2025 August, 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

Essential Cybersecurity Practices for Protecting Industrial Infrastructure

Understand the practices necessary to shield critical infrastructure from cyber threats that could disrupt operations or endanger lives.

SANS Institute, a leading cybersecurity training provider, empowers cybersecurity professionals through top-notch training, certifications, and degree programs, all designed to enhance global security. Dragos, an industrial cybersecurity firm, specializes in providing software, cyber threat intelligence, and professional services to protect critical infrastructure. SANS, in partnership with Dragos, present a new blog series that delves into the critical aspects of OT cybersecurity. This series aims to educate both practitioners and executives on the intricacies of securing operational environments. This is Part 3. If you're new to this blog series, read Part 1 here and Part 2 here.

In an era where industrial operations increasingly rely on digital technologies, the security of operational technology (OT) and industrial control systems (ICS) is paramount. The latest blog from Dragos, titled "The Five Critical Controls for Industrial Cybersecurity," underscores the practices necessary to shield critical infrastructure from cyber threats that could disrupt operations or endanger lives.

Key Controls for Effective OT Cybersecurity Programs:

1. ICS Incident Response Plan
2. Defensible Architecture
3. ICS Network Visibility and Monitoring
4. Secure Remote Access
5. Risk-Based Vulnerability Management

Utilizing the Five Critical Controls

Dragos emphasizes the importance of these controls with an easy-to-follow infographic and a Benchmarking Worksheet, helping organizations assess their cybersecurity maturity and make informed enhancements. For access to these resources as well as a comprehensive guide to implementing these controls, read the full blog here.

Enhance Your Cybersecurity Knowledge

For professionals looking to deepen their understanding of the distinctions between ICS/OT and IT security, SANS Institute offers a valuable free resource. Our white paper, The Five ICS Cybersecurity Critical Controls, provides clear details and implementation guidance on the five most relevant critical controls for an ICS/OT cybersecurity strategy. Download the free SANS white paper here.

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

https://www.sans.org/blog/essential-cybersecurity-practices-for-protecting-industrial-infrastructure

ICS conferences

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

CS4CA Nordic Summit Co-Hosted With Nordic Cyber Summit

With the CS4CA series seeing success across the globe, the Cyber Security for Critical Assets Summit launches in Copenhagen in September 2025! Over 2 days, IT & OT security leaders from across critical infrastructure will unite for 2-days of insight building and expert knowledge exchange for safeguarding their assets from cyber threats.

Copenhagen, Denmark; 10th – 11th September 2025

More details can be found on the following website:

https://nordic.cs4ca.com/

12th Cyber and SCADA Security for Energy, Power & Utilities Industry 2025

Join top cybersecurity leaders, OT/IT professionals, and infrastructure operators at the 12th Cyber and SCADA Security for Energy, Power & Utilities Industry 2025 conference to explore the latest strategies, technologies, and regulations shaping cyber defense in the energy sector.

This focused, two-day event will cover SCADA and ICS protection, NIS2 compliance, AI-driven threat detection, and OT/IT convergence.

Engage in high-impact discussions, real-world case studies, and expert panels with decision-makers from Europe’s leading TSOs, DSOs, and utility companies.

With expert speakers and unparalleled networking opportunities, this conference is designed to equip you with the tools to safeguard critical infrastructure, ensure grid reliability, and stay ahead of emerging threats.

Don’t miss this opportunity to enhance your cybersecurity strategy and build resilience in an increasingly connected energy ecosystem.

Berlin, Germany; 23rd – 24th September 2025

More details can be found on the following website:

https://cyber-scada-power-utilities.com/

Kaspersky Industrial Cybersecurity Conference 2025

Kaspersky Industrial Cybersecurity Conference — is a global conference in the field of industrial cybersecurity, which annually brings together leading information security experts, researchers, industrial automation suppliers, system integrators and customers from around the world.

They invite you to take part in a conference dedicated to the study of threats and vulnerabilities in automated process control systems, the use of promising technologies and approaches to the construction of automated process control system information security, industry regulations, as well as real cases of implementation and application of solutions.

Sochi, Russia; 23rd – 25th September 2025

More details can be found on the following website:

https://ics.kaspersky.com/conference/

ICS incidents

Cyber Espionage Group Targets Singapore's Critical Infrastructure

On July 18, 2025, Singapore's Coordinating Minister for National Security, K. Shanmugam, announced that the country is responding to cyberattacks against its critical infrastructure carried out by an espionage group known as UNC3886. According to security experts, UNC3886 is believed to have links to China.

Shanmugam described UNC3886 as a serious threat with the capacity to undermine Singapore's national security, emphasizing that the group is targeting "high-value strategic threat targets" and vital systems that deliver essential services. Due to the sensitivity of the matter, no technical details or specific consequences of the attacks were disclosed.

Mandiant, a Google-owned cybersecurity company, has previously identified UNC3886 as a "China-nexus espionage group" known for targeting defense, technology, and telecommunications organizations in both the United States and Asia. The group is suspected of conducting long-term intelligence-gathering operations through advanced intrusion techniques.

