BLACK CELL
Protecting critical infrastructures

Critical Systems security feed

2026 July

2026 July, Critical Systems security feed

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

List of Contents

1. Critical systems security practices, recommendations

CISA launches ANCHOR-CI to strengthen critical infrastructure security and resilience, improve cyber coordination

The Alliance of National Councils for Homeland Operational Resilience – Critical Infrastructure (ANCHOR-CI) is an advisory body chartered by the U.S. Department of Homeland Security (DHS) in June 2026. ANCHOR-CI is designed to provide group advice and recommendations to DHS through the Cybersecurity and Infrastructure Security Agency (CISA) that advance the federal government's ability to secure and protect the nation's critical infrastructure and cyberspace.

ANCHOR-CI provides a framework for collaboration, coordination, and information exchange between the federal government and stakeholder entities in the critical infrastructure community to foster a secure and resilient critical infrastructure, review current and emerging threats and vulnerabilities, exchange best practices, and encourage collaboration amongst Sector Risk Management Agencies (SRMAs) and critical infrastructure stakeholders.

As part of its statutory responsibility to "coordinate a national effort to secure and protect against critical infrastructure risks" (National Coordinator), CISA operates and administers the ANCHOR-CI framework, ensuring ANCHOR-CI serves as an effective convening mechanism for critical infrastructure partner engagement across the nation. CISA's Stakeholder Engagement Division implements the ANCHOR-CI framework through the ANCHOR-CI Executive Secretariat led by the ANCHOR-CI Designated Federal Officer (DFO).

Source and more information:

ANCHOR-CI | CISA

2. Critical systems security conferences

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

Fortinet OT Cybersecurity Summit 2026

Key Takeaways

- Global virtual summit focused on OT and critical infrastructure cybersecurity
- Actionable strategies for securing converged IT/OT environments
- Expert insights on risk management, threat intelligence, and operational resilience
- Industry-specific sessions for manufacturing, energy, utilities, biotech, and transportation
- Emphasis on practical solutions and minimizing operational disruption

The 2026 OT Cybersecurity Summit, hosted by Fortinet, is a premier virtual event dedicated to advancing the security of operational technology and critical infrastructure. This summit brings together industry leaders, security experts, and practitioners to address the evolving challenges faced by organizations as they modernize operations and integrate IT and OT environments.

Boston, Massachusetts, USA; 13th – 14th August 2026

More details can be found on the following website:

Fortinet OT Cybersecurity Summit 2026, Sunnyvale, United States | Cyber Event

21st Annual EnergySec Security & Compliance Summit

The Industrial Defender team is so excited to be exhibiting at this conference. EnergySec is putting the AND back in Security AND Compliance!

Join our team for the 21st EnergySec Security AND Compliance Summit, where the energy industry's leading minds come together to collaborate, connect, and celebrate the Power of AND.

For more than two decades, this Summit has been recognized for its insightful discussions, practical takeaways, and unmatched networking opportunities across the security and compliance community.

Stop by our booth at the event and connect with us about cybersecurity in the energy sector!

Anaheim, California, USA; 17th – 19th August 2026

More details can be found on the following website:

21st Annual EnergySec Security & Compliance Summit | Industrial Defender

Smart Manufacturing & AI Automation Convention 2026

The Smart Manufacturing Convention 2026 is the definitive event bringing together manufacturing executives, engineering leaders, and technology innovators across all sectors to explore the next generation of smart factory solutions. Hosted in the heart of North Texas - a national hub for industrial innovation - the forum connects high-level delegates who are key decision makers with 25+ leading solution providers.

From AI-powered production to predictive maintenance, supply chain optimization, and advanced robotics, attendees will discover how digital transformation is revolutionizing manufacturing across automotive, aerospace, electronics, food, and more.

Engage in high-impact keynotes, B2B networking sessions, and collaborative conversations that will shape the future of American manufacturing.

Dallas, Texas, USA; 18th – 20th August 2026

More details can be found on the following website:

Smart Manufacturing & Automation Convention 2026 – BMA

3. Critical systems security incidents

Russian Water System Hack Attempted to Turn Canada Dry

Canada's Communications Security Establishment (CSE) recently revealed that Russian state-sponsored cyber actors targeted and allegedly compromised the operational technology (OT) systems of a municipal water treatment utility in Quebec last year. This marks the first time the Canadian government has officially confirmed a direct cyber intrusion into its domestic water sector's physical control systems by geopolitical adversaries.

The utility itself failed to independently detect the intrusion, illustrating the rudimentary state of security among many OT operators. Instead, the CSE discovered the breach via an online claim of responsibility published by the Russian hacker group NoName057(16), which was relayed to Canadian authorities through CSIRTAmericas. The threat actors claimed they achieved the ability to covertly control physical processes, including water pumps, chlorine dosing, pressure settings, and localized monitoring/alert systems. While Russian hacktivist groups frequently make unfounded claims as part of information-warfare campaigns, the potential for severe physical consequences remains a high risk.

NoName057(16) has been identified in U.S. indictments as a "covert project" of Russian state security, heavily staffed by an IT organization established by order of the Russian President. Globally, the group has conducted over 1,500 attacks against governments, militaries, and critical infrastructure across Ukraine and NATO allies, leading the U.S. Department of State to offer a reward of up to $10 million for information on its members. Although European authorities conducted a major infrastructure takedown of the group in July 2025, NoName057(16) demonstrated high operational resilience, resuming activities after only a few weeks.

This incident underscores the escalating "grey zone" warfare targeting Western critical infrastructure. The CSE continues to warn the water sector about the severe risks facing internet-exposed industrial control systems (ICS). Asset owners are strongly urged to review perimeter security, isolate OT networks from the public internet, and implement continuous anomaly monitoring.

