2025 December, 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

ICS good practices, recommendations 2
ICS conferences 3
ICS incidents 4
Book recommendation 9
ICS security news selection 10
ICS vulnerabilities 18
ICS alerts 27
ICS trainings, education 30
ICS podcasts 33

ICS good practices, recommendations

CISA, Australia, and Partners Author Joint Guidance on Securely Integrating Artificial Intelligence in Operational Technology

CISA and the Australian Signals Directorate's Australian Cyber Security Centre, in collaboration with federal and international partners, have released new cybersecurity guidance: Principles for the Secure Integration of Artificial Intelligence in Operational Technology.

This guidance aims to help critical infrastructure owners and operators integrate artificial intelligence (AI) into operational technology (OT) systems securely, balancing the benefits of AI—such as increased efficiency, enhanced decision-making, and cost savings—with the unique risks it poses to the safety, security, and reliability of OT environments.

The document focuses on machine learning (ML), large language models (LLMs), and AI agents due to their complex security challenges, but is also applicable to systems using traditional statistical modeling and logic-based automation.

Key Principles for Secure AI Integration:

1. Understand AI: Educate personnel on AI risks, impacts, and secure development lifecycles.
2. Assess AI Use in OT: Evaluate business cases, manage OT data security risks, and address immediate and long-term integration challenges.
3. Establish AI Governance: Implement governance frameworks, test AI models continuously, and ensure regulatory compliance.
4. Embed Safety and Security: Maintain oversight, ensure transparency, and integrate AI into incident response plans.

Critical infrastructure owners and operators are encouraged to adopt these principles to maximize AI benefits while mitigating risks. For further details, review the full guidance.

For more information on related resources, visit CISA's Artificial Intelligence and Industrial Control Systems webpages.

Source and links:

CISA, Australia, and Partners Author Joint Guidance on Securely Integrating Artificial Intelligence in Operational Technology | CISA

ICS conferences

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

International Conference on Industrial Control Systems Security (ICICSS)

International Conference on Industrial Control Systems Security is a multidisciplinary research and development association. It has a group of scientists and researchers from around the world who work together to solve problems using science and technology and ensure sustainable development. They help companies, universities, and governments find solutions to challenges related to scientific progress by conducting conferences, workshops and collaborations.

Zurich, Switzerland; 10th January 2026

More details can be found on the following website:

https://internationalconferencealerts.com/eventdetails.php?id=3430714

ICS incidents

Hacktivists increasingly target industrial control systems, Canada Cyber Centre warns

The Canadian Centre for Cyber Security has issued an alert highlighting the increasing risks posed by internet-exposed industrial control systems (ICS), based on recent real-world incidents affecting the water, oil and gas, and agricultural sectors. The alert shows that hacktivists and state-aligned threat actors are actively targeting operational technology (OT) environments, often opportunistically, by exploiting publicly accessible control systems.

In one incident, attackers accessed a Canadian water utility's control system and manipulated water pressure values, resulting in service disruption. This reflects a broader trend observed internationally, particularly in the United States, where water utilities have been repeatedly targeted. Previous incidents include attempts to alter chemical dosing and pressure controls, demonstrating the potential for serious public health and safety consequences if such attacks go undetected.

The alert also describes an attack on an oil and gas company in which hackers manipulated an internet-exposed automated tank gauge (ATG). By falsifying sensor readings, the attackers triggered false alarms and created the risk of unsafe operational responses. ATGs are widely used to monitor fuel levels and detect leaks at critical facilities, and their exposure is especially concerning given the number of known vulnerabilities and previously unauthenticated devices accessible online.

A third case involved agricultural infrastructure, where attackers interfered with temperature and humidity controls in a grain-drying silo. Such manipulation could have compromised food safety and supply if it had not been identified in time.

These incidents demonstrate that insecurely exposed ICS components can lead to operational disruption, safety risks, and loss of public trust across multiple sectors. The Canadian Centre for Cyber Security emphasizes the need for secure remote access solutions, such as VPNs with multi-factor authentication, and urges organizations and authorities to improve asset visibility, documentation, and protection, particularly in sectors with limited cybersecurity regulation.

The source is available at the following link:

https://www.csoonline.com/article/4082752/hacktivists-increasingly-target-industrial-control-systems-canada-cyber-centre-warns.html?utm_source=chatgpt.com

Denmark blames Russia for destructive cyberattack on water utility

Danish intelligence authorities have publicly attributed recent cyberattacks against Denmark's critical infrastructure to Russia, describing them as part of Moscow's broader hybrid warfare campaign against Western countries. According to the Danish Defence Intelligence Service (DDIS), the attacks were intended to create insecurity, attract public attention, and punish nations that support Ukraine.

The DDIS identified two pro-Russian cyber groups acting as instruments of the Russian state. Z-Pentest was linked to a destructive cyberattack against a water utility, while NoName057(16) was blamed for distributed denial-of-service (DDoS) attacks targeting Denmark ahead of local elections and in the lead-up to the 2025 national elections. Danish authorities assessed that the election period was deliberately used to maximize visibility and influence public perception, a tactic observed in other European countries as well.

These cyber operations are viewed as part of a wider influence and destabilization campaign aimed at undermining Western support for Ukraine. Since Russia's full-scale invasion in 2022, Denmark has actively supported Ukraine through sanctions, military assistance, training, and financial aid, making it a target for retaliatory hybrid activities. Denmark's defence minister described the incidents as clear evidence that hybrid warfare is already underway in Europe and stated that such actions are unacceptable. In response, Danish authorities announced diplomatic measures, including summoning the Russian ambassador.