The Chinese government has consistently denied any involvement in such activities, maintaining that it opposes all forms of cyberattacks and is itself a victim of cyber threats. The Chinese embassy in Singapore did not issue an immediate response to the allegations.

Singapore's critical infrastructure sectors, as defined by its Cyber Security Agency, encompass:

- Energy
- Water
- Banking and finance
- Healthcare
- Transport
- Government services
- Communication and media
- Security and emergency services

This disclosure comes amid a wider pattern of alleged China-linked cyber espionage campaigns in the Asia-Pacific region. Earlier in the week, Reuters reported that hackers connected to China had targeted the Taiwanese semiconductor industry and investment analysts, underscoring the escalating cyber threat landscape in the region. The source is available on the following link:

Singapore says cyber espionage group targeting critical infrastructure | Reuters

Book recommendation

The 2025-2030 World Outlook for Industrial Cybersecurity

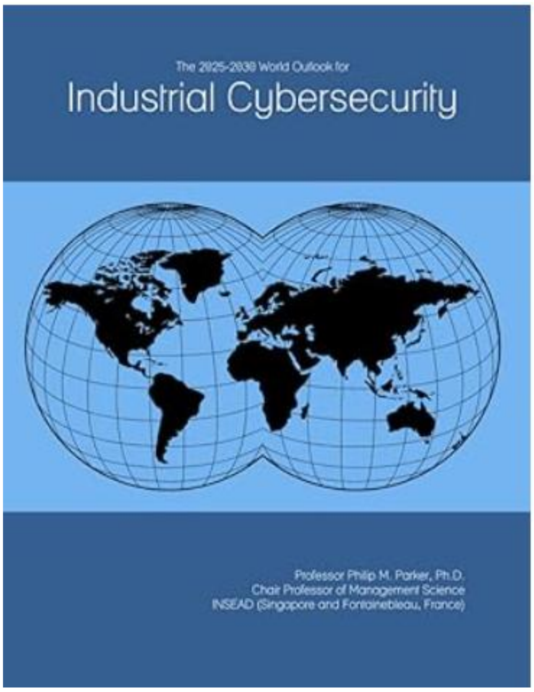
This study covers the world outlook for industrial cybersecurity across more than 190 countries. For each year reported, estimates are given for the latent demand, or potential industry earnings (P.I.E.), for the country in question (in millions of U.S. dollars), the percent share the country is of the region, and of the globe. These comparative benchmarks allow the reader to quickly gauge a country vis-à-vis others. Using econometric models which project fundamental economic dynamics within each country and across countries, latent demand estimates are created. This report does not discuss the specific players in the market serving the latent demand, nor specific details at the product level. The study also does not consider short-term cyclicalities that might affect realized sales. The study, therefore, is strategic in nature, taking an aggregate and long-run view, irrespective of the players or products involved.

Author/Editor: Prof Philip M. Parker Ph.D. (Author)

Year of issue: 2024

The book is available at the following link:

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


The 2025-2030 World Outlook for
Industrial Cybersecurity
Professor Philip M. Parker, Ph.D.
Chair Professor of Management Science
INSEAD (Singapore and Fontainebleau, France)

ICS security news selection

CISO Conversations: How IT and OT Security Worlds Are Converging

Dark Reading's Kelly Jackson Higgins interviews Carmine Valente, deputy CISO at Con Edison, about his role at the New York-based electric utility and the state of IT and OT security. Valente highlights current threats, including ransomware and supply chain attacks, as well as the impact of AI on both defense and threats. ...

Source and more information:

https://www.darkreading.com/ics-ot-security/ciso-conversations-convergence-of-it-and-ot-security

Order Out of Chaos – Using Chaos Theory Encryption to Protect OT and IoT

Chaos is unpredictable – but research demonstrates that chaos theory can be manipulated to provide strong security.

Ravi Monani, a design engineer at AMD, is on a journey to provide secure encryption for small resource-constrained edge devices such as, but not entirely limited to, Internet of Things (IoT). The chosen route is to control chaos – or more specifically harness chaos theory.

The need

The need for secure encryption in IoT and IIoT devices is obvious, and potentially critical for OT and, by extension, much of the critical infrastructure. ...

Source and more information:

https://www.securityweek.com/order-out-of-chaos-using-chaos-theory-encryption-to-protect-ot-and-iot/

Mounting OT cyber risks demand stronger cyber-physical security to protect legacy systems and operational continuity

Rising adoption of 5G, edge computing, and IoT technologies across operational technology (OT) environments is driving organizations to rethink how they protect interconnected machines and critical processes, as cyber-physical security becomes increasingly intertwined. Such integration creates a two-pronged challenge, which includes how to keep operational safety in real-time and contend with policy timelines that are measured in years to secure legacy systems never designed with today’s threat landscape. ...

Source and more information:

https://industrialcyber.co/features/mounting-ot-cyber-risks-demand-stronger-cyber-physical-security-to-protect-legacy-systems-and-operational-continuity/

Utilities, Factories at Risk From Encryption Holes in Industrial Protocol

The OPC UA communication protocol is widely used in industrial settings, but despite its complex cryptography, the open source protocol appears to be vulnerable in a number of different ways.