The source is available at the following link:

Russian Water System Hack Attempted to Turn Canada Dry

4. Book recommendation

Securing Operational Technology: Protecting Industrial Systems in the Digital Age

Dive into the critical Operational Technology (OT) security world with this comprehensive guide. As our industrial systems become increasingly connected, the need for robust cybersecurity measures has never been more urgent. This book offers a deep dive into the unique challenges and solutions for protecting the systems that run our power plants, manufacturing facilities, and critical infrastructure.

Written by an experienced IT & OT security specialist, this book bridges the gap between traditional IT security and the specialized needs of industrial control systems. Whether you're an OT engineer looking to enhance your security knowledge or a cybersecurity professional aiming to understand the intricacies of industrial environments, this book provides the insights and practical knowledge you need.

Author/Editor: Edgardo Fernandez Climent (Author)

Year of issue: 2024

The book is available at the following link:

Securing Operational Technology: Protecting Industrial Systems in the Digital Age: Fernandez Climent, Edgardo: 9798343468892: Amazon.com: Books

5. Critical systems security news selection

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

1. **FCC adopts new rules to secure submarine cable infrastructure deployment, support AI-driven global connectivity**
2. **While OT security is maturing, risk is not slowing down**
3. **Cydome reports FortiBleed credential leak poses elevated risks to maritime and energy critical infrastructure**
4. **EU Action Plan sets roadmap to counter AI-driven cyber threats, strengthen critical infrastructure security**
5. **Nozomi identifies Apex2 and c2c Golang malware driving faster IoT botnet attacks, raising risks for OT environments**
6. **Dozens of Minnesota Water Utilities Targeted in Coordinated OT Attacks**
7. **OT Security Startup Frenos Raises $1.52 Million**
8. **OT Environments Ever More in Hacktivist Crosshairs**
9. **Hall of Fame – Industrial Cybersecurity Power Grid Scientist Emma Stewart**
10. **SonicWall warns OT/IT convergence expanding manufacturing cybersecurity risks despite fewer detected attacks**
11. **EU releases initial CRA implementation guidance, clarifies cybersecurity obligations for manufacturers and software developers**
12. **Quantum Readiness for OT Is More Than Encryption**

FCC adopts new rules to secure submarine cable infrastructure deployment, support AI-driven global connectivity

The U.S. FCC (Federal Communications Commission) adopted new rules to accelerate deployment of secure submarine cable infrastructure, aiming to strengthen the backbone of global internet connectivity while addressing growing national security concerns. The measures streamline licensing for operators meeting high security standards, expand FCC oversight of submarine line terminal equipment, and introduce new safeguards targeting vulnerabilities tied to critical equipment and third-party service providers, as the agency seeks to support rising connectivity and AI-driven computing demands while improving resilience across communications infrastructure. …

Source and more information:

FCC adopts new rules to secure submarine cable infrastructure deployment, support AI-driven global connectivity - Industrial Cyber

While OT security is maturing, risk is not slowing down

Over the last several years, operational technology (OT) security has shifted from a specialised concern to a board-level business priority. Industrial organisations now rely on interconnected systems, remote access, cloud-based analytics, and unified IT and OT environments to maintain production. While this advanced connectivity offers increased efficiency and resilience, it has also enlarged the attack surface for cybercriminals, ransomware groups, and nation-state actors.

The 2026 Fortinet State of Operational Technology and Cybersecurity Report shows that organisations are becoming more diligent in addressing these risks. Based on a worldwide survey of over 700 OT professionals, the report highlights a market that is increasingly realistic about OT cybersecurity maturity, more alert to intrusions, and more dedicated to meeting upcoming regulatory requirements. …

Source and more information:

While OT security is maturing, risk is not slowing down | iTWire

Cydome reports FortiBleed credential leak poses elevated risks to maritime and energy critical infrastructure

A newly disclosed cyber campaign dubbed FortiBleed allegedly exposed administrator credentials for tens of thousands of internet-facing Fortinet firewalls, with maritime organizations emerging among the hardest-hit sectors. According to maritime cybersecurity firm Cydome, attackers obtained unauthorized administrative access to Fortinet devices by exploiting legacy password hashes stored in configuration files, exposing more than 86,000 confirmed working credentials across 194 countries. Cydome's analysis identified more than 250 maritime and energy organizations in the leaked dataset, including shipping companies, ports, and satellite communications providers that support maritime operations. …

Source and more information:

Cydome reports FortiBleed credential leak poses elevated risks to maritime and energy critical infrastructure - Industrial Cyber

EU Action Plan sets roadmap to counter AI-driven cyber threats, strengthen critical infrastructure security

The European Commission unveiled an Action Plan outlining a coordinated approach to address cybersecurity risks posed by advanced AI (artificial intelligence) capabilities, as adoption accelerates and need to strengthen cyber defenses across the European Union widens. The Commission warned that increasingly capable AI models are reshaping cyber

threat landscape, enabling attackers to identify vulnerabilities, automate malicious activities and launch cyberattacks at unprecedented speed and scale. Building on the EU's existing AI and cybersecurity legislation, the EU Action Plan seeks to bring together Member States, industry and EU institutions to strengthen resilience of the bloc's digital ecosystem against AI-driven threats. …

Source and more information:

EU Action Plan sets roadmap to counter AI-driven cyber threats, strengthen critical infrastructure security - Industrial Cyber

Nozomi identifies Apex2 and c2c Golang malware driving faster IoT botnet attacks, raising risks for OT environments

Cybersecurity researchers at Nozomi Networks Labs identified two Golang-based malware families, Apex2 and c2c/meow, that illustrate a growing shift in IoT botnet development toward faster, more modular and reusable malware. The researchers found that attackers are increasingly leveraging reusable open source components, commodity infrastructure and automation to rapidly assemble DDoS (distributed denial-of-service) botnets targeting exposed Linux and IoT systems, reducing the effort required to develop and deploy new malware variants. …

Source and more information:

Nozomi identifies Apex2 and c2c Golang malware driving faster IoT botnet attacks, raising risks for OT environments - Industrial Cyber

Dozens of Minnesota Water Utilities Targeted in Coordinated OT Attacks

State and federal agencies are conducting an investigation after a coordinated cyberattack hit operational technology (OT) systems at dozens of water utilities in Minnesota.

