2025 September, 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

Best Practices for Enhancing Security in Industrial Control Systems

As industries increasingly embrace automation, industrial control systems (ICS) and SCADA environments face growing cybersecurity threats. These systems run critical processes such as manufacturing lines, utilities, and energy grids, making strong protection essential to ensure both safety and operational continuity.

Key Challenges

Unlike standard IT systems, many ICS devices still rely on default settings and limited security features. Default passwords, weak authentication, and insecure remote connections leave systems vulnerable to manipulation or disruption. As remote monitoring becomes more common, strong authentication and secure communications are no longer optional - they are critical.

Best Practices for ICS Security

1. Role-Based Access Control

Assign access rights based on roles and responsibilities:

- Read-Only: view data only.
- Control: make operational changes within limits.
- Technician: adjust configurations but not critical functions.
- Supervisor: full system access except administration.
- Superuser: unrestricted system modifications.

This layered model prevents unauthorized or accidental changes to sensitive system settings.

2. Strong Password Policies

- Change all default credentials before deployment.
- Enforce complexity (upper/lowercase, numbers, symbols).
- Set expiration periods for regular password updates.
- Limit failed login attempts to block brute-force attacks.
- Encrypt stored credentials to protect against theft.

3. Secure Remote Access

- Use multi-factor authentication (MFA) with tokens, keys, or biometric factors.
- Employ VPNs and encrypted channels to prevent interception.
- Apply IP whitelisting and session timeouts to reduce exposure.

4. System Hardening

- Disable unused ports and restrict insecure protocols (e.g., MODBUS).
- Deploy firewalls and intrusion detection systems.
- Keep software and patches up to date.

5. Encryption and Data Protection

- Encrypt configuration files and credential storage.
- Use TLS/SSL for secure data transmission.
- Ensure intercepted data remains unreadable to attackers.

6. Continuous Monitoring and Auditing

- Maintain detailed audit trails of user activity.
- Use automated alerts for unauthorized access attempts.
- Regularly review access rights and password policies.

Why It Matters

Industries such as oil and gas demonstrate the importance of continuous monitoring and secure process control. From upstream exploration to downstream distribution, critical systems must not only function reliably but also resist cyber threats. Without strong authentication and protective measures, the safety and integrity of operations can be compromised.

Conclusion

Cybersecurity in ICS and SCADA is not optional - it's mission-critical. By enforcing password hygiene, applying role-based access control, securing remote authentication, and continuously monitoring activity, organizations can significantly reduce risks. Taking proactive steps today ensures that vital infrastructure remains safe, resilient, and operational tomorrow.

Source, links and more detailed information available on the following link:

https://www.thermofisher.com/blog/identifying-threats/best-practices-for-enhancing-security-in-industrial-control-systems/

ICS conferences

In October 2025, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

The IET Cyber Security Conference

The IET Cyber Security for Critical Industries Conference will focus on identifying the latest cyber security challenges facing companies today and examine how these can be mitigated against by building resilient and responsive systems. You will also get exclusive insights into new techniques and technologies. This a must-attend conference for anyone working in critical systems in the UK.

London, UK; 9th – 10th October 2025

More details can be found on the following website:

https://www.txone.com/events/iet-2025/

The Original ICS/SCADA Cybersecurity Conference

SecurityWeek's Industrial Control Systems (ICS) Cyber Security Conference is the largest and longest-running event series focused on industrial cybersecurity. Since 2002, the conference has gathered ICS cyber security stakeholders across various industries and attracts operations and control engineers, IT, government, vendors and academics.

Atlanta GA, USA; 27th – 30th October 2025

More details can be found on the following website:

https://www.icscybersecurityconference.com/

ICS incidents

Jaguar Land Rover manufacturing and retail 'severely disrupted' by cyber incident

Jaguar Land Rover (JLR), Britain's largest carmaker, has confirmed that a major cyber incident forced the company to shut down critical systems, causing severe disruption across its manufacturing and retail operations. The company emphasized that there is currently no evidence customer data has been stolen, but the impact on production has been immediate and far-reaching.

The disruption began early on a Monday morning when workers at JLR's Halewood plant in Merseyside were told not to report for work. Similar effects were felt across the company's global production network, as JLR proactively shut down its IT systems to contain the incident. According to cybersecurity experts, the scale and speed of the shutdown suggest the attackers may have targeted JLR's operational technology rather than customer-facing systems alone. Oakley Cox of Darktrace noted that halting production across multiple sites is a strong indication of serious concerns regarding manufacturing operations.

JLR issued a brief statement confirming that its "global applications" had been taken offline as a precaution and that teams were "working at pace to restart" them in a controlled manner. The company stressed that immediate steps were taken to mitigate the impact, but production and retail activities remain severely disrupted. Shares in Tata Motors, JLR's Indian parent company, fell by 0.9% following disclosure of the incident, reflecting investor concern over potential losses.

The attack comes at a time of financial strain for JLR. The company has faced declining sales, U.S. tariffs, and delays in the rollout of its new electric vehicle lineup. In the most recent quarter, pre-tax profits dropped 49%, and revenue fell by £700 million year on year. The cyber disruption, occurring during one of the busiest weeks for UK dealerships, has further complicated the firm's operations, with dealers unable to register newly released 75-plate vehicles.

Although JLR has not confirmed the nature of the attack, parallels are being drawn with recent ransomware incidents in the UK retail sector, including Marks & Spencer and the Co-op. A ransomware group called Hellcat previously claimed to have breached JLR's systems in March, though this remains unverified. The UK's National Cyber Security Centre has been notified, but no details have been released regarding attribution or recovery timelines.

