRON Powermanager | CISA

ICSA-26-043-05: **Siemens Solid Edge**

High level vulnerability: Out-of-bounds Read.

Siemens Solid Edge | CISA

ICSA-26-043-06: **Siemens SINEC OS**

Critical level vulnerabilities: Out-of-bounds Write, Double Free, Improper Input Validation, Use After Free, Improper Restriction of Operations within the Bounds of a Memory Buffer, Free of Memory not on the Heap, Buffer Over-read, Out-of-bounds Read, NULL Pointer Dereference, Improper Certificate Validation, Incorrect Comparison, Exposure of Sensitive Information to an Unauthorized Actor, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Multiple Releases of Same Resource or Handle, Integer Overflow to Buffer Overflow, Improper Access Control, Integer Overflow or Wraparound, Buffer Underwrite ('Buffer Underflow'), Incorrect Calculation, Stack-based Buffer Overflow, Covert Timing Channel, Generation of Predictable Numbers or Identifiers, Missing Authentication for Critical Function, Allocation of Resources Without Limits or Throttling.

Siemens SINEC OS | CISA

ICSA-26-043-07: **Siemens Siveillance Video Management Servers**

Medium level vulnerability: Missing Authorization.

Siemens Siveillance Video Management Servers | CISA

ICSA-26-043-08: **Siemens NX**

High level vulnerabilities: Stack-based Buffer Overflow, Out-of-bounds Read.

Siemens NX | CISA

ICSA-26-043-09: **Hitachi Energy SuprOS**

High level vulnerability: Use of Default Credentials.

Hitachi Energy SuprOS | CISA

ICSA-26-043-10: **Airleader Master**

Critical level vulnerability: Unrestricted Upload of File with Dangerous Type.

Airleader Master | CISA

ICSA-25-140-04: **Mitsubishi Electric Iconics Digital Solutions / Mitsubishi Electric GENESIS64 (Update E)**

Medium level vulnerability: Execution with Unnecessary Privileges.

Mitsubishi Electric Iconics Digital Solutions / Mitsubishi Electric GENESIS64 (Update E) | CISA

ICSA-26-041-01: **Yokogawa FAST/TOOLS**

High level vulnerabilities: Generation of Error Message Containing Sensitive Information, Cross-Site Request Forgery (CSRF), Use of a Broken or Risky Cryptographic Algorithm, Exposure of Sensitive System Information to an Unauthorized Control Sphere, Improperly Implemented Security Check for Standard, Reliance on IP Address for Authentication, Cleartext Transmission of Sensitive Information, Exposure of Private Personal Information to an Unauthorized Actor, Improper Neutralization of Invalid Characters in Identifiers in Web Pages, Path Traversal: '\..\filename'.

Yokogawa FAST/TOOLS | CISA

ICSA-26-041-02: **ZLAN Information Technology Co. ZLAN5143D**

Critical level vulnerability: Missing Authentication for Critical Function.

ZLAN Information Technology Co. ZLAN5143D | CISA

ICSA-26-041-03: **AVEVA PI Data Archive**

High level vulnerability: Uncaught Exception.

AVEVA PI Data Archive | CISA

ICSA-26-041-04: **AVEVA PI to CONNECT Agent**

Medium level vulnerability: Insertion of Sensitive Information into Log File.

AVEVA PI to CONNECT Agent | CISA

ICSMA-26-041-01: **ZOLL ePCR IOS Mobile Application**

Medium level vulnerability: Insertion of Sensitive Information into Externally-Accessible File or Directory.

ZOLL ePCR IOS Mobile Application | CISA

ICSA-26-036-01: **TP-Link Systems Inc. VIGI C330I IP Camera**

High level vulnerability: Improper Authentication.

TP-Link Systems Inc. VIGI Series IP Camera | CISA

ICSA-26-036-02: **Mitsubishi Electric MELSEC iQ-R Series**

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

Mitsubishi Electric MELSEC iQ-R Series | CISA

ICSA-26-036-03: **o6 Automation GmbH Open62541**

Medium level vulnerability: Out-of-bounds Write.

o6 Automation GmbH Open62541 | CISA

ICSA-26-036-04: **Ilevia EVE X1 Server**

Critical level vulnerabilities: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Insertion of Sensitive Information into Log File, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

Ilevia EVE X1 Server | CISA

ICSA-26-036-05: **Hitachi Energy XMC20**

Critical level vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel.

Hitachi Energy XMC20 | CISA

ICSA-26-036-06: **Hitachi Energy FOX61x**

Critical level vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel.

Hitachi Energy FOX61x | CISA

ICSA-25-184-03: **Mitsubishi Electric MELSOFT Update Manager (Update B)**

High level vulnerabilities: Integer Underflow (Wrap or Wraparound), Protection Mechanism Failure.

Mitsubishi Electric MELSOFT Update Manager (Update B) | CISA

ICSA-25-184-01: **Hitachi Energy Relion 670/650 and SAM600-IO Series (Update C)**

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

Hitachi Energy Relion 670/650 and SAM600-IO Series (Update C) | CISA

ICSA-25-343-03: **Multiple India-based CCTV Cameras (Update A)**

Critical level vulnerability: Missing Authentication for Critical Function.

Multiple India-based CCTV Cameras (Update A) | CISA

ICSA-26-029-01: **KiloView Encoder Series (Update A)**

Critical level vulnerability: Missing Authentication for Critical Function.

KiloView Encoder Series (Update A) | CISA

ICSA-26-034-01: **Mitsubishi Electric FREQSHIP-mini**

High level vulnerability: Incorrect Default Permissions.