According to Minnesota IT Services (MNIT), more than 30 community water systems were targeted on July 26 and 27.

Statements issued by some of the cities whose systems have been targeted – including Maple Plain, Braham, South St. Paul, and Plymouth – revealed that some "automated control functions" were affected. Still, contingency procedures were activated and in a majority of cases water and wastewater operations remained operational. …

Source and more information:

Dozens of Minnesota Water Utilities Targeted in Coordinated OT Attacks - SecurityWeek

OT Security Startup Frenos Raises $1.52 Million

AI-native OT security startup Frenos today announced raising $1.52 million in a seed funding round extension that brings the total raised by the company to $6.4 million.

The new investment round was led by Momenta and Exposition Ventures, with additional support from Riptide Ventures.

Frenos will use the new funding to expand its customer success team and to grow its AI R&D.

In addition to the fresh funding, the startup launched SAIRA Co-Work, an AI reasoning agent designed to provide evidence-based insights during complex investigations. ...

Source and more information:

OT Security Startup Frenos Raises $1.52 Million - SecurityWeek

OT Environments Ever More in Hacktivist Crosshairs

Hacktivist groups are increasingly turning their sights to Western operational technology environments and industrial control systems, security researchers warn.

Geopolitical tensions in Eastern Europe and the Middle East have "catalyzed a surge in hacktivist collectives acting as state proxies or independent ideologues, demonstrating a growing willingness to target critical civilian infrastructure," said researchers at threat intelligence firm Kela.

Many self-proclaimed hacktivist groups wield distributed-denial-of-service attacks and website defacements as part of pro-Putin information operations. Other groups appear to be tied to Tehran. Their activities often cause little if any actual disruption but they're designed to project power, trigger headlines and stoke uncertainty (see: Russian Attacks on Polish Water Utilities Use Fear as Weapon). ...

Source and more information:

OT Environments Ever More in Hacktivist Crosshairs

US Space Cybersecurity: 'No One Is in Charge'

No single senior official is in charge of U.S. efforts to help secure commercial satellites and their land-based infrastructure against hackers, online spies and cyber attackers.

That leadership void has hampered the ability to impose cybersecurity standards on space vendors providing critical services to the U.S. government over the past eight years, said panelists at a symposium co-hosted by the George Washington University Space Policy Institute and the Aerospace Corp., a federally funded research and development center.

"If everyone's in charge, no one's in charge," said Sam Visner, a former senior U.S. official who currently chairs the Space Information Sharing and Analysis Center, or Space-ISAC, an industry-led partnership that shares threat intelligence across the space sector. ...

Source and more information:

US Space Cybersecurity: 'No One Is in Charge'

Hall of Fame – Industrial Cybersecurity Power Grid Scientist Emma Stewart

In its latest edition of its Hall of Fame series, Industrial Cyber held an in-depth conversation with Emma Stewart, who has spent over two decades working at the intersection of secure power grid development, critical infrastructure resilience, and cybersecurity. She has helped shape how governments and utilities protect some of society's most critical infrastructure installations. Her mission comes down to one line, hers, unembellished. Keep the lights on. …

Source and more information:

Hall of Fame – Industrial Cybersecurity Power Grid Scientist Emma Stewart - Industrial Cyber

SonicWall warns OT/IT convergence expanding manufacturing cybersecurity risks despite fewer detected attacks

Manufacturers are facing a more targeted cyber threat landscape as the convergence of OT (operational technology) and IT creates new pathways into production environments, according to SonicWall's 2026 Manufacturing Protect Brief. Although intrusion prevention system (IPS) detections across the manufacturing sector fell 56.2% year over year in the first half of 2026, the company said the decline does not indicate lower risk. Manufacturing still recorded 474 million IPS events during the period, while expanding connectivity through remote monitoring, predictive maintenance and vendor access is increasing the industry's attack surface and enabling more selective, high-impact attacks. …

Source and more information:

SonicWall warns OT/IT convergence expanding manufacturing cybersecurity risks despite fewer detected attacks - Industrial Cyber

EU releases initial CRA implementation guidance, clarifies cybersecurity obligations for manufacturers and software developers

The European Commission on Monday published its first guidance to help manufacturers, software developers and businesses prepare for implementation of the Cyber Resilience Act (CRA), offering practical clarification on how the regulation will apply ahead of key compliance deadlines. While the guidance is non-binding, it is intended to help organizations understand their cybersecurity obligations, prepare for mandatory reporting requirements that take effect on Sept. 11, 2026, and meet the CRA's full cybersecurity requirements before they become applicable on Dec. 11, 2027. …

Source and more information:

EU releases initial CRA implementation guidance, clarifies cybersecurity obligations for manufacturers and software developers - Industrial Cyber

Quantum Readiness for OT Is More Than Encryption

As enterprises race toward post-quantum readiness, OT environments across the power sector face a very different reality. Anwaya Bilas Sengupta, deputy general manager and alternate CISO at Grid Controller of India, explains why legacy protocols, real-time availability requirements and a fragmented vendor ecosystem mean post-quantum cryptography migration for OT will lag well behind IT, and why national quantum readiness must be measured by more than simply replacing encryption algorithms.