Despite the promises of OPC UA, a standardized, open source communication protocol often used in industrial settings as a replacement for VPNs, turns out to have a number of vulnerabilities, issues, and potential for exploits.

Last week, Tom Tervoort, principal security specialist for Secura, hosted a session at DEF CON 33 dedicated to OPC UA (short for Open Platform Communications Unified Architecture), which was first introduced in 2006. The protocol includes its own cryptographic authentication and transport security layer, and is interoperable between different vendors. ...

Source and more information:

https://www.darkreading.com/vulnerabilities-threats/utilities-factories-encryption-holes-industrial-protocol

Russian Hacktivists Take Aim at Polish Power Plant, Again

Russian hackers targeted a Polish hydropower plant again, this time disrupting its control systems and turbines.

The power plant — located in Tczew, near Gdańsk — was previously targeted in May. Now the hacktivists have released a video, which at first appeared to be a recording of the earlier attack. However, upon closer inspection, it's clear that the same hacktivists targeted the same facility again.

According to the collected data from the plant's turbines, Polish analysts believe that the hack disrupted operations, making this attack more destructive than the previous one, which allegedly occurred when the plant was offline. ...

Source and more information:

https://www.darkreading.com/cyberattacks-data-breaches/russian-hacktivists-polish-power-plant-attack

The energy sector has no time to wait for the next cyberattack

The energy sector remains a major target for cybercriminals. Beyond disrupting daily routines, a power outage can undermine economic stability and public safety. Rising demand for electricity, fueled by technology and digital growth, only adds to the sector’s vulnerability. A major driver of that demand is artificial intelligence: Goldman Sachs predicts that data center power consumption could rise by 160% by 2030, as AI’s enormous energy appetite strains already fragile grids. …

Source and more information:

https://www.helpnetsecurity.com/2025/08/26/energy-sector-cyber-risks/

Water Systems Under Attack: Norway, Poland Blame Russia Actors

Nation-state cyberattackers are increasingly targeting water and wastewater systems, causing concern following attacks on the critical utilities in Norway, Poland, and the US, and shining a light on the lack of readiness of multiple countries' water infrastructure.

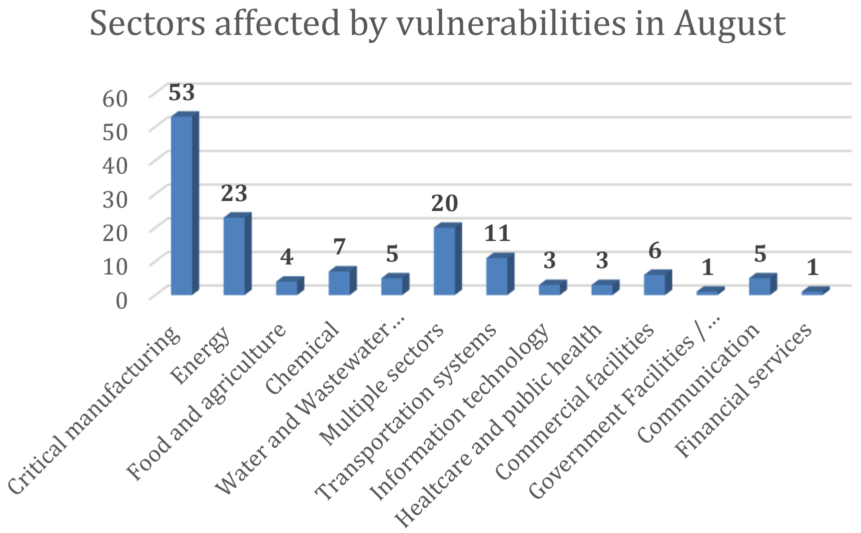
On Aug. 13, the head of Norway's counter-intelligence agency blamed Russian hackers for an April attack on a dam that allowed the attackers to open a flood gate and dump 500 liters of water per second for about four hours. The attribution of the hack underscores the vulnerability of water systems and the potential for them to become pawns in geopolitics. …

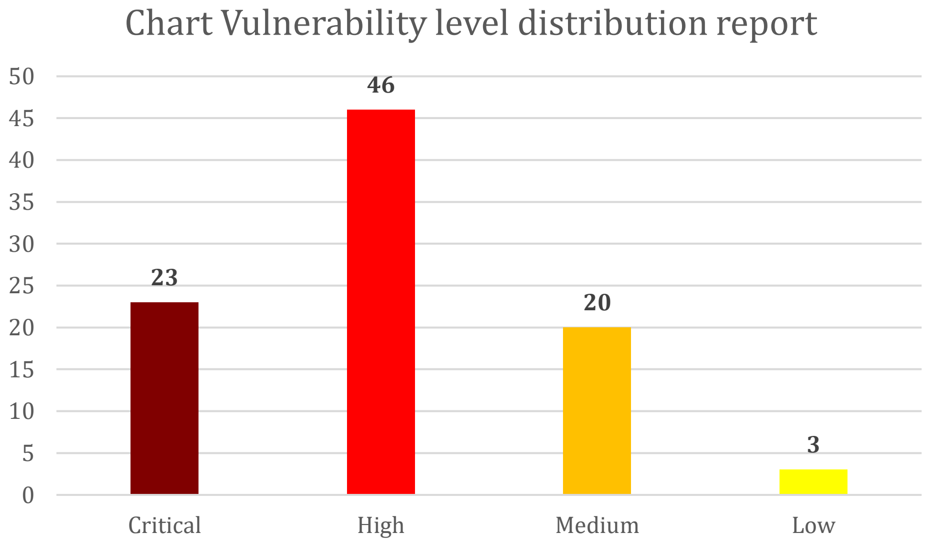
Source and more information:

https://www.darkreading.com/ics-ot-security/water-systems-attack-norway-poland-russia-actors