Similar activity has been observed elsewhere in the region. In Norway, authorities previously attributed the manipulation of dam outflow valves to pro-Russian hackers who gained access to operational systems, while earlier DDoS attacks disrupted key public services. The growing threat has prompted international warnings, including a recent joint advisory by CISA and multiple allied agencies, cautioning that pro-Russian hacktivist groups are actively targeting critical infrastructure organizations worldwide. …

The source is available at the following link:

https://www.bleepingcomputer.com/news/security/denmark-blames-russia-for-destructive-cyberattack-on-water-utility/

Book recommendation

Industrial Control Systems

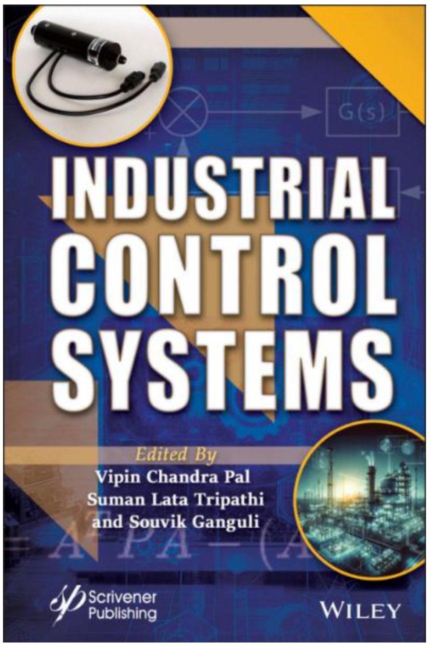
The journey of the control system may be viewed from the control of steam engines to spacecraft, aeroplane missile control systems to networked control systems and cybersecurity controls. In terms of industrial control and application, the journey starts from the design of P-I-D controllers to fuzzy controllers, neuro-fuzzy controllers, backstepping controllers, sliding mode controllers, and event-triggered controls for networked control systems. Recently, control theory has spread its golden feathers in different fields of engineering by use of the splendid tool of the control system. In this era, the boom of the Internet of Things is at its maximum pace. Different biomedical applications also come under this umbrella and provide the easiest way to continuous monitoring. One of the prominent research areas of green energy and sustainable development in which control plays a vital role is load frequency controllers, control of solar thermal plants, an event-driven building energy management system, speed-sensorless voltage and frequency control in autonomous DFIG-based wind energy, Hazardous Energy Control Programs, and many more.

Author/Editor: Vipin Chandra Pal, Suman Lata Tripathi, Souvik Ganguli editors

Year of issue: 2023

The book is available at the following link:

https://www.amazon.in/Industrial-Control-Systems-Vipin-Chandra/dp/1119829259



ICS security news selection

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

1. **DoW’s ZT for OT Activities and Outcomes document sets foundation for Zero Trust across defense infrastructure**
2. **AI Drives Faster Industrial Software Development Cycles**
3. **Smart grids are trying to modernize and attackers are treating it like an invitation**
4. **OTMEC initiative aims to bridge gaps in industrial cybersecurity in Middle East, North Africa**
5. **Threat Landscape Grows Increasingly Dangerous for Manufacturers**
6. **US, Allies Warn AI in OT May Undermine System Safety**
7. **Global Cyber Agencies Issue AI Security Guidance for Critical Infrastructure OT**
8. **AI in OT Sparks Cascade of Complex Challenges**
9. **Monitoring the Electric Grid Is Easier Said Than Done**
10. **AXA XL joins ISASecure to boost cybersecurity risk prevention by adopting ISA/IEC 62443 cybersecurity standards**
11. **Zabbix: Open-source IT and OT observability solution**
12. **MITRE expands D3FEND cybersecurity ontology to support cybersecurity in OT environments**
13. **Who Decides When Security Levels Are “Enough”?**
14. **A Hacker's Perspective: Why OT Systems Are Still Exposed**
15. **When the Cloud Rains on Everyone's IoT Parade**

DoW’s ZT for OT Activities and Outcomes document sets foundation for Zero Trust across defense infrastructure

The U.S. Department of War (DoW) recently published a Zero Trust Guidance that provides a revised set of activities and outcomes to facilitate current and future adoption of ZT principles in OT (operational technology) environments, accounting for the distinct differences between IT and OT practices. The ZT for OT Activities and Outcomes is aligned with the ZT for Enterprise IT Activities and Outcomes to facilitate interoperability between the two.

Titled 'Zero Trust for Operational Technology – Scope and Purpose,' the 28-page guidance focuses on DoW-owned OT environments and control systems up to and including the point of demarcation, encompassing facility-related control systems, power grids, water treatment facilities, security and life safety systems, energy management systems, transportation networks, logistics handling, and manufacturing control systems. …

Source and more information:

https://industrialcyber.co/zero-trust/dows-zt-for-ot-activities-and-outcomes-document-sets-foundation-for-zero-trust-across-defense-infrastructure/

AI Drives Faster Industrial Software Development Cycles

Modern industrial plants require digital systems that evolve quickly, and the rapid pace of operational change is pushing companies to rethink outdated development models. Artificial intelligence is helping industries drive faster development cycles, increase productivity, and push real-time updates and innovations, said Rajesh Ramachandran, global chief digital officer for process automation at ABB. …

Source and more information:

https://www.ot.today/ai-drives-faster-industrial-software-development-cycles-a-30149

Smart grids are trying to modernize and attackers are treating it like an invitation

In this Help Net Security interview, Sonia Kumar, Senior Director Cyber Security at Analog Devices, discusses how securing decentralized smart grids demands a shift in defensive strategy. Millions of distributed devices are reshaping the attack surface, and she explains why utilities must rethink threats, resilience, and trust.