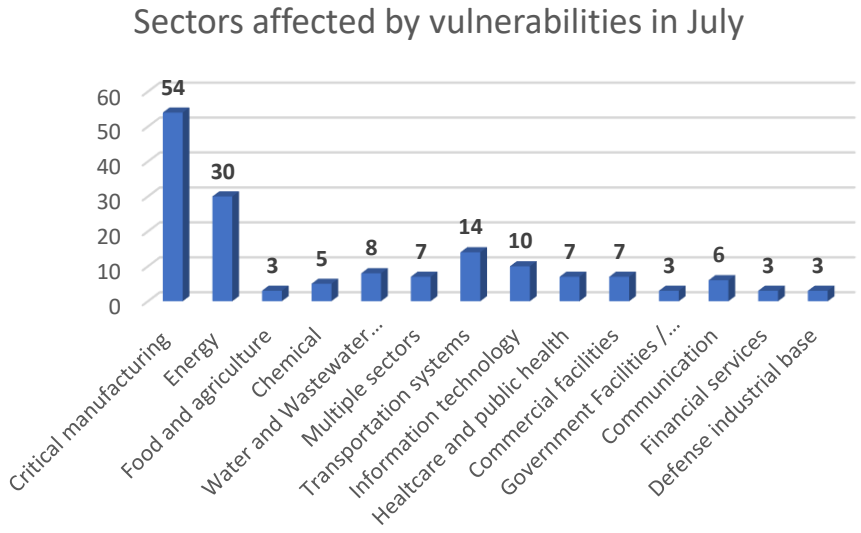
PQC migration is often framed as an IT readiness task focused on upgrading certificates, VPNs and remote access to withstand a future quantum-capable adversary. But in the power sector, OT that keeps the grid running relies on legacy kernels, proprietary OEM protocols and real-time systems that cannot tolerate downtime. Sengupta outlines why PQC adoption in OT will trail IT by several years, what a realistic migration road map entails and the steps critical infrastructure operators must take to prepare for the quantum era. …

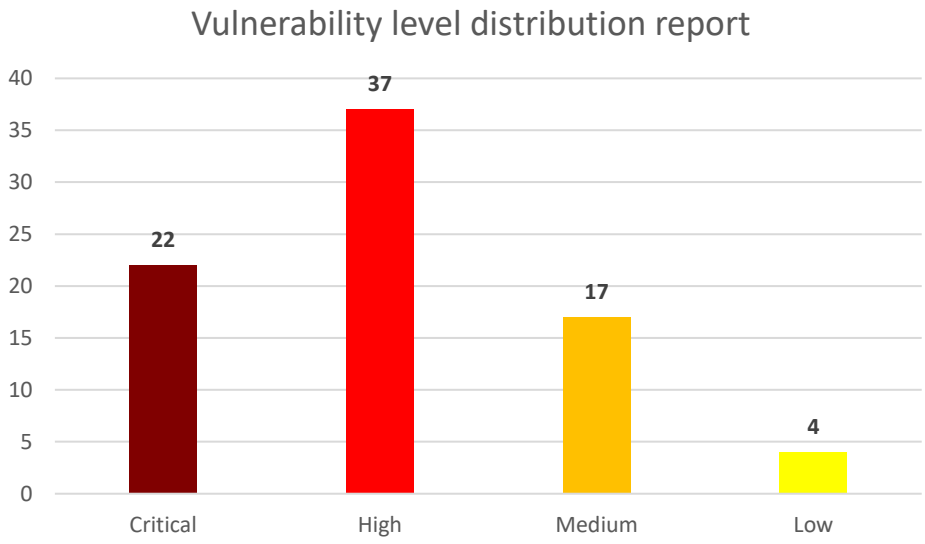
Source and more information:

Quantum Readiness for OT Is More Than Encryption

6. Critical systems vulnerabilities

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





SSA-967325: **Multiple Vulnerabilities in Palo Alto Networks PAN-OS on RUGGEDCOM APE1808 Devices (Update: 1.2.)**

Critical level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Reliance on Cookies without Validation and Integrity Checking, Server-Side Request Forgery (SSRF), Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Check for Unusual or Exceptional Conditions, Heap-based Buffer Overflow, Improper Verification of Cryptographic Signature, Improper Check for Unusual or Exceptional Conditions, Out-of-bounds Write.

SSA-967325

SSA-864900: **Multiple Vulnerabilities in Fortigate NGFW on RUGGEDCOM APE1808 Devices (Update: 1.9.)**

High level vulnerabilities: Multiple.

SSA-864900

SSA-688146: **Multiple Cross-Site Scripting Vulnerabilities in SIMATIC S7 PLCs Web Server (Update: 1.1.)**

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

SSA-688146

SSA-555707: **Information Disclosure Vulnerability in Simcenter STAR-CCM+(Update: 1.1.)** **Medium** level vulnerability: Exposure of Sensitive Information to an Unauthorized Actor.

SSA-555707

SSA-434797: **Buffer Overflow Vulnerability in OpenSSL affecting Siemens Products (Update: 1.1.)**

Critical level vulnerability: Out-of-bounds Write.

SSA-434797

SSA-392349: **Denial of Service Vulnerability in Industrial Devices (Update: 1.1.)**

High level vulnerability: NULL Pointer Dereference.

SSA-392349

SSA-082556: **Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1.5 (Update: 1.6.)**

High level vulnerabilities: Multiple.

SSA-082556

ICSA-26-211-01: **MikroTik RouterOS**

Low level vulnerability: Insufficient Session Expiration.

MikroTik RouterOS | CISA

ICSA-26-211-02: **Johnson Controls OpenBlue Employee**

Low level vulnerabilities: Unrestricted Upload of File with Dangerous Type, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS).

Johnson Controls OpenBlue Employee | CISA

ICSA-26-211-03: **Toptech Systems RCU II+ and Multiload II+**

High level vulnerability: Missing Authentication for Critical Function.

Toptech Systems RCU II+ and Multiload II+ | CISA

ICSA-26-211-04: **Schneider Electric IGSS**

High level vulnerability: Out-of-bounds Write.

Schneider Electric IGSS | CISA

ICSA-26-211-05: **Rockwell Automation CompactLogix 5380 ControlLogix 5580 / 1756-EN4 Communications Module**

Medium level vulnerability: Improper Check for Certificate Revocation.