ICS vulnerabilities

In August 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-25-240-01: **Mitsubishi Electric MELSEC iQ-F Series CPU Module**

Medium level vulnerability: Missing Authentication for Critical Function.

Mitsubishi Electric MELSEC iQ-F Series CPU Module | CISA

ICSA-25-240-02: **Mitsubishi Electric MELSEC iQ-F Series CPU Module**

High level vulnerability: Cleartext Transmission of Sensitive Information.

Mitsubishi Electric MELSEC iQ-F Series CPU Module | CISA

ICSA-25-240-03: **Schneider Electric Saitel DR & Saitel DP Remote Terminal Unit**

Medium level vulnerability: Improper Privilege Management.

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

ICSA-25-240-04: **Delta Electronics CNCSoft-G2**

High level vulnerability: Out-of-bounds Write.

Delta Electronics CNCSoft-G2 | CISA

ICSA-25-240-05: **Delta Electronics COMMGR**

High level vulnerabilities: Stack-based Buffer Overflow, Code Injection.

Delta Electronics COMMGR | CISA

ICSA-25-240-06: **GE Vernova CIMPLICITY**

High level vulnerability: Uncontrolled Search Path Element.

GE Vernova CIMPLICITY | CISA

ICSA-24-135-04: **Mitsubishi Electric Multiple FA Engineering Software Products (Update D)**

Low level vulnerabilities: Improper Privilege Management, Uncontrolled Resource Consumption, Out-of-bounds Write.

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

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

Medium level vulnerability: Execution with Unnecessary Privileges.

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

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

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

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

ICSA-25-238-01: **INVT VT-Designer and HMITool**

High level vulnerabilities: Out-of-bounds Write, Access of Resource Using Incompatible Type ('Type Confusion').

INVT VT-Designer and HMITool | CISA

ICSA-25-238-03: **Schneider Electric Modicon M340 Controller and Communication Modules**

High level vulnerability: Improper Input Validation.

Schneider Electric Modicon M340 Controller and Communication Modules | CISA

ICSA-25-140-03: **Danfoss AK-SM 8xxA Series (Update A)**

High level vulnerabilities: Improper Authentication, Command Injection, External Control of System or Configuration Setting.

Danfoss AK-SM 8xxA Series (Update A) | CISA

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

Medium level vulnerability: Improper Handling of Length Parameter Inconsistency.

Mitsubishi Electric Corporation MELSEC iQ-F Series CPU Module | CISA

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

Critical level vulnerability: Missing Authentication for Critical Function.

Mitsubishi Electric Air Conditioning Systems (Update A) | CISA

ICSMA-25-233-01: **FUJIFILM Healthcare Americas Synapse Mobility**

Medium level vulnerability: External Control of Assumed-Immutable Web Parameter.

FUJIFILM Healthcare Americas Synapse Mobility | CISA

ICSA-25-231-01: **Siemens Desigo CC Product Family and SENTRON Powermanager**

High level vulnerability: Least Privilege Violation.

Siemens Desigo CC Product Family and SENTRON Powermanager | CISA

ICSA-25-231-02: **Siemens Mendix SAML Module**

High level vulnerability: Improper Verification of Cryptographic Signature.

Siemens Mendix SAML Module | CISA

ICSA-25-217-02: **Tigo Energy Cloud Connect Advanced (Update A)**

Critical level vulnerabilities: Use of Hard-coded Credentials, Command Injection, Predictable Seed in Pseudo-Random Number Generator (PRNG).

Tigo Energy Cloud Connect Advanced (Update A) | CISA

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

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 A) | CISA

ICSA-25-226-01: **Siemens SIMATIC RTLS Locating Manager**

Medium level vulnerabilities: Reachable Assertion, Insufficiently Protected Credentials.

Siemens SIMATIC RTLS Locating Manager | CISA

ICSA-25-226-02: **Siemens COMOS**

High level vulnerability: Out-of-bounds Write.

Siemens COMOS | CISA

ICSA-25-226-03: **Siemens Engineering Platforms**

High level vulnerability: Deserialization of Untrusted Data.

Siemens Engineering Platforms | CISA

ICSA-25-226-04: **Siemens Simcenter Femap**

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

Siemens Simcenter Femap | CISA

ICSA-25-226-05: **Siemens Wibu CodeMeter Runtime**

High level vulnerability: Least Privilege Violation.

Siemens Wibu CodeMeter Runtime | CISA

ICSA-25-226-06: **Siemens Opcenter Quality**

High level vulnerabilities: Incorrect Authorization, Missing Encryption of Sensitive Data, Generation of Error Message Containing Sensitive Information, Insufficient Session Expiration, Use of a Broken or Risky Cryptographic Algorithm.

