2022 June, 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, 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

9 Best Cybersecurity Practices for the IT/OT Environment

IIoT-world.com published an article in 2017, but the actuality of the best practices still exists.

As digital transformation continues to take shape with the convergence of IT and OT, there are some fundamental security best practices that we recommend for organizations across all industries. The specific network architecture might vary across the different verticals, but the general approach is the same.

1. The vision, strategy and execution of the business plan need to include security for IoT devices, reliability and safety. These should be part of the business planning process at all levels of the organization (regardless if you are an IoT solution provider or a customer).
2. Security should be "owned" by one person at the executive level who is responsible for both IT and operations. Security policy, governance and end-user education need to extend across the IT and OT environments as systems are interconnected.
3. Technologies and threats across the IT and OT environments should be clearly understood. Technologies that work in the IT environment may not necessarily work in the OT environment. Additionally, threats may be different in the IT and OT environments.
4. A threat intelligence framework needs to be set up so that the organization can be up to date on the latest information on threats and be prepared to deal with them.
5. Baseline security controls should be deployed across all layers of the organization's environments.
6. Regular risk assessments across all environments must be performed to identify vulnerabilities and ensure that the appropriate security controls are in place.
7. The organization and customers should consider NIST 800-5310 for IT and NIST 800-8211 and ISA/IEC 6244312 for ICS and OT.
8. Establish or update the security patch process to better address vulnerabilities. Follow the recommendations laid out in IEC 62443-2-3, which describes requirements for patch management for control systems.
9. Develop ICS-specific policies and procedures that are consistent with IT security, physical safety and business continuity.

ics.blackcell.hu

Source and more information available on the following link:

https://www.iiot-world.com/ics-security/cybersecurity/9-best-cybersecurity-practices-itot-environment/

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in July 2022:

Periodic online courses:

The Coursera (https://www.coursera.org/) website provides an opportunity to take advantage of online trainings regarding ICS security. The trainings provide video instructions, and the candidates could demonstrate their knowledge in the field of ICS and IoT and the related cloud security. After the course, the University of Colorado, Boulder issues a certificate to the graduates. The following courses are available:

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

More details can be found on the following website:

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

ICS CERT offers the following courses:

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems (201), (202)
- ICS Cybersecurity
- ICS Evaluation

More details can be found on the following website:

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

ICS-CERT Virtual Learning Portal (VLP) provides the following short courses:

- Operational Security (OPSEC) for Control Systems (100W) - 1 hour
- Differences in Deployments of ICS (210W-1) – 1.5 hours
- Influence of Common IT Components on ICS (210W-2) – 1.5 hours
- Common ICS Components (210W-3) – 1.5 hours
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
- Cybersecurity Risk (210W-5) – 1.5 hours
- Current Trends (Threat) (210W-6) – 1.5 hours
- Current Trends (Vulnerabilities) (210W-7) – 1.5 hours
- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
- Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11) – 1.5 hours
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115) - 1 hour

VLP courses are available on the same website, like the other ICS-CERT courses.

SANS online courses in the field of ICS security:

- ICS410: ICS/SCADA Security Essentials
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - anytime, on demand.

More details can be found on the following website:

https://www.sans.org/find-training/search?types=10&coursecode=ICS410,ICS515

Udemy provides online courses in ICS and SCADA security. From the basics of ICS and SCADA security principles to the technological solutions and governance questions, the below course could help to understand the essence of the ICS/SCADA security.

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

More details can be found on the following website:

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

The Department of Homeland Security's two days training is useful for the ICS/SCADA operators:

- SCADA security training

The courses are available live online.

More details can be found on the following website:

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

The SCADAhacker.com website provides ICS security online courses:

- Fundamentals of Industrial Control System Cyber Security

The training takes 40-120 hours, and 8 modules can help to understand the ICS cybersecurity issues. The training focuses on the „Blue teaming" activities, for ICS and SCADA systems.

If you have a certificate, like CISSP or CEH, the course can help to add some ICS and SCADA specific knowledge.

Ethical Hacking for Industrial Control Systems

This exciting new and very advanced course supplies an environment to learn and apply offensive cyber operational (OCO) skills to a range of operational technology architectures. It introduces tactics, techniques, and procedures (TTP) to a range of real-world architectures, components, devices, and protocols that leverage both traditional software vulnerabilities and other more subtle, hard-to-find yet equally or more powerful human vulnerabilities that arise from typical system configuration and usage.