Kumar explains that next-generation architectures need to build in security from edge devices through to cloud systems to keep up with emerging risks. …

Source and more information:

https://www.helpnetsecurity.com/2025/12/04/sonia-kumar-analog-devices-securing-smart-grids/

OTMEC initiative aims to bridge gaps in industrial cybersecurity in Middle East, North Africa

The Operational Technology Middle East Community (OTMEC) has officially launched as a regional initiative dedicated to enhancing ICS/OT cybersecurity across the Middle East and North Africa. The co-founders of the initiative include Reem Faraj AlShammari, Bryson Bort, Thomas VanNorman, Saltanat Mashirova, and Michael Hoffman. The advisory board includes Robert M. Lee and Tim Conway.

OTMEC aims to foster vendor-neutral knowledge sharing, build and support the OT security workforce, and drive collaboration, innovation, and the protection of critical infrastructure. The community provides a platform for ICS and OT cybersecurity professionals in the region to exchange insights and best practices. It seeks to strengthen workforce training, encourage collaboration and innovation within the industry, and advocate for greater public awareness and robust cybersecurity policies related to critical infrastructure. …

Source and more information:

https://industrialcyber.co/industrial-cyber-attacks/otmec-initiative-aims-to-bridge-gaps-in-industrial-cybersecurity-in-middle-east-north-africa/

Threat Landscape Grows Increasingly Dangerous for Manufacturers

Manufacturers continued to be a top target — if not the top target — of financially motivated cyberattacks in 2025, with their sensitivity to operational disruptions and their shortage of expertise and well-designed protections causing issues for the business sector as a whole, experts say.

In 2025, half of manufacturers (51%) fell prey to ransomware and paid a ransom, with the average ransom costing $1 million and the average recovery cost (excluding the ransom) approaching $1.3 million, according to data that cybersecurity firm Sophos collected from more than 330 manufacturing organizations. In addition, for the first time in three years, exploited vulnerabilities were the most common root cause of compromises affecting the sector. In 2024, malicious emails were the top vector, while compromised credentials took the top slot in 2023. …

Source and more information:

https://www.darkreading.com/cyberattacks-data-breaches/threat-landscape-increasingly-dangerous-manufacturers

US, Allies Warn AI in OT May Undermine System Safety

The U.S. cyber defense agency warned that machine learning and large language model deployments can introduce new attack surfaces across critical infrastructure sectors in a document setting out principles for safely integrating artificial intelligence into operational technology.

The Cybersecurity and Infrastructure Security Agency and international partners advise critical infrastructure operators to have a deep understanding of how AI models behave, how they fail and how those failures can potentially cascade before implementing them in technology that manages energy, manufacturing, water, transportation and other services. …

Source and more information:

https://www.ot.today/us-allies-warn-ai-in-ot-may-undermine-system-safety-a-30193

Global Cyber Agencies Issue AI Security Guidance for Critical Infrastructure OT

Cyber agencies from several countries have published joint guidance outlining principles for the safe and secure use of artificial intelligence in operational technology (OT) environments, particularly in critical infrastructure.

The guidance, published on the website of the cybersecurity agency CISA, was authored by government organizations in the United States, the United Kingdom, Canada, Germany, the Netherlands, and New Zealand.

Integrating AI with industrial control systems (ICS) and other OT can have significant benefits. The agencies have provided several examples of use cases. …

Source and more information:

https://www.securityweek.com/global-cyber-agencies-issue-ai-security-guidance-for-critical-infrastructure-ot/

AI in OT Sparks Cascade of Complex Challenges

Artificial intelligence (AI) integration poses security, governance, and data privacy risks — challenges that will only increase in operational technology (OT) environments. A new government advisory seeks to provide guidance, but it omits some key points.

The Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency, and the Australian Signals Directorate's Australian Cyber Security Centre published a joint government advisory that details four key principles to help OT owners and operators of critical infrastructure: to understand AI, assess AI use in OT, establish AI governance, and embed safety and security. …

Source and more information:

https://www.darkreading.com/ics-ot-security/ai-ot-too-incompatible-work-securely

Monitoring the Electric Grid Is Easier Said Than Done

A new reliability standard for U.S. and Canadian electric grid tells major power companies to monitor and log traffic on their operational technology and industrial control systems networks. Operators, regulators said, should be able to detect, prevent and respond to unauthorized intrusions aimed at sabotaging the North American power supply.

OT security experts say that the new rules - mandated after attacks on the Ukrainian electric grid by Russian hackers and the discovery of Chinese threat actors prepositioned in the networks of U.S. power companies - will be a heavy lift for the electricity sector. …

Source and more information:

https://www.ot.today/monitoring-electric-grid-easier-said-than-done-a-30275

AXA XL joins ISASecure to boost cybersecurity risk prevention by adopting ISA/IEC 62443 cybersecurity standards

The International Society of Automation (ISA), a professional society for automation, announced that AXA XL has officially joined ISASecure, the globally recognized certification program that validates conformance to the ISA/IEC 62443 series of standards for industrial automation and control systems (IACS) cybersecurity.