The incident underscores the vulnerability of industrial and manufacturing systems to cyberattacks. By disrupting production, attackers have not only interrupted day-to-day operations but also risked exacerbating JLR's already challenging business environment. The company, which employs more than 32,000 staff across 17 UK sites, now faces the dual challenge of restoring manufacturing continuity while maintaining investor and customer confidence.

The source is available at the following link:

https://www.theguardian.com/business/2025/sep/02/jaguar-land-rover-cyber-incident-manufacturing-retail

Russian APT Attacks Kazakhstan's Largest Oil Company

Researchers from Seqrite Labs have identified a new Russia-linked threat actor, which they named "Noisy Bear." Active since at least April 2024, the group has been operating in Central Asia and recently conducted a major cyber-espionage campaign against KazMunayGas (KMG), Kazakhstan's state-owned oil and gas giant and the country's largest company.

The attackers compromised an email account belonging to a KMG finance department employee and used it to send phishing emails to colleagues. Disguised as routine internal communications about work schedules and salary adjustments, the messages contained urgent subject lines and linked to a ZIP file. Inside was a decoy document and a malicious LNK shortcut labeled "Salary Schedule.lnk." When executed, this triggered a multi-stage infection:

The first script disabled Windows AMSI (Antimalware Scan Interface) using a known bypass trick, allowing malicious code to avoid detection.

The second script used CreateRemoteThread Injection to run hidden code inside Windows Explorer, establishing a reverse shell for persistent attacker access.

KMG publicly denied being attacked, claiming instead that this was part of a penetration test or security exercise. Seqrite Labs rejected this explanation, pointing out that genuine penetration tests are rarely visible in public malware sandboxes and are conducted under NDAs. The researchers argued that the campaign clearly targeted employees and deployed tools designed for long-term covert access, which aligns with espionage rather than testing.

Forensic analysis revealed that Noisy Bear's infrastructure relied on Aeza Group, a Russian bulletproof hosting provider linked to multiple cybercrime operations.

Researchers also observed overlaps between this activity and other attacks in Central Asia, further suggesting a broader strategic campaign.

As Kazakhstan's largest enterprise, KMG plays a key role in the European energy market. At a time when European countries are reducing reliance on Russian gas due to geopolitical tensions and the war in Ukraine, a Russia-linked intrusion into Kazakhstan's energy sector suggests an effort to maintain intelligence advantage and leverage in the region. Persistent access to critical infrastructure could provide Moscow with both espionage opportunities and political influence.

Seqrite Labs concludes that if confirmed, Noisy Bear represents a strategic Russia-aligned threat actor focused on Central Asia's vital energy infrastructure.

The source is available at the following link:

https://www.darkreading.com/cyberattacks-data-breaches/russian-apt-kazakhstan-largest-oil-company

Book recommendation

The Definitive Industrial Cyber Manufacturing Cybersecurity Handbook 2025

The Manufacturing Cybersecurity Handbook 2025 is a free, in-depth resource created to help industrial organizations address today's evolving cyber threats. Written by leading CISOs, industry professionals, and OT security experts, it offers practical guidance grounded in real-world manufacturing experience.

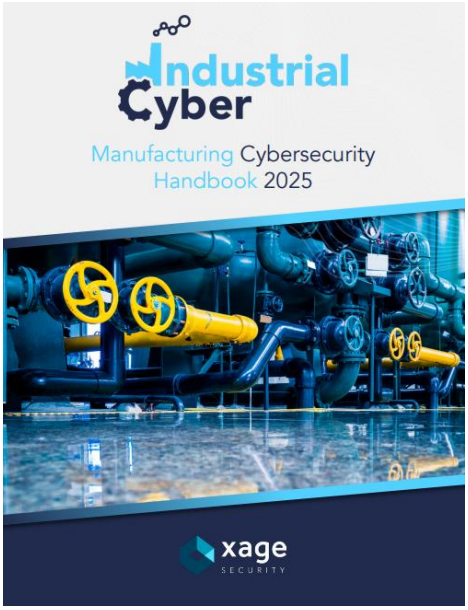
Covering IT-OT convergence, zero trust, secure remote access, disaster recovery, and more, the handbook delivers actionable strategies to strengthen resilience across both legacy and smart factory environments. It's designed for CISOs, OT leads, plant managers, and risk professionals seeking to build secure, compliant, and future-ready operations.

Author/Editor: Industrial Cyber

Year of issue: 2025

The book is available at the following link:

https://www.amazon.com/2025-2030-World-Outlook-Industrial-Cybersecurity/dp/B0D1565PJQ



ICS security news selection

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

- **Redefining industrial crown jewels in hyper-connected world as cyber-physical sabotage increases**
- **Attackers use "Contact Us" forms and fake NDAs to phish industrial manufacturing firms**
- **Using OT cybersecurity as a growth lever by protecting assets while enabling agile industrial transformation**
- **How Has IoT Security Changed Over the Past 5 Years?**
- **OT security needs continuous operations, not one-time fixes**
- **Industrial sector faces tougher cyber insurance landscape with escalating premiums, coverage gaps**
- **How a fake ICS network can reveal real cyberattacks**
- **Rising threats push industrial supply chains to adopt real-time monitoring, proactive cybersecurity practices**
- **Airport Chaos Shows Human Impact of 3rd-Party Attacks**
- **Unpatched Vulnerabilities Expose Novakon HMIs to Remote Hacking**
- **UK Cyber Growth Action Plan highlights sector expansion, rising threats as demand for resilience grows**