Siemens Opcenter Quality | CISA

ICSA-25-226-07: **Siemens Third-Party Components in SINEC OS**

Critical level vulnerabilities: Improper Input Validation, Use After Free, Out-of-bounds Read, Incorrect Check of Function Return Value, Incorrect Comparison, Improper Control of Resource Identifiers ('Resource Injection'), Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'), NULL Pointer Dereference, Excessive Platform Resource Consumption within a Loop, Allocation of Resources Without Limits or Throttling, Improper Restriction of Operations within the Bounds of a Memory Buffer, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Improper Resource Shutdown or Release, Transmission of Private Resources into a New Sphere ('Resource Leak'), Return of Wrong Status Code, Integer Overflow or Wraparound, Double Free, Buffer Access with Incorrect Length Value, Use of Uninitialized Variable, Missing Release of Memory after Effective Lifetime, Improper Locking, Improper Handling of Values, Use of Uninitialized Resource, Uncontrolled Resource Consumption, Improper Resource Locking, Buffer Underwrite ('Buffer Underflow'), Out-of-bounds Write, Expired Pointer Dereference, Improper Control of a Resource Through its Lifetime, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Incomplete Cleanup, Access of Resource Using Incompatible Type ('Type Confusion'), Divide By Zero, Improper Validation of Array Index, Access of Uninitialized Pointer, Operation on a Resource after Expiration or Release, Sensitive Information in Resource Not Removed Before Reuse, Improper Handling of Exceptional Conditions, Deadlock, Improper Initialization, Detection of Error Condition Without Action, Improper Check for Unusual or Exceptional Conditions, Time-of-check Time-of-use (TOCTOU) Race Condition, Incorrect Calculation of Buffer Size, Improper Cleanup on Thrown Exception, Integer Underflow (Wrap or Wraparound), Missing Initialization of a Variable, Improper Handling of Unexpected Data Type, Always-Incorrect Control Flow Implementation.

Siemens Third-Party Components in SINEC OS | CISA

ICSA-25-226-08: **Siemens RUGGEDCOM CROSSBOW Station Access Controller**

Medium level vulnerabilities: Heap-Based Buffer Overflow, Integer Overflow or Wraparound.

Siemens RUGGEDCOM CROSSBOW Station Access Controller | CISA

ICSA-25-226-09: **Siemens RUGGEDCOM APE1808**

High level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Execution with Unnecessary Privileges.

Siemens RUGGEDCOM APE1808 | CISA

ICSA-25-226-10: **Siemens SIPROTEC 5**

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

Siemens SIPROTEC 5 | CISA

ICSA-25-226-11: **Siemens SIMATIC S7-PLCSIM**

High level vulnerability: Deserialization of Untrusted Data.

Siemens SIMATIC S7-PLCSIM | CISA

ICSA-25-226-12: **Siemens SIPROTEC 4 and SIPROTEC 4 Compact**

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

Siemens SIPROTEC 4 and SIPROTEC 4 Compact | CISA

ICSA-25-226-13: **Siemens SIMATIC RTLS Locating Manager**

Critical level vulnerability: Improper Input Validation.

Siemens SIMATIC RTLS Locating Manager | CISA

ICSA-25-226-14: **Siemens RUGGEDCOM ROX II**

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

Siemens RUGGEDCOM ROX II | CISA

ICSA-25-226-15: **Siemens SINEC OS**

Critical level vulnerabilities: NULL Pointer Dereference, Use After Free, Unchecked Input for Loop Condition, Out-of-bounds Write, Out-of-bounds Read, Uncontrolled Resource Consumption, Missing Encryption of Sensitive Data, Improper Restriction of Operations within the Bounds of a Memory Buffer, Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'), Deadlock, Improper Resource Locking, Improper Input Validation, Stack-based Buffer Overflow, Use of NullPointerException Catch to Detect NULL Pointer Dereference, Improper Control of Resource Identifiers ('Resource Injection'), Incorrect Calculation of Buffer Size, Missing Write Protection for Parametric Data Values, Missing Initialization of a

Variable, Divide By Zero, Transmission of Private Resources into a New Sphere ('Resource Leak'), Incomplete Cleanup, Double Free, Improper Locking.

Siemens SINEC OS | CISA

ICSA-25-226-16: **Siemens SICAM Q100/Q200**

Medium level vulnerability: Cleartext Storage of Sensitive Information.

Siemens SICAM Q100/Q200 | CISA

ICSA-25-226-17: **Siemens SINEC Traffic Analyzer**

High level vulnerabilities: NULL Pointer Dereference, Use After Free, Uncontrolled Resource Consumption, Execution with Unnecessary Privileges, Exposure of Sensitive Information to an Unauthorized Actor, Irrelevant Code, Channel Accessible by Non-Endpoint.