AXA XL is the commercial property and casualty and specialty risk division of AXA SA, one of the world’s largest commercial insurance reinsurance companies. Among its offerings are comprehensive cyber insurance solutions. Risk consulting is another key component of AXA XL's service offerings. ...

Source and more information:

https://industrialcyber.co/news/axa-xl-joins-isasecure-to-boost-cybersecurity-risk-prevention-by-adopting-isa-iec-62443-cybersecurity-standards/

Zabbix: Open-source IT and OT observability solution

Zabbix is an open source monitoring platform designed to track the availability, performance, and integrity of IT environments. It monitors networks along with servers, virtual machines, applications, services, databases, websites, and cloud resources. For cybersecurity professionals, this visibility matters because operational issues and security incidents often overlap. Early signs of compromise can surface as performance changes, service failures, or unusual system behavior that monitoring tools detect first. ...

Source and more information:

https://www.helpnetsecurity.com/2025/12/17/zabbix-open-source-it-ot-observability-solution/

MITRE expands D3FEND cybersecurity ontology to support cybersecurity in OT environments

Non-profit organization MITRE announced on Tuesday the extension of its D3FEND cybersecurity ontology to OT (operational technology) environments, creating a structured knowledge base for defending cyber-physical systems. D3FEND for OT delivers a stable, extensible, and integration-friendly framework to support cybersecurity operations and strategic decision-making in OT environments.

Funded by the Cyber Warfare Directorate in the U.S. Office of the Under Secretary of War for Acquisition and Sustainment and the National Security Agency, D3FEND is expanding into specific domains, including cyber-physical systems that create real-world effects through programmed actions. The D3FEND extension provides a common framework to help the cybersecurity community better understand, secure, and sustain these essential systems. ...

Source and more information:

https://industrialcyber.co/control-device-security/mitre-expands-d3fend-cybersecurity-ontology-to-support-cybersecurity-in-ot-environments/

Who Decides When Security Levels Are “Enough”?

Security Levels are not the problem.

In fact, they are one of the most pragmatic inventions in industrial cybersecurity. They give structure to chaos. They allow large, messy installations to be segmented, hardened, and improved without requiring perfect knowledge or endless analysis. In organizations with limited people, time, and budget, they make cyber protection possible at all.

The problem starts when Security Levels quietly become something they were never meant to be a substitute for deciding whether risk is acceptable. …

Source and more information:

https://industrialcyber.co/expert/who-decides-when-security-levels-are-enough/

A Hacker's Perspective: Why OT Systems Are Still Exposed

Insider threats are overlooked attack vectors in industrial systems, said Jesse McGraw, a former black hat hacker turned cybersecurity researcher. Organizations have hardened remote access controls to block remote hackers but they continue to underestimate the risk posed by employees and contractors with physical or logical access to operational technology systems.

McGraw said the legacy design of OT systems, including unauthenticated protocols such as Modbus, makes them vulnerable to attacks even without sophisticated tools.

"Today's industries aren't prepared for insider threats," McGraw said. "I was the guy who had every protocol memorized - the one they called on holidays to train new hires. But behind the scenes, I was gaining unauthorized access just for the thrill of it." …

Source and more information:

https://www.ot.today/hackers-perspective-ot-systems-are-still-exposed-a-30405

When the Cloud Rains on Everyone's IoT Parade

Cloud outages mounted over the past year, disrupting everything from finance and food delivery apps to travel systems. In an era of smart devices, people struggled to scroll social media, shop online, or even adjust their thermostats. Disruptions to Amazon Web Services (AWS), Cloudflare, and Azure left people wondering: Why do so many things need to be connected to the Internet to work?

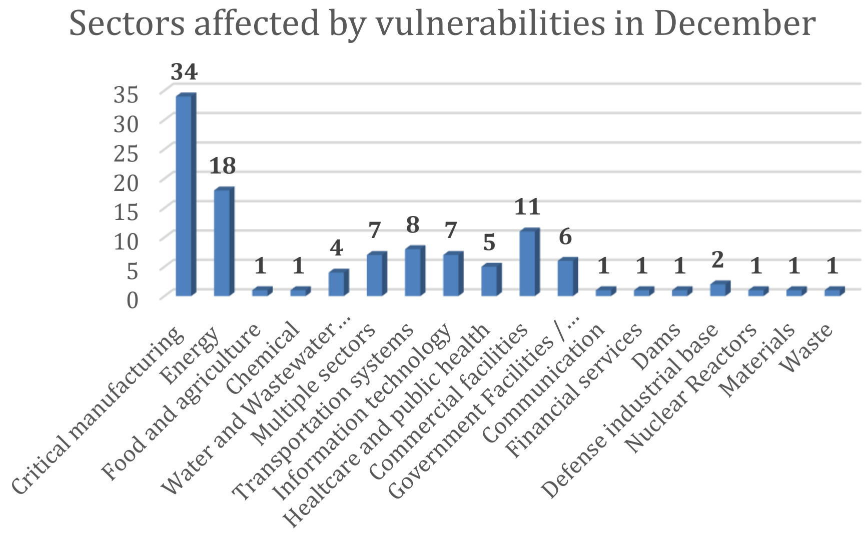
The AWS outage in mid-October lasted nearly 15 hours, and an onslaught of delays and disruptions swiftly followed — due, in particular, to Amazon's share of the Internet of Things, with products like Ring and Alexa. The daily routine many people depended on was suddenly and significantly interrupted in ways they did not expect. …