Redefining industrial crown jewels in hyper-connected world as cyber-physical sabotage increases

The interconnected nature of organizational systems has made it more complicated to identify and protect industrial crown jewels, especially as nation-state hackers and state-sponsored adversaries attempt to breach such environments. Apart from the physical machines and production systems, these crown jewels now include legacy equipment, digital twins, remote access gateways, and cloud platforms, with the flow of data between these technologies spread widely. These systems keep industries

functioning, but they are often frail, patchy, or next to impossible to take offline, so defense is a constant game of balancing acts. …

Source and more information:

https://industrialcyber.co/features/redefining-industrial-crown-jewels-in-hyper-connected-world-as-cyber-physical-sabotage-increases/

Attackers use "Contact Us" forms and fake NDAs to phish industrial manufacturing firms

A recently uncovered phishing campaign – carefully designed to bypass security defenses and avoid detection by its intended victims – is targeting firms in industrial manufacturing and other companies critical to various supply chains, Check Point researchers have warned.

The phishing campaign(s)

The researchers believe that the campaign has been mounted by financially motivated threat actors. …

Source and more information:

https://www.helpnetsecurity.com/2025/08/29/phishing-manufacturing-supply-chain/

Using OT cybersecurity as a growth lever by protecting assets while enabling agile industrial transformation

Rising cybersecurity threats and attacks are pushing industrial enterprises to view cybersecurity through a very different lens. OT cybersecurity is increasingly driving business objectives and innovation to safeguard operational uptime and enable greater operational flexibility. Beyond protecting continuous operations, OT security empowers critical infrastructure to pivot, innovate, and maintain resilience in dynamic industrial environments. In sectors such as manufacturing, energy, and healthcare, OT security serves to safeguard uptime and enable operational agility, innovation, and strategic flexibility. …

Source and more information:

https://industrialcyber.co/features/using-ot-cybersecurity-as-a-growth-lever-by-protecting-assets-while-enabling-agile-industrial-transformation/

How Has IoT Security Changed Over the Past 5 Years?

Internet of Things (IoT) usage has expanded across industries over the past five years and will only continue to do so, but has security grown with it? Experts say progress is not fast enough.

While organizations increasingly use IoT devices and applications to improve operational efficiency or save money, the technology is inherently insecure. It makes everything more connected, leaving a treasure trove of internet-exposed data. On top of that, many IoT devices are not equipped to receive easy vulnerability patching updates, or even alerting users that any update is needed. …

Source and more information:

https://www.darkreading.com/ics-ot-security/how-has-iot-security-changed-over-the-past-5-years-

OT security needs continuous operations, not one-time fixes

Cyberattacks keep hitting the OT systems that critical infrastructure operators run, according to new research from Forrester. In a survey of 262 OT security decision-makers, 91% reported at least one breach or system failure caused by a cyberattack in the past 18 months. These attacks disrupted essential services, damaged reputations, and created regulatory and financial consequences.

The study highlights the limits of current OT security approaches. While many vendors build products using Secure by Design principles, these controls alone do not protect complex operational environments where different systems and assets must work together. The report calls for a shift to Secure by Operations, a strategy focused on ongoing protection throughout the lifecycle of OT assets. …

Source and more information:

https://www.helpnetsecurity.com/2025/09/16/ciso-ot-cybersecurity-strategy/

Industrial sector faces tougher cyber insurance landscape with escalating premiums, coverage gaps

Filing cyber insurance claims has become a tough journey for many industrial organizations, especially because more policies now exclude coverage for attacks linked to nation-states or ‘war-like’ incidents. Take Lloyd’s of London, for instance; they mandated in 2023 that their policies won’t cover losses from state-backed cyber

incidents. This leaves organizations stuck in a difficult spot, as proving a cyberattack came from a nation-state is incredibly tough, and insurers have various reasons they can use to deny a payout. Even with a policy in hand, many firms could find themselves exposed when it matters most. Insurance companies and underwriters, in response, began getting stricter about what risks they're willing to take on in operational technology (OT) environments. …

Source and more information:

https://industrialcyber.co/features/industrial-sector-faces-tougher-cyber-insurance-landscape-with-escalating-premiums-coverage-gaps/

How a fake ICS network can reveal real cyberattacks

Researchers have introduced a new way to study and defend against ICS threats. Their project, called ICSLure, is a honeynet built to closely mimic a real industrial environment.

Why traditional honeypots fall short

Honeypots are systems designed to attract attackers so that security teams can study their behavior without putting production equipment at risk. Most ICS honeypots today are low interaction, using software to simulate devices like programmable logic controllers (PLCs). …

Source and more information:

https://www.helpnetsecurity.com/2025/09/17/icslure-ics-threat-detection/

Rising threats push industrial supply chains to adopt real-time monitoring, proactive cybersecurity practices

Supply chain cybersecurity in industrial settings mirrors the increasing complexity and interdependence of today's operations. Industrial supply chains are now subject to dynamic cyber threats at software, hardware, and service layers, prompting businesses to adopt a new age of continuous assurance. As opposed to traditional single-point safety checks, continuous assurance involves regular verification and monitoring processes that keep software and components safe throughout their lifespan. This strategy hardens security and makes it more difficult for attackers to target vulnerabilities. …

Source and more information:

https://industrialcyber.co/features/rising-threats-push-industrial-supply-chains-to-adopt-real-time-monitoring-proactive-cybersecurity-practices/

Airport Chaos Shows Human Impact of 3rd-Party Attacks

Major EU airports such as Heathrow were disrupted over the weekend after a cyberattack hit the provider of check-in kiosk software, which caused delays and flight cancellations.