Siemens SINEC Traffic Analyzer | CISA

ICSA-25-226-18: **Siemens SIMOTION SCOUT, SIMOTION SCOUT TIA, and SINAMICS STARTER**

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

Siemens SIMOTION SCOUT, SIMOTION SCOUT TIA, and SINAMICS STARTER | CISA

ICSA-25-226-19: **Siemens SINUMERIK**

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

Siemens SINUMERIK | CISA

ICSA-25-226-20: **Siemens RUGGEDCOM ROX II**

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

Siemens RUGGEDCOM ROX II | CISA

ICSA-25-226-21: **Siemens BFCClient**

High level vulnerabilities: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Out-of-bounds Read, Loop with Unreachable Exit Condition ('Infinite Loop'), Access of Resource Using Incompatible Type ('Type Confusion'), Improper Certificate Validation.

Siemens BFCClient | CISA

ICSA-25-226-22: **Siemens Web Installer**

High level vulnerability: Uncontrolled Search Path Element.

Siemens Web Installer | CISA

ICSA-25-226-23: **Rockwell Automation FactoryTalk Viewpoint**

High level vulnerability: Improper Handling of Insufficient Permissions or Privileges.

Rockwell Automation FactoryTalk Viewpoint | CISA

ICSA-25-226-24: **Rockwell FactoryTalk Linx**

High level vulnerability: Improper Access Control.

Rockwell FactoryTalk Linx | CISA

ICSA-25-226-25: **Rockwell Automation Micro800**

Critical level vulnerabilities: Dependency on Vulnerable Third-Party Component, Improper Input Validation.

Rockwell Automation Micro800 | CISA

ICSA-25-226-26: **Rockwell Automation FLEX 5000 I/O**

High level vulnerability: Improper Input Validation.

Rockwell Automation FLEX 5000 I/O | CISA

ICSA-25-226-27: **Rockwell Automation ArmorBlock 5000 I/O – Webserver**

High level vulnerabilities: Incorrect Authorization, Improper Authentication.

Rockwell Automation ArmorBlock 5000 I/O - Webserver | CISA

ICSA-25-226-28: **Rockwell Automation ControlLogix Ethernet Modules**

Critical level vulnerability: Initialization of a Resource with an Insecure Default.

Rockwell Automation ControlLogix Ethernet Modules | CISA

ICSA-25-226-29: **Rockwell Automation Studio 5000 Logix Designer**

High level vulnerability: Improper Input Validation.

Rockwell Automation Studio 5000 Logix Designer | CISA

ICSA-25-226-30: **Rockwell Automation FactoryTalk Action Manager**

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

Rockwell Automation FactoryTalk Action Manager | CISA

ICSA-25-226-31: **Rockwell Automation 1756-ENT2R, 1756-EN4TR, 1756-EN4T**

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

Rockwell Automation 1756-ENT2R, 1756-EN4TR, 1756-EN4TRXT | CISA

ICSA-25-212-01: **Güralp Systems FMUS Series and MIN Series Devices (Update A)**

Critical level vulnerability: Missing Authentication for Critical Function.

Güralp Systems FMUS Series and MIN Series Devices (Update A) | CISA

SSA-028723: **Multiple OpenSSL Vulnerabilities in BFCClient Before V2.17 (Update 1.1.)** **High** level vulnerabilities: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Out-of-bounds Read, Loop with Unreachable Exit Condition ('Infinite Loop'), Access of Resource Using Incompatible Type ('Type Confusion'), Improper Certificate Validation.

SSA-028723

SSA-914892: **Race Condition Vulnerability in Basic Authentication Implementation of Mendix Runtime (Update 1.1.)**

Medium level vulnerability: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition').

SSA-914892

SSA-908185: **Mirror Port Isolation Vulnerability in RUGGEDCOM ROS Devices (Update 1.2.)**

Critical level vulnerability: Incorrect Provision of Specified Functionality.

SSA-908185

SSA-864900: **Multiple Vulnerabilities in Fortigate NGFW on RUGGEDCOM APE1808 Devices (Update 1.2.)**

Medium level vulnerabilities: Insufficiently Protected Credentials, Insufficient Session Expiration, Out-of-bounds Write, Improperly Implemented Security Check for Standard, Authentication Bypass Using an Alternate Path or Channel, Improper Certificate Validation, Exposure of Sensitive Information to an Unauthorized Actor.

SSA-864900

SSA-856721: **Vulnerability in RUGGEDCOM Discovery Protocol (RCDP) of Industrial Communication Devices (Update 1.3.)**

High level vulnerability: Initialization of a Resource with an Insecure Default.

SSA-856721

SSA-840800: **Code Injection Vulnerability in RUGGEDCOM ROS (Update 1.5.)**

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

SSA-840800

SSA-800126: **Deserialization Vulnerability in Siemens Engineering Platforms before V20 (Update 1.1.)**

High level vulnerability: Deserialization of Untrusted Data.

SSA-800126

SSA-794185: **RADIUS Protocol Susceptible to Forgery Attacks (CVE-2024-3596) - Impact to SIPROTEC, SICAM and Related Products (Update 1.1.)**

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

SSA-794185

SSA-787941: **Denial of Service Vulnerability in RUGGEDCOM ROS devices (Update 1.5.)** **Medium** level vulnerability: Uncontrolled Resource Consumption.