More details can be found on the following website:

https://scadahacker.com/training.html

INFOSEC-Flex SCADA/ICS Security Training Boot Camp gives the possibility for ICS/SCADA operators to get ready for external and internal threats.

The 4 days course guarantees the "Certified SCADA Security Architect" certification for the candidates (93% exam pass rate).

The basics of the ICS/SCADA security, governance, security controls, penetration testing and other topics can help the participants to become an ICS/SCADA security expert.

More details can be found on the following website:

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

Industrial Control System (ICS) & SCADA Cyber Security Training

This is a three day course, what is designed for:

- IT and ICS cybersecurity personnel
- Field support personnel and security operators
- Auditors, vendors and team leaders
- Electric utility engineers
- System personnel & System operators
- Independent system operator personnel
- Electric utility personnel involved with ICS security.
- Technicians, operators, and maintenance personnel
- Investors and contractors in the electric industry
- Managers, accountants, and executives of electric industry

More details can be found on the following website:

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

Bsigroup: Certified Lead SCADA Security Professional training course

This five-day training course will enable you to develop the expertise to plan, design and implement an effective programme to protect SCADA systems. You'll gain an understanding of common Industrial Control Systems (ICS) threats, vulnerabilities, and risks, and how they can be managed.

By attending this course you'll gain the knowledge and skills to advise on or manage risks related to SCADA environments and systems as a qualified professional. On successful completion of the PECB exam that takes place on the final day of this course, you'll gain Certified Lead SCADA Security Professional status.

Duration: 5 days, anytime at your office

More details can be found on the following website:

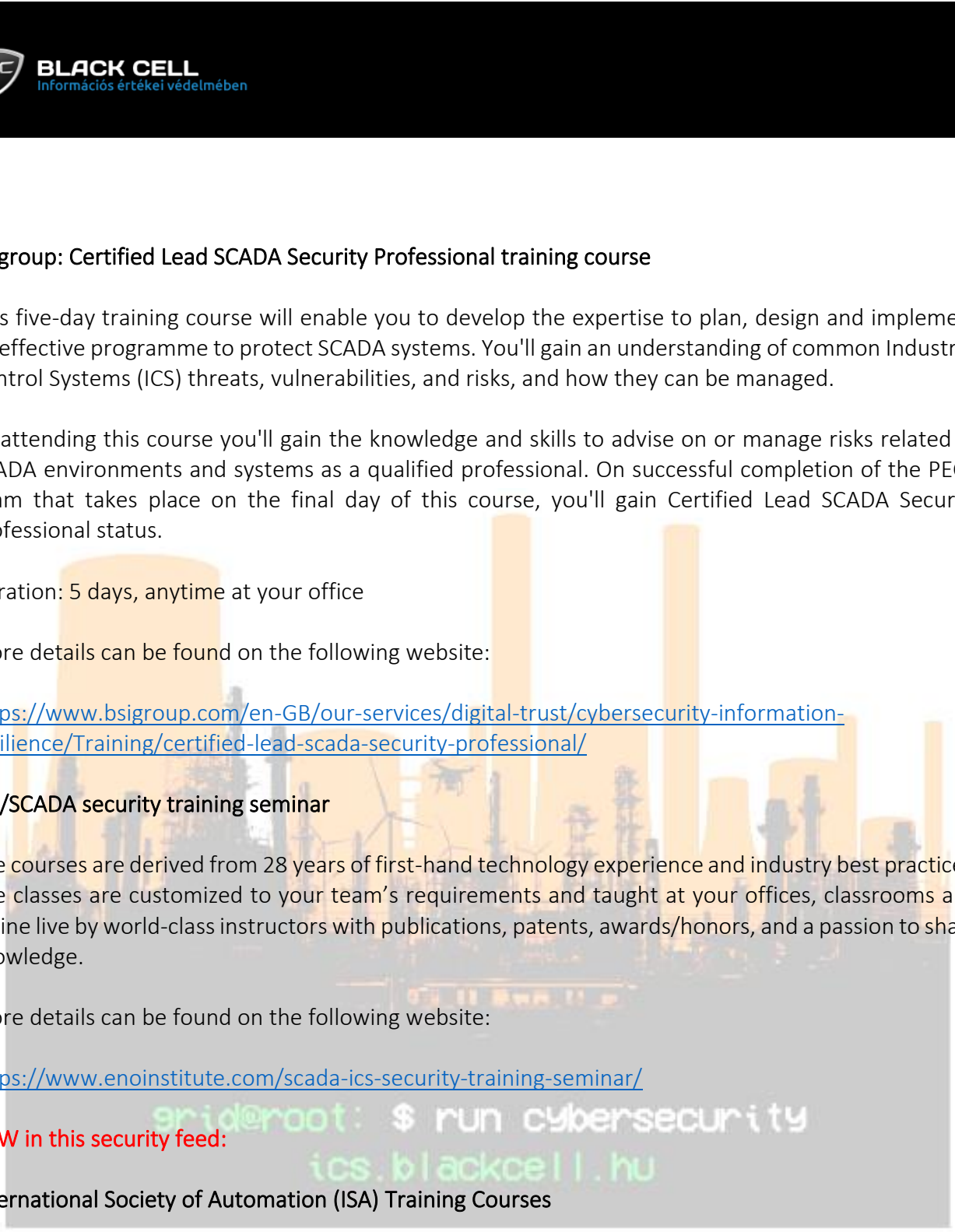
https://www.bsigroup.com/en-GB/our-services/digital-trust/cybersecurity-information-resilience/Training/certified-lead-scada-security-professional/