A cyberattack targeting ticketing and check-in software used in several European airports caused widespread disruptions over the weekend that continued to affect flights and passengers on Monday. The ongoing incident demonstrates the human impact of increasing cyberattacks on critical infrastructure, especially through third-party software and services, security experts said. …

Source and more information:

https://www.darkreading.com/cyberattacks-data-breaches/airport-chaos-human-impact-3rd-party-attacks

Unpatched Vulnerabilities Expose Novakon HMIs to Remote Hacking

Some of the industrial control system (ICS) products made by Taiwan-based Novakon are affected by serious vulnerabilities, and the vendor does not appear to have released any patches.

A subsidiary of iBASE Technology, Novakon designs and manufactures human-machine interfaces (HMIs), industrial PCs, and IIoT solutions. The company serves 18 countries across North America, Europe and Asia. Marketing materials show that 40,000 units of Novakon's 7" HMIs have been deployed in global data centers. …

Source and more information:

https://www.securityweek.com/unpatched-vulnerabilities-expose-novakon-hmis-to-remote-hacking/

UK Cyber Growth Action Plan highlights sector expansion, rising threats as demand for resilience grows

The U.K. government report, informed by input from both the supply and demand sides of the cyber sector, focuses on the growth pillar of the refreshed National Cyber Strategy. Cybersecurity is identified as a frontier technology in the Industrial Strategy's Digital and Technologies sector plan. The UK Cyber Growth Action Plan will feed into the refreshed National Cyber Strategy and was laid in Parliament as a Command Paper last week.

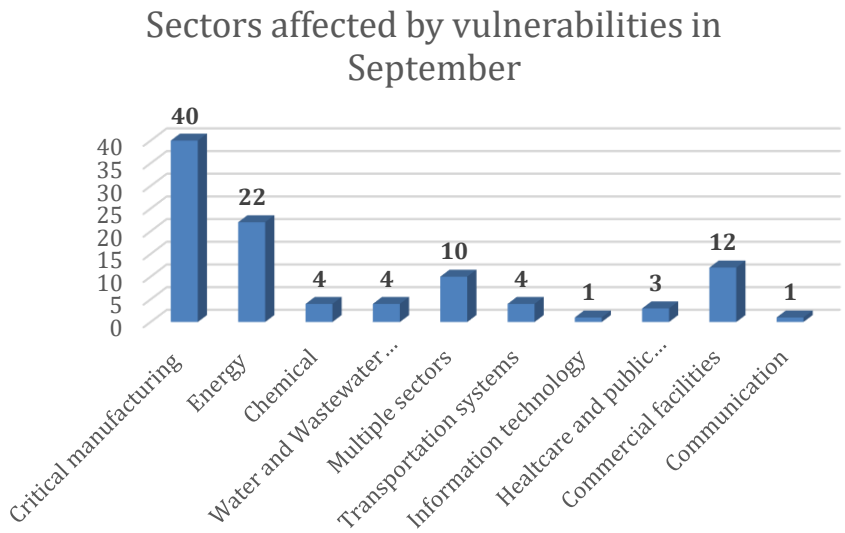
An independent report by the University of Bristol and Imperial College London, the UK Cyber Growth Action Plan provides insights on growing the U.K.'s cybersecurity sector, emphasizing resilience, value for money, and supporting the country's ambition to be the safest online. While the U.K. cyber sector is expanding, cyber threats are growing in parallel. With organizations increasingly reliant on digital infrastructure, cyber resilience is essential to sustaining broader economic growth, which in turn can drive innovation and growth within the cyber sector. …

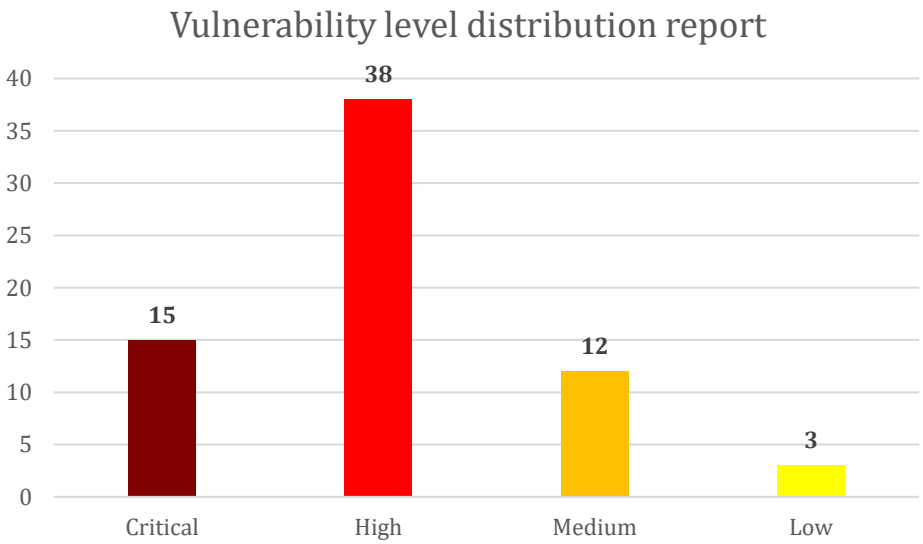
Source and more information:

https://industrialcyber.co/reports/uk-cyber-growth-action-plan-highlights-sector-expansion-rising-threats-as-demand-for-resilience-grows/

ICS vulnerabilities

In September 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-25-268-01: **Dingtian DT-R002**

High level vulnerability: Insufficiently Protected Credentials.