SSA-787941

SSA-770902: **Denial of Service Vulnerability in the Web Server of RUGGEDCOM ROS Devices (Update 1.2.)**

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

SSA-770902

SSA-770770: **Multiple Vulnerabilities in Fortigate NGFW Before V7.4.7 on RUGGEDCOM APE1808 Devices (Update 1.6.)**

Critical level vulnerabilities: Multiple.

SSA-770770

SSA-767615: **Information Disclosure Vulnerability in SIPROTEC 5 Devices (Update 1.4.)** **High** level vulnerability: Use of Default Credentials.

SSA-767615

SSA-764417: **Weak Encryption Vulnerability in RUGGEDCOM ROS Devices (Update 1.9.)**

Medium level vulnerability: Inadequate Encryption Strength.

SSA-764417

SSA-687955: **Accessible Development Shell via Physical Interface in SIPROTEC 5 (Update 1.1.)**

High level vulnerability: Active Debug Code.

SSA-687955

SSA-460466: **Denial of Service Vulnerability in TIA Project-Server and TIA Portal (Update 1.1.)**

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

SSA-460466

SSA-446307: **Authentication Bypass Vulnerability in BMC (CVE-2024-54085) affects SIMATIC IPC RS-828A (Update 1.1.)**

Critical level vulnerability: Authentication Bypass by Spoofing.

SSA-446307

SSA-398330: **Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP >= V3.1.0 and < V3.1.5 (Update 2.7.)** **Critical** level vulnerabilities: Multiple.

SSA-398330

SSA-392859: **Local Arbitrary Code Execution Vulnerability in Siemens Engineering Platforms before V20 (Update 1.1.)**

High level vulnerability: Improper Input Validation.

SSA-392859

SSA-353002: **Multiple Vulnerabilities in SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family (Update 1.2.)**

Medium level vulnerabilities: Use of Hard-coded Cryptographic Key, Uncontrolled Resource Consumption.

SSA-353002

SSA-265688: **Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 TM MFP V1.1** **(Update 1.8.)**

Medium level vulnerabilities: Multiple.

SSA-265688

SSA-256353: **Third-Party Component Vulnerabilities in RUGGEDCOM ROS** **(Update 1.6.)**

Critical level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Observable Timing Discrepancy, Improperly Implemented Security Check for Standard, Heap-based Buffer Overflow, Integer Overflow or Wraparound, Improper Check for Unusual or Exceptional Conditions.

SSA-256353

SSA-170375: **Multiple Vulnerabilities in RUGGEDCOM ROS Before V5.9** **(Update 1.1.)** **High** level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Incorrect Privilege Assignment, Exposure of Sensitive System Information to an Unauthorized Control Sphere.

SSA-170375

SSA-097435: **Usernames Disclosure Vulnerability in Mendix Runtime** **(Update 1.9.)**

Medium level vulnerability: Observable Response Discrepancy.

SSA-097435

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 1.1.)**

High level vulnerabilities: Multiple.

SSA-082556

ICSA-25-224-01: **Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, Cobalt Share**

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

Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, Cobalt Share | CISA

ICSA-25-224-02: **Johnson Controls iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE, iSTAR Edge G2**

High level vulnerabilities: OS Command Injection, Insufficient Verification of Data Authenticity, Use of Default Credentials, Missing Protection Mechanism for Alternate Hardware Interface, Insecure Storage of Sensitive Information.

Johnson Controls iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE, iSTAR Edge G2 | CISA

ICSA-25-224-03: **Schneider Electric EcoStruxure Power Monitoring Expert**

High level vulnerabilities: Path Traversal, Deserialization of Untrusted Data, Server-Side Request Forgery.

Schneider Electric EcoStruxure Power Monitoring Expert | CISA

ICSA-25-224-04: **AVEVA PI Integrator**

High level vulnerabilities: Unrestricted Upload of File with Dangerous Type, Insertion of Sensitive Information into Sent Data.

AVEVA PI Integrator | CISA

ICSA-24-263-04: **MegaSys Computer Technologies Telenium Online Web Application (Update A)**

Critical level vulnerability: Improper Input Validation.

MegaSys Computer Technologies Telenium Online Web Application (Update A) | CISA

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

High level vulnerability: Weak Authentication.

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

ICSMA-25-224-01: **Santesoft Sante PACS Server**

Critical level vulnerabilities: Path Traversal, Double Free, Cleartext Transmission of Sensitive Information, Cross-site Scripting.

Santesoft Sante PACS Server | CISA

ICSA-25-219-01: **Delta Electronics DIAView**

Critical level vulnerability: Improper Limitation of a Pathname to a Restricted Directory.

Delta Electronics DIAView | CISA

ICSA-25-219-02: **Johnson Controls FX80 and FX90**

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

Johnson Controls FX80 and FX90 | CISA

ICSA-25-219-03: **Burk Technology ARC Solo**

Critical level vulnerability: Missing Authentication for Critical Function.

Burk Technology ARC Solo | CISA

ICSA-25-219-04: **Rockwell Automation Arena**

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

Rockwell Automation Arena | CISA

ICSA-25-219-05: **Packet Power EMX and EG**

Critical level vulnerability: Missing Authentication for Critical Function.