ICS/SCADA security training seminar

The courses are derived from 28 years of first-hand technology experience and industry best practices. The classes are customized to your team's requirements and taught at your offices, classrooms and online live by world-class instructors with publications, patents, awards/honors, and a passion to share knowledge.

More details can be found on the following website:

https://www.enoinstitute.com/scada-ics-security-training-seminar/



NEW in this security feed:

International Society of Automation (ISA) Training Courses

ISA training equips control system engineers and security professionals with the essential security awareness, work-specific knowledge, and hands-on technical skills they need to respond quickly and successfully to cybersecurity threats and to protect automation and control system technology against cyberattack.

One-Day Classroom Course

- Introduction to Industrial Automation Security and the ISA/IEC 62443 Standards (IC32C)

Multi-Day Classroom Courses

- IT and OT Survival Basics for I & C Personnel (TS06)
- IT and OT Advanced Skills for I& C Personnel (TS12)
- Cybersecurity Awareness Training for Water/Wastewater Industry Professionals (IC31)
- Using the ISA/IEC 62443 Standards to Secure Your Control System (IC32)
- Assessing the Cybersecurity of New or Existing IACS Systems (IC33)
- IACS Cybersecurity Design & Implementation (IC34)
- IACS Cybersecurity Operations & Maintenance (IC37)

Multi-Week, Instructor-Guided Online Courses

- Cybersecurity for Automation, Control, and SCADA Systems (IC32E)

Self-Paced Modular Courses

- Assessing the Cybersecurity of New or Existing IACS Systems (IC33M)
- Cybersecurity Design & Implementation (IC34M)
- IACS Cybersecurity Operations & Maintenance (IC37M)

More details can be found on the following website:

https://www.isa.org/training-and-certification/isa-training/top-tier-training-for-top-notch-protection

ICS conferences

In July 2022, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

16. International Conference on Industrial Control Systems Cyber Security

The International Research Conference is a federated organization dedicated to bringing together a significant number of diverse scholarly events for presentation within the conference program. Events will run over a span of time during the conference depending on the number and length of the presentations. With its high quality, it provides an exceptional value for students, academics and industry researchers.

International Conference on Industrial Control Systems Cyber Security aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Industrial Control Systems Cyber Security. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Industrial Control Systems Cyber Security.

Singapore, Singapore; July 12nd – 13rd, 2022

More details can be found on the following website:

https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ndstrl-cntrl-sstms/sympsm-en.aspx

22th Industrial Conference on Data Mining ICDM 2022

The Industrial Conference on Data Mining ICDM is held on yearly basis.

Researchers from all over the world will present theoretical and application-oriented topics on Data Mining. Practicioners can present and discuss their ongoing projects in Industry Sessions.

Industrial Exhibition · Best-Paper-Award for Talks and Posters · Workshops: Case-Based Reasoning CBR-MD, DM in Marketing DMM, Multimedia Forensic Data Analysis Forensic and Advanced Internet of Things for Medicine and Others IoTMO.