Dingtian DT-R002 | CISA

ICSA-25-266-01: **AutomationDirect CLICK PLUS**

High level vulnerabilities: Cleartext Storage of Sensitive Information, Use of Hard-coded Cryptographic Key, Use of a Broken or Risky Cryptographic Algorithm, Predictable Seed in Pseudo-Random Number Generator, Improper Resource Shutdown or Release, Missing Authorization.

AutomationDirect CLICK PLUS | CISA

ICSA-25-266-02: **Mitsubishi Electric MELSEC-Q Series CPU Module**

Medium level vulnerability: Improper Handling of Length Parameter Inconsistency.

Mitsubishi Electric MELSEC-Q Series CPU Module | CISA

ICSA-25-266-03: **Schneider Electric SESU**

High level vulnerability: Improper Link Resolution Before File Access ('Link Following').

Schneider Electric SESU | CISA

ICSA-25-266-04: **Viessmann Vitogate 300**

High level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Client-Side Enforcement of Server-Side Security.

Viessmann Vitogate 300 | CISA

ICSA-25-023-02: **Hitachi Energy RTU500 Series Product (Update A)**

High level vulnerability: Improperly Implemented Security Check for Standard.

Hitachi Energy RTU500 Series Product (Update A) | CISA

ICSA-25-093-01: **Hitachi Energy RTU500 Series (Update B)**

High level vulnerabilities: Null Pointer Dereference, Insufficient Resource Pool, Missing Synchronization.

Hitachi Energy RTU500 Series (Update B) | CISA

ICSA-25-261-01: **Westermo Network Technologies WeOS 5**

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

Westermo Network Technologies WeOS 5 | CISA

ICSA-25-261-02: **Westermo Network Technologies WeOS 5**

High level vulnerability: Improper Validation of Syntactic Correctness of Input.

Westermo Network Technologies WeOS 5 | CISA

ICSA-25-261-03: **Schneider Electric Saitel DR & Saitel DP Remote Terminal Unit**

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

Schneider Electric Saitel DR & Saitel DP Remote Terminal Unit | CISA

ICSA-25-261-04: **Hitachi Energy Asset Suite**

High level vulnerabilities: Server-Side Request Forgery (SSRF), Deserialization of Untrusted Data, Cleartext Storage of Sensitive Information, Uncontrolled Resource Consumption, URL Redirection to Untrusted Site ('Open Redirect'), Improper Authentication.

Hitachi Energy Asset Suite | CISA

ICSA-25-261-05: **Hitachi Energy Service Suite**

Critical level vulnerability: Deserialization of Untrusted Data.

Hitachi Energy Service Suite | CISA

ICSA-25-261-06: **Cognex In-Sight Explorer and In-Sight Camera Firmware**

High level vulnerabilities: Use of Hard-coded Password, Cleartext Transmission of Sensitive Information, Incorrect Default Permissions, Improper Restriction of Excessive Authentication Attempts, Incorrect Permission Assignment for Critical Resource, Authentication Bypass by Capture-replay, Client-Side Enforcement of Server-Side Security.

Cognex In-Sight Explorer and In-Sight Camera Firmware | CISA

ICSA-25-261-07: **Dover Fueling Solutions ProGauge MagLink LX4 Devices**

Critical level vulnerabilities: Integer Overflow or Wraparound, Use of Hard-coded Cryptographic Key, Use of Weak Credentials.

Dover Fueling Solutions ProGauge MagLink LX4 Devices | CISA

ICSA-25-191-10: **End-of-Train and Head-of-Train Remote Linking Protocol (Update C)**

High level vulnerability: Weak Authentication.

End-of-Train and Head-of-Train Remote Linking Protocol (Update C) | CISA

ICSA-24-030-02: **Mitsubishi Electric FA Engineering Software Products (Update D)**

Critical level vulnerabilities: Missing Authentication for Critical Function, Unsafe Reflection.

Mitsubishi Electric FA Engineering Software Products (Update D) | CISA

ICSA-25-259-01: **Schneider Electric Altivar Products, ATVdPAC Module, ILC992 InterLink Converter**

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

Schneider Electric Altivar Products, ATVdPAC Module, ILC992 InterLink Converter | CISA

ICSA-25-259-02: **Hitachi Energy RTU500 Series**

High level vulnerabilities: NULL Pointer Dereference, Improper Validation of Integrity Check Value, Improper Restriction of XML External Entity Reference, Heap-based Buffer Overflow, Integer Overflow or Wraparound, Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion'), Stack-based Buffer Overflow.

Hitachi Energy RTU500 Series | CISA

ICSA-25-259-03: **Siemens SIMATIC NET CP, SINEMA, and SCALANCE**

High level vulnerability: Integer Overflow or Wraparound.

Siemens SIMATIC NET CP, SINEMA, and SCALANCE | CISA

ICSA-25-259-04: **Siemens RUGGEDCOM, SINEC NMS, and SINEMA**

Critical level vulnerabilities: NULL Pointer Dereference, Out-of-bounds Write, Server-Side Request Forgery (SSRF).

Siemens RUGGEDCOM, SINEC NMS, and SINEMA | CISA

ICSA-25-259-05: **Siemens OpenSSL Vulnerability in Industrial Products**

High level vulnerability: Out-of-bounds Read.

Siemens OpenSSL Vulnerability in Industrial Products | CISA

ICSA-25-259-06: **Siemens Multiple Industrial Products**

High level vulnerability: Loop with Unreachable Exit Condition ('Infinite Loop').