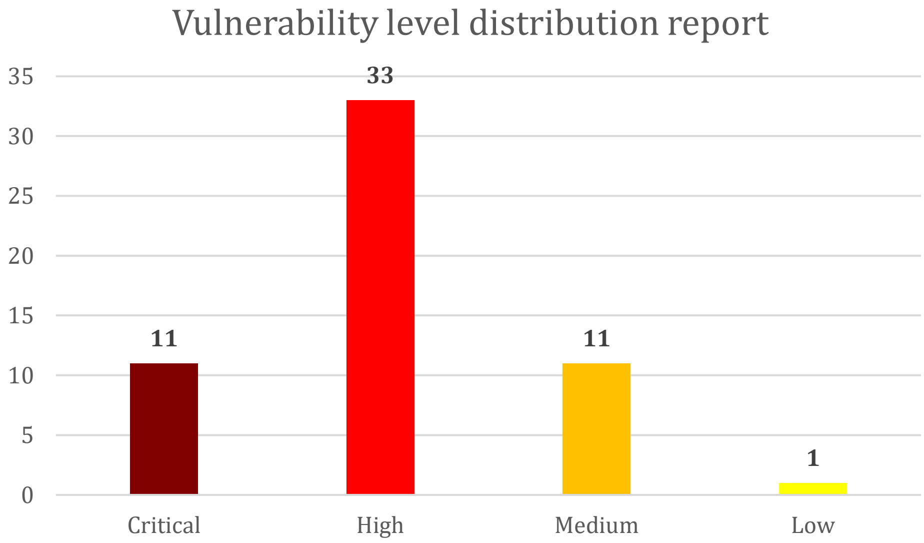
Source and more information:

https://www.darkreading.com/iot/when-cloud-rains-on-everyone-iot-parade

ICS vulnerabilities

In December 2025, 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-25-364-01: **WHILL C2 Wheelchairs**

Critical level vulnerability: Missing Authentication for Critical Function.

WHILL Model C2 Electric Wheelchairs and Model F Power Chairs | CISA

ICSA-25-345-03: **AzeoTech DAQFactory (Update A)**

High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Access of Uninitialized Pointer, Access of Resource Using Incompatible Type ('Type Confusion'), Use After Free.

AzeoTech DAQFactory (Update A) | CISA

ICSA-25-177-01: **Mitsubishi Electric Air Conditioning Systems (Update B)**

Critical level vulnerability: Missing Authentication for Critical Function.

Mitsubishi Electric Air Conditioning Systems (Update B) | CISA

ICSA-25-352-01: **Inductive Automation Ignition**

Medium level vulnerability: Execution with Unnecessary Privileges.

Inductive Automation Ignition | CISA

ICSA-25-352-02: **Schneider Electric EcoStruxure Foxboro DCS Advisor**

Critical level vulnerability: Deserialization of Untrusted Data.

Schneider Electric EcoStruxure Foxboro DCS Advisor | CISA

ICSA-25-352-03: **National Instruments LabView**

High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Use After Free, Stack-based Buffer Overflow.

National Instruments LabView | CISA

ICSA-25-352-04: **Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electrics Products**

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

Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electrics Products | CISA

ICSA-25-352-05: **Siemens Interniche IP-Stack**

High level vulnerability: Improper Verification of Source of a Communication Channel.

Siemens Interniche IP-Stack | CISA

ICSA-25-352-06: **Advantech WebAccess/SCADA**

High level vulnerabilities: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Unrestricted Upload of File with Dangerous Type, Absolute Path Traversal, Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

Advantech WebAccess/SCADA | CISA

ICSA-25-352-07: **Rockwell Automation Micro820, Micro850, Micro 870**

High level vulnerabilities: Dependency on Vulnerable Third-Party Component, Release of Invalid Pointer or Reference.

Rockwell Automation Micro820, Micro850, Micro870 | CISA

ICSA-25-352-08: **Axis Communications Camera Station Pro, Camera Station, and Device Manager**

Critical level vulnerabilities: Deserialization of Untrusted Data, Improper Certificate Validation, Authentication Bypass Using an Alternate Path or Channel.

Axis Communications Camera Station Pro, Camera Station, and Device Manager | CISA

ICSA-24-291-03: **Mitsubishi Electric CNC Series (Update C)**

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

Mitsubishi Electric CNC Series (Update C) | CISA

ICSA-25-350-01: **Güralp Systems FMUS (Fortimus) Series and MIN (Minimus) Series** **Medium** level vulnerability: Allocation of Resources Without Limits or Throttling.

Güralp Systems Fortimus Series, Minimus Series, and Certimus Series | CISA

ICSA-25-350-02: **Johnson Controls PowerG, IQPanel and IQHub**

High level vulnerabilities: Cleartext Transmission of Sensitive Information, Reusing a Nonce, Key Pair in Encryption, Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG), Origin Validation Error.

Johnson Controls PowerG, IQPanel and IQHub | CISA

ICSA-25-350-03: **Hitachi Energy AFS, AFR and AFF Series**

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

Hitachi Energy AFS, AFR and AFF Series | CISA

ICSA-25-350-04: **Mitsubishi Electric GT Designer3**

Medium level vulnerability: Cleartext Storage of Sensitive Information.

Mitsubishi Electric GT Designer3 | CISA

ICSA-25-140-04: **Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update C)**

Medium level vulnerability: Execution with Unnecessary Privileges.