Mitsubishi Electric FREQSHIP-mini for Windows | CISA

ICSA-26-034-02: **Avation Light Engine Pro**

Critical level vulnerability: Missing Authentication for Critical Function.

Avation Light Engine Pro | CISA

ICSA-26-034-03: **RISS SRL MOMA Seismic Station**

Critical level vulnerability: Missing Authentication for Critical Function.

RISS SRL MOMA Seismic Station | CISA

ICSA-26-034-04: **Synectix LAN 232 TRIO**

Critical level vulnerability: Missing Authentication for Critical Function.

Synectix LAN 232 TRIO | CISA

ICSA-23-068-05: **Hitachi Energy Relion 670, 650 and SAM600-IO Series (Update B)**

Low level vulnerability: Insufficient Verification of Data Authenticity.

Hitachi Energy Relion 670, 650 and SAM600-IO Series (Update B) | CISA

ICSA-23-089-01: **Hitachi Energy IEC 61850 MMS-Server (Update B)**

Medium level vulnerability: Improper Resource Shutdown or Release.

Hitachi Energy IEC 61850 MMS-Server (Update B) | CISA

ICSA-24-345-06: **Rockwell Automation Arena (Update B)**

High level vulnerabilities: Use After Free, Out-of-bounds Write, Improper Initialization, Out-of-bounds Read, Dependency on Vulnerable Third-Party Component.

Rockwell Automation Arena (Update B) | CISA

ICSA-25-028-06: **Schneider Electric RemoteConnect and SCADAPack x70 Utilities (Update A)** **High** level vulnerability: Deserialization of Untrusted Data.

Schneider Electric RemoteConnect and SCADAPack x70 Utilities (Update A) | CISA

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

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

Mitsubishi Electric Multiple FA Products (Update B) | CISA

ICSA-25-310-02: **Ubia Ubox (Update A)**

Medium level vulnerability: Insufficiently Protected Credentials.

Ubia Ubox (Update A) | 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. ICS alerts

CISA has published alerts in 2026 February:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2019-19006 Sangoma FreePBX Improper Authentication Vulnerability;
CVE-2021-39935 GitLab Community and Enterprise Editions Server-Side Request Forgery (SSRF) Vulnerability;
CVE-2025-40551 SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability;
CVE-2025-64328 Sangoma FreePBX OS Command Injection Vulnerability;
CVE-2025-11953 React Native Community CLI OS Command Injection Vulnerability;
CVE-2026-24423 SmarterTools SmarterMail Missing Authentication for Critical Function Vulnerability;
CVE-2026-21510 Microsoft Windows Shell Protection Mechanism Failure Vulnerability;
CVE-2026-21513 Microsoft MSHTML Framework Security Feature Bypass Vulnerability;
CVE-2026-21514 Microsoft Office Word Reliance on Untrusted Inputs in a Security Decision Vulnerability;
CVE-2026-21519 Microsoft Windows Type Confusion Vulnerability;
CVE-2026-21525 Microsoft Windows NULL Pointer Dereference Vulnerability;
CVE-2026-21533 Windows Remote Desktop Services Elevation of Privilege Vulnerability;
CVE-2024-43468 Microsoft Configuration Manager SQL Injection Vulnerability;
CVE-2025-15556 Notepad++ Download of Code Without Integrity Check Vulnerability;
CVE-2025-40536 SolarWinds Web Help Desk Security Control Bypass Vulnerability;
CVE-2026-20700 Apple Multiple Buffer Overflow Vulnerability;
CVE-2008-0015 Microsoft Windows Video ActiveX Control Remote Code Execution Vulnerability;
CVE-2020-7796 Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery Vulnerability;
CVE-2024-7694 TeamT5 ThreatSonar Anti-Ransomware Unrestricted Upload of File with Dangerous Type Vulnerability;
CVE-2026-2441 Google Chromium CSS Use-After-Free Vulnerability;
CVE-2021-22175 GitLab Server-Side Request Forgery (SSRF) Vulnerability;
CVE-2026-22769 Dell RecoverPoint for Virtual Machines (RP4VMs) Use of Hard-coded Credentials Vulnerability;
CVE-2025-49113 RoundCube Webmail Deserialization of Untrusted Data Vulnerability;
CVE-2025-68461 RoundCube Webmail Cross-site Scripting Vulnerability;
CVE-2026-25108 Soliton Systems K.K. FileZen OS Command Injection Vulnerability;
Links and more information:
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Six Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA

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

BOD 26-02: Mitigating Risk From End-of-Support Edge Devices

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 26-02: Mitigating Risk From End-of-Support Edge Devices.

A Binding Operational Directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems. 44 U.S.C. § 3552(b)(1). Section 3553(b)(2) of title 44, U.S. Code, authorizes the Secretary of the Department of Homeland Security (DHS) to develop and oversee the implementation of binding operational directives to implement cybersecurity policies, principles, standards, and guidelines issued by the Director of the Office of Management and Budget (OMB). Federal agencies are required to comply with these directives under 44 U.S.C. § 3554(a)(1)(B)(ii). These directives do not apply to statutorily defined "national security systems" or to certain systems operated by the Department of War or the Intelligence Community. 44 U.S.C. § 3553(b), (d), (e)(2), (e)(3). This directive refers to the systems to which it applies as "Federal Civilian Executive Branch" systems, and to agencies operating those systems as "Federal Civilian Executive Branch" agencies.

Links and more information:
BOD 26-02: Mitigating Risk From End-of-Support Edge Devices | CISA

8. ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in February 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

9. ICS 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/