Siemens Multiple Industrial Products | CISA

ICSA-25-259-07: **Delta Electronics DIALink**

Critical level vulnerability: Path Traversal.

Delta Electronics DIALink | CISA

ICSA-25-140-07: **Schneider Electric Galaxy VS, Galaxy VL, Galaxy VXL (Update A)**

Critical level vulnerability: Missing Authentication for Critical Function.

Schneider Electric Galaxy VS, Galaxy VL, Galaxy VXL (Update A) | CISA

ICSA-25-254-01: **Siemens SIMOTION Tools**

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

Siemens SIMOTION Tools | CISA

ICSA-25-254-02: **Siemens SIMATIC Virtualization as a Service (SIVaaS)**

Critical level vulnerability: Incorrect Permission Assignment for Critical Resource.

Siemens SIMATIC Virtualization as a Service (SIVaaS) | CISA

ICSA-25-254-03: **Siemens SINAMICS Drives**

Medium level vulnerability: Improper Privilege Management.

Siemens SINAMICS Drives | CISA

ICSA-25-254-04: **Siemens SINEC OS**

Low level vulnerabilities: Uncontrolled Resource Consumption, Exposure of Sensitive Information to an Unauthorized Actor.

Siemens SINEC OS | CISA

ICSA-25-254-05: **Siemens Apogee PXC and Talon TC Devices**

Medium level vulnerability: Exposure of Sensitive Information to an Unauthorized Actor.

Siemens Apogee PXC and Talon TC Devices | CISA

ICSA-25-254-06: **Siemens Industrial Edge Management OS (IEM-OS)**

High level vulnerability: Allocation of Resources Without Limits or Throttling.

Siemens Industrial Edge Management OS (IEM-OS) | CISA

ICSA-25-254-07: **Siemens User Management Component (UMC)**

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

Siemens User Management Component (UMC) | CISA

ICSA-25-254-08: **Schneider Electric EcoStruxure**

Low level vulnerabilities: Uncontrolled Resource Consumption, Exposure of Sensitive Information to an Unauthorized Actor.

Schneider Electric EcoStruxure | CISA

ICSA-25-254-09: **Schneider Electric Modicon M340, BMXNOE0100, and BMXNOE0110**

Medium level vulnerability: Files or Directories Accessible to External Parties.

Schneider Electric Modicon M340, BMXNOE0100, and BMXNOE0110 | CISA

ICSA-25-254-10: **Daikin Security Gateway**

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

Daikin Security Gateway | CISA

ICSA-25-035-06: **Schneider Electric Modicon M340 and BMXNOE0100/0110, BMXNOR0200H (Update A)**

High level vulnerability: Exposure of Sensitive Information to an Unauthorized Actor.

Schneider Electric Modicon M340 and BMXNOE0100/0110, BMXNOR0200H (Update A) | CISA

SSA-864900: **Multiple Vulnerabilities in Fortigate NGFW on RUGGEDCOM APE1808 Devices (Update: 1.3.)**

High level vulnerabilities: Insufficient Session Expiration, Out-of-bounds Write, Improperly Implemented Security Check for Standard, Authentication Bypass Using an Alternate Path or Channel, Improper Certificate Validation, Integer Overflow or Wraparound, Exposure of Sensitive Information to an Unauthorized Actor, Incorrect Privilege Assignment.

SSA-864900

SSA-712929: **Denial of Service Vulnerability in OpenSSL (CVE-2022-0778) Affecting Industrial Products (Update: 3.0.)**

High level vulnerability: Loop with Unreachable Exit Condition ('Infinite Loop').

SSA-712929

SSA-691715: **Vulnerability in OPC Foundation Local Discovery Server Affecting Siemens Products (Update: 1.7.)**

High level vulnerability: Improper Input Validation.

SSA-691715

SSA-503939: **Vulnerabilities in the BIOS of the SIMATIC S7-1500 TM MFP (Update: 1.2.)** **Medium** level vulnerabilities: Multiple.

SSA-503939

SSA-366067: **Multiple Vulnerabilities in Fortigate NGFW Before V7.4.1 on RUGGEDCOM APE1808 Devices (Update: 1.6.)**

Critical level vulnerabilities: Multiple.

SSA-366067

SSA-331739: **Privilege Escalation Vulnerability in WIBU CodeMeter Runtime Affecting Siemens Products (Update: 1.1.)**

High level vulnerability: Least Privilege Violation.

SSA-331739

SSA-282044: **DLL Hijacking Vulnerability in Siemens Web Installer used by the Online Software Delivery (Update: 1.1.)**

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: 1.9.)**

Medium level vulnerabilities: Multiple.

SSA-265688

SSA-707630: **Multiple Vulnerabilities in SIMATIC RTLS Locating Manager Before V3.3 (Update: 1.1.)**

Medium level vulnerabilities: Reachable Assertion, Insufficiently Protected Credentials.

SSA-707630

SSA-201595: **Privilege Escalation Vulnerability in WIBU CodeMeter Runtime Affecting the Desigo CC Product Family and SENTRON Powermanager (Update: 1.1.)** **High** level vulnerability: Least Privilege Violation.

SSA-201595

SSA-711309: **Denial of Service Vulnerability in the OPC UA Implementations of SIMATIC Products (Update: 2.4.)**

High level vulnerability: Integer Overflow or Wraparound.

SSA-711309

ICSA-25-252-01: **Rockwell Automation ThinManager**

High level vulnerability: Server-Side Request Forgery (SSRF).