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

ICSA-25-224-02: **Johnson Controls iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE, iSTAR Edge G2 (Update A)**

High level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Insufficient Verification of Data Authenticity, Use of Default Credentials, Missing Protection Mechanism for Alternate Hardware Interface, Insecure Storage of Sensitive Information.

Johnson Controls iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE, iSTAR Edge G2 (Update A) | CISA

ICSA-25-308-01: **Fuji Electric Monitouch V-SFT-6 (Update A)**

High level vulnerability: Heap-based Buffer Overflow, Stack-based Buffer Overflow, Out-of-bounds Write.

Fuji Electric Monitouch V-SFT-6 (Update A) | CISA

ICSA-25-345-01: **Johnson Controls iSTAR**

High level vulnerability: Improper Neutralization of Special Elements used in an OS Command.

Johnson Controls iSTAR | CISA

ICSA-25-345-02: **Johnson Controls iSTAR Ultra**

High level vulnerability: OS Command Injection.

Johnson Controls iSTAR Ultra | CISA

ICSA-25-345-03: **AzeoTech DAQFactory**

High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Access of Uninitialized Pointer, Heap-based Buffer Overflow, Type Confusion, Use After Free, Stack-based Buffer Overflow.

AzeoTech DAQFactory | CISA

ICSA-25-345-04: **Siemens IAM Client**

Critical level vulnerability: Improper Certificate Validation.

Siemens IAM Client | CISA

ICSA-25-345-05: **Siemens Advanced Licensing (SALT) Toolkit**

Critical level vulnerability: Improper Certificate Validation.

Siemens Advanced Licensing (SALT) Toolkit | CISA

ICSA-25-345-06: **Siemens SINEMA Remote Connect Server**

Low level vulnerabilities: Incorrect Permission Assignment for Critical Resource, Incorrect Authorization.

Siemens SINEMA Remote Connect Server | CISA

ICSA-25-345-07: **Siemens Building X - Security Manager Edge Controller**

Medium level vulnerability: Improper Verification of Cryptographic Signature.

Siemens Building X - Security Manager Edge Controller | CISA

ICSA-25-345-08: **Siemens Energy Services**

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

Siemens Energy Services | CISA

ICSA-25-345-09: **Siemens Gridscale X Prepay**

Medium level vulnerabilities: Observable Response Discrepancy, Authentication Bypass by Capture-replay.

Siemens Gridscale X Prepay | CISA

ICSA-25-345-10: **OpenPLC_V3**

High level vulnerability: Cross-Site Request Forgery (CSRF).

OpenPLC_V3 | CISA

ICSMA-25-345-01: **Grassroots DICOM (GDCM)**

Medium level vulnerability: Out-of-bounds Write.

Grassroots DICOM (GDCM) | CISA

ICSMA-25-345-02: **Varex Imaging Panoramic Dental Imaging Software**

High level vulnerability: Uncontrolled Search Path Element.

Varex Imaging Panoramic Dental Imaging Software | CISA

ICSA-25-343-01: **Universal Boot Loader (U-Boot)**

High level vulnerability: Improper Access Control for Volatile Memory Containing Boot Code.

Universal Boot Loader (U-Boot) | CISA

ICSA-25-343-02: **Festo LX Appliance**

Medium level vulnerability: Cross-site Scripting.

Festo LX Appliance | CISA

ICSA-25-343-03: **Multiple India-Based CCTV Cameras**

Critical level vulnerability: Missing Authentication for Critical Function.

Multiple India-based CCTV Cameras | CISA

SSA-800126: **Deserialization Vulnerability in Siemens Engineering Platforms before V20 (Update 1.2.)**

High level vulnerability: Deserialization of Untrusted Data.

SSA-800126

SSA-723487: **RADIUS Protocol Susceptible to Forgery Attacks (CVE-2024-3596) - Impact to SCALANCE, RUGGEDCOM and Related Products (Update 1.8.)**

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

SSA-723487

SSA-693808: **Deserialization Vulnerability in Siemens Engineering Platforms (Update 1.2.)**

High level vulnerability: Deserialization of Untrusted Data.

SSA-693808

SSA-673996: **Buffer Overflow Vulnerability in Third-Party Component in SICAM and SITIPE Products (Update 1.3.)**

High level vulnerability: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').

SSA-673996

SSA-493396: **Deserialization Vulnerability in Siemens Engineering Platforms (Update 1.2.)**

High level vulnerability: Deserialization of Untrusted Data.

SSA-493396

SSA-408105: **Buffer Overflow Vulnerabilities in OpenSSL 3.0 Affecting Siemens Products (Update 1.3.)**

High level vulnerability: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').

SSA-408105

SSA-392859: **Local Arbitrary Code Execution Vulnerability in Siemens Engineering Platforms before V20 (Update 1.2.)**

High level vulnerability: Improper Input Validation.

SSA-392859

SSA-282044: **DLL Hijacking Vulnerability in Siemens Web Installer used by the Online Software Delivery (Update 1.4.)**

High level vulnerability: Uncontrolled Search Path Element.

SSA-282044

ICSA-25-338-01: **Mitsubishi Electric GX Works2**

Medium level vulnerability: Cleartext Storage of Sensitive Information.

Mitsubishi Electric GX Works2 | CISA

ICSA-25-338-02: **MAXHUB Pivot**

High level vulnerability: Weak Password Recovery Mechanism for Forgotten Password.