New York, USA; July 13rd – 17th, 2022

More details can be found on the following website:

https://www.data-mining-forum.de/

ICS incidents

Foxconn Factory Hit by Ransomware Suffers from Production Impacts

The Mexican Factory of Foxconn suffered a ransomware attack in late May. 2 years ago, Foxconn operations also hit by ransomware. The LockBit ransomware group attacked the organization.

“The company’s cybersecurity team has been carrying out the recovery plan accordingly. The factory is gradually returning to normal,” the spokesperson said.

The attack affected the production capacity and the overall operation of the company as well, but it had a minimal impact on the latter.

The attacker has not given any hint about the data they hold but they usually look to exfiltrate valuable information that could be used as leverage for the victim to pay.

All affected clients, suppliers, and affected management team members are being kept up to date with the impacts and fallout from the Lockbit attack.

The sources and more information are available on the following links:

https://www.tomshardware.com/news/foxconn-factory-hit-by-ransomware-suffers-from-production-impacts

https://www.bleepingcomputer.com/news/security/foxconn-confirms-ransomware-attack-disrupted-production-in-mexico/

https://therecord.media/foxconn-mexico-factory-operations-gradually-returning-to-normal-after-ransomware-attack/

Source: https://therecord.media/foxconn-mexico-factory-operations-gradually-returning-to-normal-after-ransomware-attack/

Book recommendation

Distributed control methods and cyber security issues in microgrids

Distributed Control and Cyber Security Issues in Microgrids presents a thorough treatment of distributed control methods and cyber security issues for power system researchers and engineers. With the help of mathematical tools, this reference gives a deep understanding of microgrids and new research directions, addressing emerging concepts, methodologies and applications of monitoring, control and protection in smart microgrids with large-scale renewables. With the integration of more distributed or aggregated renewables and the wide utilization of power electronic devices, the smart microgrid is facing new stability and security challenges.

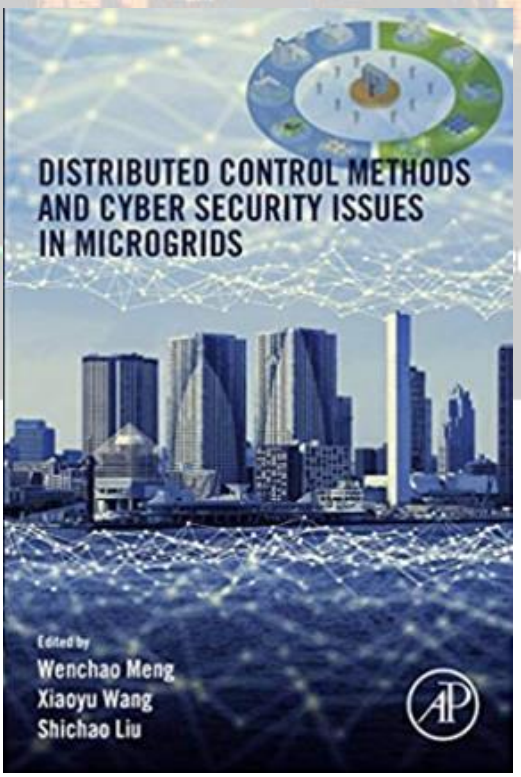
- Includes global case studies to demonstrate distributed control success stories,
- Offers detailed illustrations and flowcharts to address challenges and technical solutions for those working in power systems in utilities and industry,
- Showcases new challenges faced in the stability and security of smart microgrids.

Authors/Editors: Dr. Wenchao Meng; Dr. Xiaoyu Wang; Dr. Shichao Liu

Year of issue: 2020

The book is available at the following link:

https://www.amazon.com/Distributed-Control-Methods-Security-Microgrids-ebook/dp/B086D715DS



ICS security news selection

Critical OAS Bugs Open Industrial Systems to Takeover

The most serious flaw gives attackers a way to remotely execute code on systems that many organizations use to move data in critical ICS environments, security vendor says. A pair of critical flaws in industrial Internet of Things data platform vendor Open Automation Software (OAS) are threatening industrial control systems (ICS), according to Cisco Talos. They're part of a group of eight vulnerabilities in OAS software that the vendor patched this week. Among the flaws is one (CVE-2022-26082) that gives attackers the ability to remotely execute malicious code on a targeted machine to disrupt or alter its functioning; another (CVE-2022-26833) enables unauthenticated use of a REST application programming interface (API) for configuration and viewing data on systems.