Packet Power EMX and EG | CISA

ICSA-25-219-06: **Dreame Technology iOS and Android Mobile Applications**

High level vulnerability: Improper Certificate Validation.

Dreame Technology iOS and Android Mobile Applications | CISA

ICSA-25-219-07: **EG4 Electronics EG4 Inverters**

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 | CISA

ICSA-25-219-08: **Yealink IP Phones and RPS (Redirect and Provisioning Service)**

Medium level vulnerabilities: Improper Restriction of Excessive Authentication Attempts, Allocation of Resources Without Limits or Throttling, Incorrect Authorization, Improper Certificate Validation.

Yealink IP Phones and RPS (Redirect and Provisioning Service) | CISA

ICSA-25-148-04: **Instantel Micromate (Update A)**

Critical level vulnerability: Missing Authentication for Critical Function.

Instantel Micromate (Update A) | CISA

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

Medium level vulnerability: Execution with Unnecessary Privileges.

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

ICSA-25-217-01: **Mitsubishi Electric Iconics Digital Solutions Multiple Products**

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

Mitsubishi Electric Iconics Digital Solutions Multiple Products | CISA

ICSA-25-217-02: **Tigo Energy Cloud Connect Advanced**

Critical level vulnerabilities: Use of Hard-coded Credentials, Command Injection, Predictable Seed in Pseudo-Random Number Generator (PRNG).

Tigo Energy Cloud Connect Advanced | 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 August:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2020-25078 D-Link DCS-2530L and DCS-2670L Devices Unspecified Vulnerability;
CVE-2020-25079 D-Link DCS-2530L and DCS-2670L Command Injection Vulnerability;
CVE-2022-40799 D-Link DNR-322L Download of Code Without Integrity Check Vulnerability;
CVE-2013-3893 Microsoft Internet Explorer Resource Management Errors Vulnerability;
CVE-2007-0671 Microsoft Office Excel Remote Code Execution Vulnerability;
CVE-2025-8088 RARLAB WinRAR Path Traversal Vulnerability;
CVE-2025-54948 Trend Micro Apex One OS Command Injection Vulnerability;
CVE-2025-43300 Apple iOS, iPadOS, and macOS Out-of-Bounds Write Vulnerability;
CVE-2024-8069 Citrix Session Recording Deserialization of Untrusted Data Vulnerability;
CVE-2024-8068 Citrix Session Recording Improper Privilege Management Vulnerability;
CVE-2025-48384 Git Link Following Vulnerability;
CVE-2025-7775 Citrix NetScaler Memory Overflow Vulnerability;
Links and more information:
CISA Adds Three 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 Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA Releases Malware Analysis Report Associated with Microsoft SharePoint Vulnerabilities
CISA published a Malware Analysis Report (MAR) with analysis and associated detection signatures on files related to Microsoft SharePoint vulnerabilities:

- *CVE-2025-49704 [CWE-94: Code Injection],*
- *CVE-2025-49706 [CWE-287: Improper Authentication],*
- *CVE-2025-53770 [CWE-502: Deserialization of Untrusted Data], and*
- *CVE-2025-53771 [CWE-287: Improper Authentication]*

Links and more information:
CISA Releases Malware Analysis Report Associated with Microsoft SharePoint Vulnerabilities | CISA

Microsoft Releases Guidance on High-Severity Vulnerability (CVE-2025-53786) in Hybrid Exchange Deployments
CISA is aware of the newly disclosed high-severity vulnerability, CVE-2025-53786, that allows a cyber threat actor with administrative access to an on-premise Microsoft Exchange server to escalate privileges by exploiting vulnerable hybrid-joined

configurations. This vulnerability, if not addressed, could impact the identity integrity of an organization's Exchange Online service.

Links and more information:

Microsoft Releases Guidance on High-Severity Vulnerability (CVE-2025-53786) in Hybrid Exchange Deployments | CISA

CISA Issues ED 25-02: Mitigate Microsoft Exchange Vulnerability

CISA issued Emergency Directive (ED) 25-02: Mitigate Microsoft Exchange Vulnerability in response to CVE-2025-53786, a vulnerability in Microsoft Exchange server hybrid deployments.

Links and more information:

CISA Issues ED 25-02: Mitigate Microsoft Exchange Vulnerability | CISA

CISA Requests Public Comment for Updated Guidance on Software Bill of Materials

CISA released updated guidance for the Minimum Elements for a Software Bill of Materials (SBOM) for public comment—comment period begins today and concludes on October 3, 2025. These updates build on the 2021 version of the National Telecommunications and Information Administration SBOM Minimum Elements to reflect advancements in tooling and implementation.

Links and more information:

CISA Requests Public Comment for Updated Guidance on Software Bill of Materials | CISA

CISA and Partners Release Joint Advisory on Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage Systems

CISA, along with the National Security Agency, Federal Bureau of Investigation, and international partners, released a joint Cybersecurity Advisory on People's Republic of China (PRC) state-sponsored Advanced Persistent Threat (APT) actors targeting critical infrastructure across sectors and continents to maintain persistent, long-term access to networks.

Links and more information:

CISA and Partners Release Joint Advisory on Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage Systems | CISA

ICS trainings, education

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