Rockwell Automation CompactLogix 5380 ControlLogix 5580 / 1756-EN4TR Communications Module | CISA

ICSA-26-211-06: **NASA Core Flight System (cFS) Health & Safety (HS) Application**

High level vulnerability: NULL Pointer Dereference.

NASA Core Flight System (cFS) Health & Safety (HS) Application | CISA

ICSA-26-211-07: **Mitsubishi Electric CC-Link IE TSN Communication Protocol**

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

Mitsubishi Electric CC-Link IE TSN Communication Protocol | CISA

ICSA-26-211-08: **o6 Automation open62541**

High level vulnerabilities: Integer Underflow (Wrap or Wraparound), Integer Overflow or Wraparound, Use After Free.

o6 Automation open62541 | CISA

ICSA-26-211-09: **Watchfire Controller Software**

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

Watchfire Controller Software | CISA

ICSA-26-211-10: **MZ Automation GmbH libiec61850**

High level vulnerability: Out-of-bounds Read.

MZ Automation GmbH libiec61850 | CISA

ICSA-26-211-11: **MZ Automation lib60870**

Medium level vulnerability: Out-of-bounds Read.

MZ Automation lib60870 | CISA

ICSA-25-111-05: **Hardy Barth Salia EV Charge Controller (Update A)**

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

Hardy Barth Salia EV Charge Controller (Update A) | CISA

ICSA-26-209-01: **Siemens Desigo CC**

Critical level vulnerability: Out-of-bounds Write.

Siemens Desigo CC | CISA

ICSA-26-209-02: **Siemens Mendix Runtime**

Critical level vulnerability: Insecure Inherited Permissions.

Siemens Mendix Runtime | CISA

ICSA-26-209-03: **Siemens SIMATIC S7-PLCSIM Advanced**

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

Siemens SIMATIC S7-PLCSIM Advanced | CISA

ICSA-26-209-04: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP**

Critical level vulnerabilities: Missing Encryption of Sensitive Data, Missing Critical Step in Authentication, Improper Input Validation, Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution, Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'), NULL Pointer Dereference, Improper Resource Shutdown or Release, Integer Overflow or Wraparound, Use of Uninitialized Variable, Improper Enforcement of Behavioral Workflow, Use After Free, Loop with Unreachable Exit Condition ('Infinite Loop'), Reachable Assertion, Improper Locking, Memory Allocation with Excessive Size Value, Use of Uninitialized Resource, Missing Release of Memory after Effective Lifetime, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Improper Resource Locking, Out-of-bounds Write, Out-of-bounds Read, Incomplete Cleanup, Divide By Zero, Uncontrolled Recursion, Race Condition within a Thread, Missing Release of Resource after Effective Lifetime, Improper Update of Reference Count, Missing Default Case in Multiple Condition Expression, Improper Following of Specification by Caller, Exposure of Sensitive Information Due to Incompatible Policies, Expired Pointer Dereference, Incorrect Type Conversion or Cast, Multiple Releases of Same Resource or Handle, Transmission of Private Resources into a New Sphere ('Resource Leak'), Improper Handling of Invalid Use of Special Elements, Improper Neutralization of Null Byte or NUL Character, Improper Handling of Missing Special Element, Time-of-check Time-of-use (TOCTOU) Race Condition, Missing Initialization of Resource, Incorrect Privilege Assignment, Trust of System Event Data, Use of Externally-Controlled Format String, Unchecked Return

Value, Signal Handler Race Condition, Incorrect Conversion between Numeric Types, Active Debug Code, Buffer Underwrite ('Buffer Underflow'), Incorrect Synchronization, Improper Handling of Structural Elements, Improper Validation of Specified Index, Position, or Offset in Input, Incorrect Calculation of Buffer Size, Operation on a Resource after Expiration or Release, Access of Uninitialized Pointer, Improper Validation of Specified Type of Input, Plaintext Storage of a Password, Improper Handling of Length Parameter Inconsistency, Missing Report of Error Condition, Missing Synchronization, Deadlock, Buffer Access with Incorrect Length Value, Untrusted Pointer Dereference, Incorrect Resource Transfer Between Spheres, Release of Invalid Pointer or Reference, Misinterpretation of Input, Improper Null Termination, Incomplete Internal State Distinction, Access of Resource Using Incompatible Type ('Type Confusion'), Improperly Implemented Security Check for Standard, Write-what-where Condition, Improper Privilege Management.

Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP | CISA

ICSA-26-209-05: **MikroTik RouterOS and Cloud Hosted Router**

High level vulnerability: Improper Restriction of Excessive Authentication Attempts.

MikroTik RouterOS and Cloud Hosted Router | CISA

ICSA-26-209-06: **igloohome Smart Lock Mobile Application**

Medium level vulnerability: Inclusion of Sensitive Information in Source Code.

igloohome Smart Lock Mobile Application | CISA

ICSA-26-209-07: **ABB KNX Update Tool**

Medium level vulnerability: Missing Support for Integrity Check.

ABB KNX Update Tool | CISA

ICSA-26-204-01: **Johnson Controls C-CURE 9000 and Victor application server**

Critical level vulnerabilities: Server-Side Request Forgery (SSRF), Execution with Unnecessary Privileges.

Johnson Controls C-CURE 9000 and Victor application server | CISA

ICSA-26-204-02: **Johnson Controls XAAP Android**

Low level vulnerability: Cleartext Storage of Sensitive Information.

Johnson Controls XAAP Android | CISA

ICSA-26-204-03: **Weintek cMT3092X**

High level vulnerabilities: Reliance on Cookies without Validation and Integrity Checking in a Security Decision, Incorrect Permission Assignment for Critical Resource, Plaintext Storage of a Password, Incorrect User Management.