Rockwell Automation ThinManager | CISA

ICSA-25-252-02: **ABB Cylon Aspect BMS/BAS**

Critical level vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Missing Authentication for Critical Function, Classic Buffer Overflow.

ABB Cylon Aspect BMS/BAS | CISA

ICSA-25-252-03: **Rockwell Automation Stratix IOS**

High level vulnerability: Injection.

Rockwell Automation Stratix IOS | CISA

ICSA-25-252-04: **Rockwell Automation FactoryTalk Optix**

High level vulnerability: Improper Input Validation.

Rockwell Automation FactoryTalk Optix | CISA

ICSA-25-252-05: **Rockwell Automation FactoryTalk Activation Manager**

High level vulnerability: Incorrect Implementation of Authentication Algorithm.

Rockwell Automation FactoryTalk Activation Manager | CISA

ICSA-25-252-06: **Rockwell Automation CompactLogix® 5480**

High level vulnerability: Missing Authentication for Critical Function.

Rockwell Automation CompactLogix® 5480 | CISA

ICSA-25-252-07: **Rockwell Automation ControlLogix 5580**

High level vulnerability: NULL Pointer Dereference.

Rockwell Automation ControlLogix 5580 | CISA

ICSA-25-252-08: **Rockwell Automation Analytics LogixAI**

High level vulnerability: Exposure of Sensitive System Information to an Unauthorized Control Sphere.

Rockwell Automation Analytics LogixAI | CISA

ICSA-25-252-09: **Rockwell Automation 1783-NATR**

Medium level vulnerability: Use of Platform-Dependent Third Party Components.

Rockwell Automation 1783-NATR | CISA

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

High level vulnerability: Incorrect Default Permissions.

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

ICSA-25-058-01: **Schneider Electric Communication Modules for Modicon M580 and Quantum controllers (Update B)**

Critical level vulnerability: Out-of-bounds Write.

Schneider Electric Communication Modules for Modicon M580 and Quantum Controllers (Update B) | CISA

ICSA-25-219-07: **EG4 Electronics EG4 Inverters (Update B)**

Critical level vulnerabilities: Cleartext Transmission of Sensitive Information, Download of Code Without Integrity Check, Observable Discrepancy, Improper Restriction of Excessive Authentication Attempts.

EG4 Electronics EG4 Inverters (Update B) | CISA

ICSA-25-233-01: **Mitsubishi Electric Corporation MELSEC iQ-F Series CPU Module (Update A)**

Medium level vulnerability: Improper Handling of Length Parameter Inconsistency.

Mitsubishi Electric Corporation MELSEC iQ-F Series CPU Module (Update A) | CISA

ICSA-25-226-31: **Rockwell Automation 1756-ENT2R, 1756-EN4TR, 1756-EN4TRXT (Update A)**

High level vulnerabilities: Improper Input Validation, Improper Handling of Exceptional Conditions.

Rockwell Automation 1756-ENT2R, 1756-EN4TR, 1756-EN4TRXT (Update A) | CISA

ICSA-25-247-01: **Honeywell OneWireless Wireless Device Manager (WDM)**

High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Sensitive Information in Resource Not Removed Before Reuse, Integer Underflow (Wrap or Wraparound), Deployment of Wrong Handler.

Honeywell OneWireless Wireless Device Manager (WDM) | CISA

ICSA-25-217-01: **Mitsubishi Electric Iconics Digital Solutions Multiple Products (Update A)**

Low level vulnerability: Windows Shortcut Following (.LNK).

Mitsubishi Electric Iconics Digital Solutions Multiple Products (Update A) | CISA

ICSA-25-105-07: **Delta Electronics COMMGR (Update A)**

Critical level vulnerability: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG).

Delta Electronics COMMGR (Update A) | CISA

ICSA-25-205-03: **Honeywell Experion PKS (Update A)**

Critical level vulnerabilities: Use of Uninitialized Variable, Improper Restriction of Operations within the Bounds of a Memory Buffer, Sensitive Information in Resource Not Removed Before Reuse, Integer Underflow (Wrap or Wraparound), Deployment of Wrong Handler.

Honeywell Experion PKS (Update A) | CISA

ICSA-25-191-10: **End-of-Train and Head-of-Train Remote Linking Protocol (Update B)**

High level vulnerability: Weak Authentication.

End-of-Train and Head-of-Train Remote Linking Protocol (Update B) | CISA

ICSA-25-245-01: **Delta Electronics EIP Builder**

Medium level vulnerability: Improper Restriction of XML External Entity Reference.

Delta Electronics EIP Builder | CISA

ICSA-25-245-02: **Fuji Electric FRENIC-Loader 4**

High level vulnerability: Deserialization of Untrusted Data.

Fuji Electric FRENIC-Loader 4 | CISA

ICSA-25-245-03: **SunPower PVS6**

Critical level vulnerability: Use of Hard-Coded Credentials.

SunPower PVS6 | CISA

ICSA-25-182-06: **Hitachi Energy Relion 670/650 and SAM600-IO Series (Update A)**

High level vulnerability: Allocation of Resources Without Limits or Throttling.