MAXHUB Pivot | CISA

ICSA-25-338-03: **Johnson Controls OpenBlue Mobile Web Application for OpenBlue Workplace**

Medium level vulnerability: Direct Request ('Forced Browsing').

Johnson Controls OpenBlue Mobile Web Application for OpenBlue Workplace | CISA

ICSA-25-338-04: **Johnson Controls iSTAR**

High level vulnerability: Improper Validation of Certificate Expiration.

Johnson Controls iSTAR | CISA

ICSA-25-338-05: **Sunbird DCIM dcTrack and Power IQ**

High level vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Use of Hard-coded Credentials.

Sunbird DCIM dcTrack and Power IQ | CISA

ICSA-25-338-06: **SolisCloud Monitoring Platform**

High level vulnerability: Authorization Bypass Through User-Controlled Key.

SolisCloud Monitoring Platform | CISA

ICSA-25-338-07: **Advantech iView**

High level vulnerability: SQL Injection.

Advantech iView | CISA

ICSA-25-148-03: **Consilium Safety CS5000 Fire Panel (Update A)**

High level vulnerability: SQL Injection.

Advantech iView | CISA

ICSA-25-219-02: **Johnson Controls FX Server, FX80 and FX90 (Update A)**

High level vulnerability: Dependency on Vulnerable Third-Party Component.

Johnson Controls FX Server, FX80 and FX90 (Update A) | CISA

ICSA-25-336-01: **Industrial Video & Control Longwatch**

Critical level vulnerability: Improper Control of Generation of Code ('Code Injection').

Industrial Video & Control Longwatch | CISA

ICSA-25-336-02: **Iskra iHUB and iHUB Lite**

Critical level vulnerability: Missing Authentication for Critical Function.

Iskra iHUB and iHUB Lite | CISA

ICSMA-25-336-01: **Mirion Medical EC2 Software NMIS BioDose**

High level vulnerabilities: Incorrect Permission Assignment for Critical Resource, Use of Client-Side Authentication, Use of Hard-coded Credentials.

Mirion Medical EC2 Software NMIS BioDose | CISA

ICSA-25-201-01: **Mitsubishi Electric CNC Series (Update A)**

High level vulnerability: Uncontrolled Search Path Element.

Mitsubishi Electric CNC Series (Update A) | CISA

ICSA-23-157-02: **Mitsubishi Electric MELSEC iQ-R Series/iQ-F Series (Update C)**

High level vulnerabilities: Weak Password Requirements, Use of Hard-coded Credentials, Missing Password Field Masking, Unrestricted Upload of File with Dangerous Type.

Mitsubishi Electric MELSEC iQ-R Series/iQ-F Series (Update C) | CISA

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

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.

ICS alerts

CISA has published alerts in 2025 December:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2025-48572 Android Framework Privilege Escalation Vulnerability ;
CVE-2025-48633 Android Framework Information Disclosure Vulnerability;
CVE-2021-26828 OpenPLC ScadaBR Unrestricted Upload of File with Dangerous Type Vulnerability;
CVE-2022-37055 D-Link Routers Buffer Overflow Vulnerability;
CVE-2025-66644 Array Networks ArrayOS AG OS Command Injection Vulnerability;
CVE-2025-6218 RARLAB WinRAR Path Traversal Vulnerability;
CVE-2025-62221 Microsoft Windows Use After Free Vulnerability;
CVE-2025-55182 Meta React Server Components Remote Code Execution Vulnerability;
CVE-2025-58360 OSGeo GeoServer Improper Restriction of XML External Entity Reference Vulnerability;
CVE-2018-4063 Sierra Wireless AirLink ALEOS Unrestricted Upload of File with Dangerous Type Vulnerability;
CVE-2025-14174 Google Chromium Out-of-Bounds Memory Access Vulnerability;
CVE-2025-14611 Gladinet CentreStack and Triofox Hard Coded Cryptographic Vulnerability;
CVE-2025-43529 Apple Multiple Products Use-After-Free WebKit Vulnerability;
CVE-2025-59718 Fortinet Multiple Products Improper Verification of Cryptographic Signature Vulnerability;
CVE-2025-20393 Cisco Multiple Products Improper Input Validation Vulnerability;
CVE-2025-40602 SonicWall SMA1000 Missing Authorization Vulnerability;
CVE-2025-59374 ASUS Live Update Embedded Malicious Code Vulnerability;
CVE-2025-14733 WatchGuard Firebox Out-of-Bounds Write Vulnerability;
CVE-2023-52163 Digiever DS-2105 Pro Missing Authorization Vulnerability;
CVE-2025-14847 MongoDB and MongoDB Server Improper Handling of Length Parameter Inconsistency Vulnerability;
Links and more information:
CISA Adds Two 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 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 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 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 One Known Exploited Vulnerability to Catalog | CISA

PRC State-Sponsored Actors Use BRICKSTORM Malware Across Public Sector and Information Technology Systems
The Cybersecurity and Infrastructure Security Agency (CISA) is aware of ongoing intrusions by People's Republic of China (PRC) state-sponsored cyber actors using BRICKSTORM malware for long-term persistence on victim systems. BRICKSTORM is a sophisticated backdoor for VMware vSphere1,2 and Windows environments.3 Victim organizations are primarily in the Government Services and Facilities and Information Technology Sectors. BRICKSTORM enables cyber threat actors to maintain stealthy access and provides capabilities for initiation, persistence, and secure command and control. The malware employs advanced functionality, including multiple layers of encryption (e.g., HTTPS, WebSockets, and nested TLS), DNS-over-HTTPS (DoH) to conceal communications, and a SOCKS proxy to facilitate lateral movement and tunneling within victim networks. BRICKSTORM also incorporates long-term persistence mechanisms, such as a self-monitoring function that automatically reinstalls or restarts the malware if disrupted, ensuring its continued operation.
Links and more information:
PRC State-Sponsored Actors Use BRICKSTORM Malware Across Public Sector and Information Technology Systems | CISA