Weintek cMT3092X | CISA

ICSA-26-204-04: **Panduit Intravue**

Critical level vulnerabilities: Plaintext Storage of a Password, Unintended Proxy or Intermediary ('Confused Deputy'), Exposure of Sensitive System Information to an Unauthorized Control Sphere, Inadequate Encryption Strength.

Panduit IntraVUE | CISA

ICSA-26-204-05: **Rockwell Automation ThinManager**

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

Rockwell Automation ThinManager | CISA

ICSA-26-204-06: **MZ Automation libIEC61850**

High level vulnerabilities: Stack-based Buffer Overflow, Heap-based Buffer Overflow, Improper Handling of Syntactically Invalid Structure, NULL Pointer Dereference.

MZ Automation libIEC61850 | CISA

ICSA-26-204-07: **MZ Automation lib60870**

High level vulnerability: Out-of-bounds Read.

MZ Automation lib60870 | CISA

ICSA-26-202-01: **Tycon Systems TPDIN-Monitor-WEB2**

Critical level vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Cleartext Storage of Sensitive Information.

Tycon Systems TPDIN-Monitor-WEB2 | CISA

ICSA-26-202-02: **Siemens RUGGEDCOM APE1808 with Palo Alto Networks Virtual NGFW**

High level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Missing Authorization, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').

Siemens RUGGEDCOM APE1808 with Palo Alto Networks Virtual NGFW | CISA

ICSA-26-202-03: **Siemens Opcenter X**

Critical level vulnerability: Improper Verification of Cryptographic Signature.

Siemens Opcenter X | CISA

ICSA-26-202-04: **Siemens SIDIS Secured SmartPlug**

Critical level vulnerabilities: Improper Enforcement of Message Integrity During Transmission in a Communication Channel, Reusing a Nonce, Key Pair in Encryption, Out-of-bounds Write, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Integer Overflow or Wraparound, Out-of-bounds Read, Covert Timing Channel, Detection of Error Condition Without Action, Incorrect Authorization.

Siemens SIDIS Secured SmartPlug | CISA

ICSA-26-202-05: **Siemens IAM Client**

Medium level vulnerability: Untrusted Search Path.

Siemens IAM Client | CISA

ICSA-26-202-06: **Siemens CADRA**

Critical level vulnerabilities: Improper Input Validation, Incorrect Bitwise Shift of Integer, Out-of-bounds Write, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Integer Overflow or Wraparound, Access of Resource Using Incompatible Type ('Type Confusion').

Siemens CADRA | CISA

ICSA-26-202-07: **Rockwell Automation FactoryTalk Services Platform**

High level vulnerability: Weak Authentication.

Rockwell Automation FactoryTalk Services Platform | CISA

ICSA-26-202-08: **Rockwell Automation 1718-AENTR/1719-AENTR**

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

Rockwell Automation 1718-AENTR/1719-AENTR | CISA

ICSA-26-202-09: **Rockwell Automation 1734 POINT I/O**

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

Rockwell Automation 1734 POINT I/O | CISA

ICSA-26-202-10: **Rockwell Automation Studio 5000 Logix Designer**

High level vulnerabilities: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Incorrect Authorization, Unquoted Search Path or Element.

Rockwell Automation Studio 5000 Logix Designer | CISA

ICSA-26-197-01: **Rockwell Automation Arena**

High level vulnerability: Out-of-bounds Write.

Rockwell Automation Arena | CISA

ICSA-26-197-02: **Rockwell Automation 1756-EN2, 1756-EN3, and 1756-ENBT**

High level vulnerability: Improper Validation of Integrity Check Value.

Rockwell Automation 1756-EN2, 1756-EN3, and 1756-ENBT | CISA

ICSA-26-197-03: **NASA Core Flight System (cFS) Health & Safety (HS) Application**

High level vulnerability: NULL Pointer Dereference.

NASA Core Flight System (cFS) Health & Safety (HS) Application | CISA

ICSA-26-197-04: **AutomationDirect Productivity Suite**

High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Divide By Zero.

AutomationDirect Productivity Suite | CISA

ICSA 26-197-05: **Siemens SICAM 8**

High level vulnerabilities: Active Debug Code, Initialization of a Resource with an Insecure Default, Unverified Password Change.

Siemens SICAM 8 | CISA

ICSA-26-197-06: **Rockwell Automation CompactLogix, ControlLogix, Compact GuardLogix and GuardLogix**

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

Rockwell Automation CompactLogix, ControlLogix, Compact GuardLogix and GuardLogix | CISA

ICSA-26-197-07: **SALTO ProAccess Space**

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

SALTO ProAccess Space | CISA

ICSA-26-197-08: **Rockwell Automation Flex 5000 Adapter**

High level vulnerability: Double Free.

Rockwell Automation Flex 5000 Adapter | CISA

ICSA-26-197-09: **Rockwell Automation FactoryTalk DataMosaix**

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

Rockwell Automation FactoryTalk DataMosaix | CISA

ICSA-26-195-01: **ABB Advant Master Online Builder**

Low level vulnerability: Uncontrolled Search Path Element.

ABB Advant Master Online Builder | CISA

ICSA-26-195-02: **ABB Ability Edgenius**

High level vulnerability: Incorrect Resource Transfer Between Spheres.

ABB Ability Edgenius | CISA

ICSA-26-195-03: **ABB T-MAC Plus**

Critical level vulnerabilities: Files or Directories Accessible to External Parties, Authorization Bypass Through User-Controlled Key, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Incorrect Authorization.

ABB T-MAC Plus | CISA

ICSA-26-195-04: **Rockwell Automation 1715 EtherNet/IP Communications Module**

Critical level vulnerability: Missing Authentication for Critical Function.

Rockwell Automation 1715-AENTR EtherNet/IP Adapter | CISA

ICSA-25-352-01: **Inductive Automation Ignition (Update A)**

Medium level vulnerability: Execution with Unnecessary Privileges.

Inductive Automation Ignition (Update A) | CISA

ICSA-26-190-01: **OpenPLC v3**

Critical level vulnerability: External Control of File Name or Path.