Hitachi Energy Relion 670/650 and SAM600-IO Series (Update A) | 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 September:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2025-57819 Sangoma FreePBX Authentication Bypass Vulnerability;
CVE-2020-24363 TP-link TL-WA855RE Missing Authentication for Critical Function Vulnerability;
CVE-2025-55177 Meta Platforms WhatsApp Incorrect Authorization Vulnerability;
CVE-2023-50224 TP-Link TL-WR841N Authentication Bypass by Spoofing Vulnerability;
CVE-2025-9377 TP-Link Archer C7(EU) and TL-WR841N/ND(MS) OS Command Injection Vulnerability;
CVE-2025-38352 Linux Kernel Time-of-Check Time-of-Use (TOCTOU) Race Condition Vulnerability;
CVE-2025-48543 Android Runtime Unspecified Vulnerability;
CVE-2025-53690 Sitecore Multiple Products Deserialization of Untrusted Data Vulnerability;
CVE-2025-5086 Dassault Systèmes DELMIA Apriso Deserialization of Untrusted Data Vulnerability;
CVE-2025-10585 Google Chromium V8 Type Confusion Vulnerability;
CVE-2021-21311 Adminer Server-Side Request Forgery Vulnerability;
CVE-2025-20352 Cisco IOS and IOS XE Stack-based Buffer Overflow Vulnerability;
CVE-2025-10035 Fortra GoAnywhere MFT Deserialization of Untrusted Data Vulnerability;
CVE-2025-59689 Libraesva Email Security Gateway Command Injection Vulnerability;
CVE-2025-32463 Sudo Inclusion of Functionality from Untrusted Control Sphere Vulnerability;
Links and more information:
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 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 Five Known Exploited Vulnerabilities to Catalog | CISA

CISA, NSA, and Global Partners Release a Shared Vision of Software Bill of Materials (SBOM) Guidance
CISA, in collaboration with NSA and 19 international partners, released joint guidance outlining A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity. This marks a significant step forward in strengthening software supply chain transparency and security worldwide.
Links and more information:

CISA, NSA, and Global Partners Release a Shared Vision of Software Bill of Materials (SBOM) Guidance | CISA

Malicious Listener for Ivanti Endpoint Mobile Management Systems

The Cybersecurity and Infrastructure Security Agency (CISA) obtained two sets of malware from an organization compromised by cyber threat actors exploiting CVE-2025-4427 and CVE-2025-4428 in Ivanti Endpoint Manager Mobile (Ivanti EPMM). Each set contains loaders for malicious listeners that enable cyber threat actors to run arbitrary code on the compromised server.

Links and more information:

Malicious Listener for Ivanti Endpoint Mobile Management Systems | CISA

SonicWall Releases Advisory for Customers after Security Incident

SonicWall released a security advisory to assist their customers with protecting systems impacted by the MySonicWall cloud backup file incident. SonicWall's investigation found that a malicious actor performed a series of brute force techniques against their MySonicWall.com web portal to gain access to a subset of customers' preference files stored in their cloud backups. While credentials within the files were encrypted, the files also included information that actors can use to gain access to customers' SonicWall Firewall devices.

CISA recommends all SonicWall customers follow guidance in the advisory,[1] which includes logging into their customer account to verify whether their device is at risk. Customers with at-risk devices should implement the advisory's containment and remediation guidance immediately.

Links and more information:

SonicWall Releases Advisory for Customers after Security Incident | CISA

CISA Releases Advisory on Lessons Learned from an Incident Response Engagement

CISA released a cybersecurity advisory detailing lessons learned from an incident response engagement following the detection of potential malicious activity identified through security alerts generated by the agency's endpoint detection and response tool. This advisory, CISA Shares Lessons Learned from an Incident Response Engagement, highlights takeaways that illuminate the urgent need for timely patching, comprehensive incident response planning, and proactive threat monitoring to mitigate risks from similar vulnerabilities.

Links and more information:

CISA Releases Advisory on Lessons Learned from an Incident Response Engagement | CISA

Widespread Supply Chain Compromise Impacting npm Ecosystem

CISA is releasing this Alert to provide guidance in response to a widespread software supply chain compromise involving the world's largest JavaScript registry, npmjs.com. A self-replicating worm—publicly known as "Shai-Hulud"—has compromised over 500 packages.[i]
After gaining initial access, the malicious cyber actor deployed malware that scanned the environment for sensitive credentials. The cyber actor then targeted GitHub Personal Access Tokens (PATs) and application programming interface (API) keys for cloud services, including Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.[ii]
Links and more information:
Widespread Supply Chain Compromise Impacting npm Ecosystem | CISA

CISA Directs Federal Agencies to Identify and Mitigate Potential Compromise of Cisco Devices
CISA issued Emergency Directive ED 25-03: Identify and Mitigate Potential Compromise of Cisco Devices to address vulnerabilities in Cisco Adaptive Security Appliances (ASA) and Cisco Firepower devices. CISA has added vulnerabilities CVE-2025-20333 and CVE-2025-20362 to the Known Exploited Vulnerabilities Catalog.
Links and more information:
CISA Directs Federal Agencies to Identify and Mitigate Potential Compromise of Cisco Devices | CISA

CISA Strengthens Commitment to SLTT Governments
The Cybersecurity and Infrastructure Security Agency (CISA) announced that it has transitioned to a new model to better equip state, local, tribal, and territorial (SLTT) governments to strengthen shared responsibility nationwide. CISA is supporting our SLTT partners with access to grant funding, no-cost tools, and cybersecurity expertise to be resilient and lead at the local level.
Links and more information:
CISA Strengthens Commitment to SLTT Governments | CISA

CISA and UK NCSC Release Joint Guidance for Securing OT Systems
CISA, in collaboration with the Federal Bureau of Investigation, the United Kingdom's National Cyber Security Centre, and other international partners has released new joint cybersecurity guidance: Creating and Maintaining a Definitive View of Your Operational Technology (OT) Architecture.
Links and more information:
CISA and UK NCSC Release Joint Guidance for Securing OT Systems | CISA

ICS trainings, education

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