Opportunistic Pro-Russia Hacktivists Attack US and Global Critical Infrastructure
CISA, in partnership with Federal Bureau of Investigation, the National Security Agency, Department of Energy, Environmental Protection Agency, the Department of Defense Cyber Crime Center, and other international partners published a joint cybersecurity advisory, Pro-Russia Hacktivists Create Opportunistic Attacks Against US and Global Critical Infrastructure.
Links and more information:
Opportunistic Pro-Russia Hacktivists Attack US and Global Critical Infrastructure | CISA

Cybersecurity Performance Goals 2.0 for Critical Infrastructure
CISA released updated Cross-Sector Cybersecurity Performance Goals (CPG 2.0) with measurable actions for critical infrastructure owners and operators to achieve a foundational level of cybersecurity.
This update incorporates lessons learned, aligns with the most recent National Institute of Standards and Technology Cybersecurity Framework revisions, and addresses the most common and impactful threats facing critical infrastructure today.
Links and more information:
Cybersecurity Performance Goals 2.0 for Critical Infrastructure | CISA

2025 CWE Top 25 Most Dangerous Software Weaknesses

The Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the Homeland Security Systems Engineering and Development Institute (HSSEDI), operated by the MITRE Corporation, has released the 2025 Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses. This annual list identifies the most critical weaknesses adversaries exploit to compromise systems, steal data, or disrupt services.

Links and more information:

2025 CWE Top 25 Most Dangerous Software Weaknesses | CISA

CISA and Partners Release Update to Malware Analysis Report BRICKSTORM Backdoor

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency, and Canadian Centre for Cyber Security released an update to the Malware Analysis Report BRICKSTORM Backdoor with indicators of compromise (IOCs) and detection signatures for additional BRICKSTORM samples. This update provides information on additional samples, including Rust-based samples. These samples demonstrate advanced persistence and defense evasion mechanisms, such as running as background services, and enhanced command and control capabilities through encrypted WebSocket connections.

Links and more information:

CISA and Partners Release Update to Malware Analysis Report BRICKSTORM Backdoor | CISA

Protecting Tokens and Assertions from Forgery, Theft, and Misuse

NIST and CISA's draft Interagency Report Protecting Tokens and Assertions from Forgery, Theft, and Misuse is now available for public comment through January 30, 2026. This report is in response to Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144, providing implementation guidance to help federal agencies and cloud service providers (CSPs) protect identity tokens and assertions from forgery, theft, and misuse.

Links and more information:

Protecting Tokens and Assertions from Forgery, Theft, and Misuse | CISA

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in December 2025:

- Developing Industrial Internet of Things Specialization
- Development of Secure Embedded Systems Specialization
- Industrial IoT Markets and Security

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

- 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)

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

- 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

https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/#training-and-pricing

- 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

https://www.udemy.com/ics-scada-cyber-security/

- SCADA security training

https://www.tonex.com/training-courses/scada-security-training/

- 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

https://www.infosecinstitute.com/courses/scada-security-boot-camp/

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

https://www.tonex.com/training-courses/industrial-control-system-scada-cybersecurity-training/

- Bsigroup: Certified Lead SCADA Security Professional training course

https://www.bsigroup.com/en-GB/our-services/digital-trust/cybersecurity-information-resilience/Training/certified-lead-scada-security-professional/

- The Industrial Cyber Security Certification Course

https://prettygoodcourses.com/courses/industrial-cybersecurity-professional/

- Secure IACS by ISA-IEC 62443 Standard

https://www.udemy.com/course/isa-iec-62443-standard-for-secure-iacs/

- Dragos Academy ICS/OT Cybersecurity Training

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

- ISA/IEC 62443 Training for Product and System Manufacturers

https://www.ul.com/services/isaiec-62443-training-product-and-system-manufacturers?utm_mktocampaign=cybersecurity_industry40&utm_mktoadid=635856951086&campaignid=18879148221&adgroupid=143878946819&matchtype=b&device=c&creative=635856951086&keyword=industrial%20cyber%20security%20training&gclid=EAIaIQobChMI2sLO8fyv_AIVWvZ3Ch0b-QJvEAMYAyAAEgJNkvD_BwE

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

https://www.udemy.com/course/ics-scada-ot-protocol-traffic-analysis-iec-60870-5-104/

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

https://www.udemy.com/course/ics-cybersecurity/

- Lead SCADA Security Manager

https://pecb.com/en/education-and-certification-for-individuals/scada/lead-scada-security-manager

- OT/IT Security Training

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

- OT Railway Cybersecurity (OTCS)

https://informaconnect.com/ot-railway-cybersecurity-otcs/

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

https://opswatacademy.com/courses/ot-security-expert

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

https://www.yokogawa.com/eu/solutions/products-and-services/trainings-und-workshops/kompetenztrainings/ctr-008-ot-security-awareness-e-learning-course/

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

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

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/