OpenPLC v3 | CISA

ICSA-26-190-02: **Schneider Electric PowerChute Serial Shutdown**

Medium level vulnerabilities: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Encoding or Escaping of Output, Improper Restriction of Excessive Authentication Attempts, Uncontrolled Resource Consumption, Improper Validation of Specified Quantity in Input, Improper Neutralization of CRLF Sequences ('CRLF Injection'), Insertion of Sensitive Information into Log File.

Schneider Electric PowerChute Serial Shutdown | CISA

ICSA-26-190-03: **Schneider Electric Easergy MiCOM Px40 Series**

Medium level vulnerability: Use of Hard-coded Credentials.

Schneider Electric Easergy MiCOM Px40 Series | CISA

ICSA-26-188-01: **Hydro-Québec Le Circuit Electrique charging station backend**

Critical level vulnerabilities: Improper Access Control, Improper Restriction of Excessive Authentication Attempts, Insufficient Session Expiration.

Hydro-Québec Le Circuit Electrique charging station backend | CISA

ICSA-26-188-02: **Hitachi Energy PROMOD V**

High level vulnerability: Reliance on HTTP instead of HTTPS.

Hitachi Energy PROMOD V | CISA

ICSA-26-188-03: **Hitachi Energy e-mesh EMS**

High level vulnerability: Heap-based Buffer Overflow.

Hitachi Energy e-mesh EMS | CISA

ICSA-26-188-04: **Siemens Mendix Studio Pro**

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

Siemens Mendix Studio Pro | CISA

ICSA-26-188-05: **Siemens SINEC OS**

Critical level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Resource Shutdown or Release, Integer Overflow or Wraparound, Stack-based Buffer Overflow, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Uncontrolled Recursion, Out-of-bounds Read, Covert Timing Channel, Improper Input Validation, Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution'), Improper Update of Reference Count, Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'), Multiple Releases of Same Resource or Handle, Permissive Regular Expression, Expired Pointer Dereference, Incorrect Bitwise Shift of Integer, Out-of-bounds Write, User Interface (UI) Misrepresentation of Critical Information, Improper Access Control, Insertion of Sensitive Information Into Sent Data, Inefficient Algorithmic Complexity, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Authentication Bypass by Primary Weakness, NULL Pointer Dereference, Active Debug Code, Loop with Unreachable Exit Condition ('Infinite Loop'), Missing Synchronization, External Control of File Name or Path, Privilege Dropping / Lowering Errors, Use of Web Browser Cache Containing Sensitive Information.

Siemens SINEC OS | CISA

ICSA-26-188-06: **Labcenter Proteus 9**

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

Labcenter Proteus 9 | CISA

ICSA-26-188-07: **Digi International PortServer TS, Digi One SP IA9**

Medium level vulnerabilities: Incorrect Authorization, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

Digi International PortServer TS, Digi One SP IA | CISA

ICSA-26-183-01: **ST Engineering iDirect iQ-Series Terminals**

High level vulnerabilities: Missing Authentication for Critical Function, Cross-Site Request Forgery (CSRF).

ST Engineering iDirect iQ-Series Terminals | CISA

ICSA-26-183-02: **CubeSpace CW0057 Reaction Wheel**

Medium level vulnerability: Improper Verification of Cryptographic Signature.

CubeSpace CW0057 Reaction Wheel | CISA

ICSA-26-183-03: **Gardyn IoT Hub**

Critical level vulnerabilities: Use of Hard-coded Credentials, Exposure of Sensitive System Information to an Unauthorized Control Sphere, Improper Neutralization of HTTP Headers for Scripting Syntax.

Gardyn IoT Hub | CISA

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

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

Mitsubishi Electric CNC Series (Update D) | CISA

ICSA-26-055-03: **Gardyn Home Kit (Update B)**

Critical level vulnerabilities: Cleartext Transmission of Sensitive Information, Use of Default Credentials, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Use of Hard-coded Credentials, Missing Authentication for Critical Function, Authorization Bypass Through User-Controlled Key, Active Debug Code.

Gardyn Home Kit (Update B) | CISA

ICSMA-25-364-01: **WHILL Model C2 Electric Wheelchairs and Model F Power Chairs (Update B)**

Critical level vulnerability: Missing Authentication for Critical Function.

WHILL Model C2 Electric Wheelchairs and Model F Power Chairs (Update B) | CISA

ICSMA-26-181-01: **OFFIS DCMTK Toolkit**

Critical level vulnerabilities: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Missing Release of Memory after Effective Lifetime, Access of Resource Using Incompatible Type ('Type Confusion').

OFFIS DCMTK Toolkit | CISA

ICSA-26-181-01: **Mitsubishi Electric MELSOFT Update Manager SW1DND-UDM-M**

High level vulnerabilities: Heap-based Buffer Overflow, NULL Pointer Dereference, Improper Link Resolution Before File Access ('Link Following'), Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

Mitsubishi Electric MELSOFT Update Manager SW1DND-UDM-M | CISA

ICSA-26-181-02: **Frangoteam FUXA SCADA/HMIM**

High level vulnerability: Authentication Bypass by Spoofing.

Frangoteam FUXA SCADA/HMI | CISA

ICSA-26-181-03: **Schneider Electric EcoStruxure IT Data Center Expert**

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

Schneider Electric EcoStruxure IT Data Center Expert | CISA

ICSA-26-181-04: **Schneider Electric EasyLogic T150 and Saitel DP RTU**

High level vulnerabilities: Insufficiently Protected Credentials, Incorrect Permission Assignment for Critical Resource.

Schneider Electric EasyLogic T150 and Saitel DP RTU | CISA

ICSA-26-181-05: **XZ Utils vulnerability impacting B&R Products**

High level vulnerability: Race Condition within a Thread.

XZ Utils vulnerability impacting B&R Products | CISA

ICSA-26-181-06: **StoneFly Storage Concentrator**

Critical level vulnerabilities: Use of Hard-coded Credentials, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

StoneFly Storage Concentrator | CISA

ICSA-26-181-07: **Delta Electronics DVP12SE PLC**

Critical level vulnerabilities: Missing Authentication for Critical Function, Allocation of Resources Without Limits or Throttling.

Delta Electronics DVP12SE PLC | CISA

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

ICS Advisories | CISA

Cybersecurity Alerts & Advisories | CISA

CERT Services | Services | Siemens Siemens global website

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

7. Critical systems security alerts

CISA has published alerts in 2026 July:

CISA Adds Known Exploited Vulnerabilities to Catalog

CVE-2026-45659 Microsoft SharePoint Server Deserialization of Untrusted Data Vulnerability;

Links and more information:

CISA Adds One Known Exploited Vulnerability to Catalog | CISA

Improve Router Hygiene to Protect Against Russian State-Sponsored Targeting

Russian Federal Security Service (FSB) Center 16 cyber actors continue to exploit poorly configured and vulnerable networking devices worldwide, opportunistically compromising multiple critical infrastructure sector networks. This joint Cybersecurity Advisory (CSA) builds on FBI's Russian Government Cyber Actors Targeting Networking Devices, Critical Infrastructure Public Service Announcement of the decade-plus FSB Center 16 cyber activity by providing additional tactics, techniques, and procedures (TTPs) to enable defenders to more fully understand and counter the threat.

Links and more information:

Improve Router Hygiene to Protect Against Russian State-Sponsored Targeting | CISA

CISA Urges SharePoint Hardening After New Exploitations

CISA is aware of active exploitation of vulnerabilities CVE-2026-32201, CVE-2026-45659, CVE-2026-56164, CVE-2026-58644, and CVE-2026-50522 enabling cyber threat actors to gain unauthorized access to on-premises SharePoint Server instances. These vulnerabilities affect all supported on-premises SharePoint Server versions (Subscription Edition, 2019, and 2016) and involve establishing remote code execution (RCE) and post-exploitation activities, such as stealing Internet Information Services (IIS) machine keys and performing deserialization techniques, to gain persistence and deploy malware. Organizations should monitor affected SharePoint Servers closely for any signs of exploitation or unusual activity.

Links and more information:

CISA Urges SharePoint Hardening After New Exploitations | CISA

Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure

The authoring agencies urgently warn U.S. organizations of ongoing Iranian-affiliated cyber targeting of internet-connected operational technology (OT) devices, including programmable logic controllers (PLCs). These actions disrupted PLCs across several U.S. critical infrastructure sectors through malicious project file interactions and manipulation of data on human machine interface (HMI) and supervisory control and data acquisition (SCADA) displays, resulting in operational disruption and financial loss.

Links and more information:

Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure | CISA

Russian State-Supported Cyber Actors Conduct Phishing Campaign Targeting Users of Zimbra Collaboration Suite

A group of Russian state-supported cyber actors has been targeting and compromising various Western government and commercial organizations using the Zimbra Collaboration Suite (ZCS) software since at least July 2025. The Russian state-supported advanced persistent threat (APT) group's activity is tracked in the cybersecurity community under several names (see Cybersecurity industry tracking), primarily as "LAUNDRY BEAR," a name initially coined by the Netherlands General Intelligence and Security Service (AIVD) and Defence Intelligence and Security Service (MIVD).

Links and more information:

Russian State-Supported Cyber Actors Conduct Phishing Campaign Targeting Users of Zimbra Collaboration Suite | CISA

CISA Urges Water and Wastewater Systems Sector to Protect OT Against Activity Targeting PLCs

CISA is currently observing a significant increase in cyber threat actors targeting programmable logic controllers (PLCs) in the Water and Wastewater Systems (WWS) Sector. CISA urges critical infrastructure owners, operators, and integrators to remove publicly exposed PLCs and other operational technology (OT) from the internet as soon as possible. Threat actors targeting exposed PLCs have modified passwords to lock out operators and disconnected the PLCs by changing their IP addresses. This activity has resulted in boil water notices and sustained manual operations.

Links and more information:

CISA Urges Water and Wastewater Systems Sector to Protect OT Against Activity Targeting PLCs | CISA

8. Critical systems security trainings, education

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

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

Coursera | Online Courses From Top Universities. Join for Free

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

ICS Training Available Through CISA | CISA

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

ICS410: ICS/SCADA Security Essentials | SANS Institute

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

ICS/SCADA Cyber Security

- SCADA security training

SCADA Security Training | SCADA Security Training Course

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

https://scadahacker.com/training.html

- INFOSEC-Flex SCADA/ICS Security Training Boot Camp

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

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

Industrial Control System and SCADA Cybersecurity Training - Tonex Training

- Bsigroup: Certified Lead SCADA Security Professional training course

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

- The Industrial Cyber Security Certification Course

Certified Industrial Cybersecurity Professional Certification | CICP Course

- Secure IACS by ISA-IEC 62443 Standard

Secure IACS by ISA-IEC 62443 Standard

- Dragos Academy ICS/OT Cybersecurity Training

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

- ISA/IEC 62443 Training for Product and System Manufacturers

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

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

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

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

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

- Lead SCADA Security Manager

Lead SCADA Security Manager | PECB

- OT/IT Security Training

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

- OT Railway Cybersecurity (OTCS)

OT Railway Cybersecurity (OTCS) Training - Informa Academy

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

OT Security Expert - OPSWAT Academy

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

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

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

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

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

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

!!! New in this feed!!!

- Operational Technology (OT) Security Learning Path

Infosec's Operational Technology (OT) Security Learning Path

9. Critical systems security podcasts

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

Dale Peterson

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

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

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

Industrial Cybersecurity Pulse

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

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

BEERISAC: OT/ICS Security Podcast Playlist

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

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

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