Source and more information:
https://www.darkreading.com/application-security/critical-oas-bugs-industrial-takeover

The Vulnerable Maritime Supply Chain - a Threat to the Global Economy

Merchant vessels and ports are extraordinarily vulnerable to increasingly sophisticated cyberattacks against OT systems.

Around 90% to 95% of all shipped goods at some stage travel by sea. This makes the global maritime industry the world's single largest and most important supply chain. Successful cyberattacks against the maritime supply chain would have the potential to damage individual companies, national finances and even the global economy.

Attack vectors …

Source and more information:
https://www.securityweek.com/vulnerable-maritime-supply-chain-threat-global-economy

4 Ways to Close the OT Cybersecurity Talent Gap

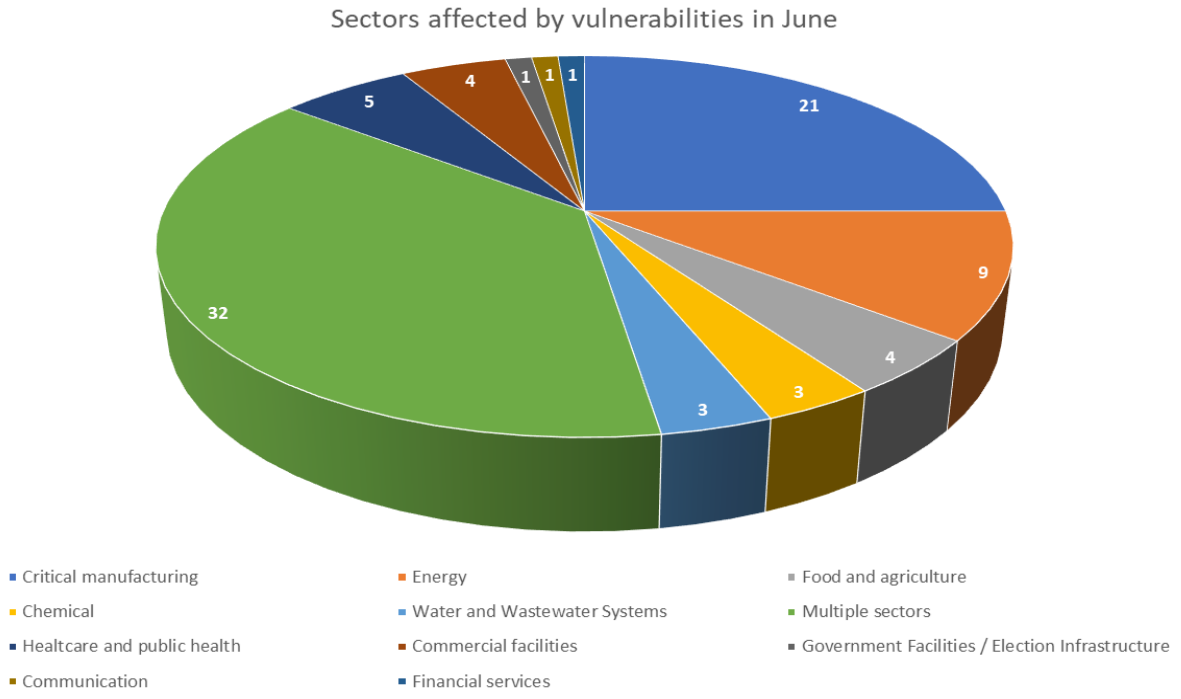
We have a great challenge with the gap in cybersecurity jobs in general, with estimates ranging from 2.72 million to 3.5 million job openings in 2021. However, the gap in very specialized Operational Technology (OT) cybersecurity is even greater since IT has a decades-long head start in building expertise and, therefore, a larger talent pool. According to a global survey of IT and OT security professionals conducted by Pollfish in September 2021, 90% of respondents say they are looking to hire more industrial cybersecurity professionals and roughly the same number (88%) say it has been difficult to find enough candidates with the skills and experience required to properly manage an OT network's cybersecurity.

There are no easy solutions to close the OT cybersecurity talent gap, but the article gives some…

Source and more information:
https://www.securityweek.com/4-ways-close-ot-cybersecurity-talent-gap

ICS vulnerabilities

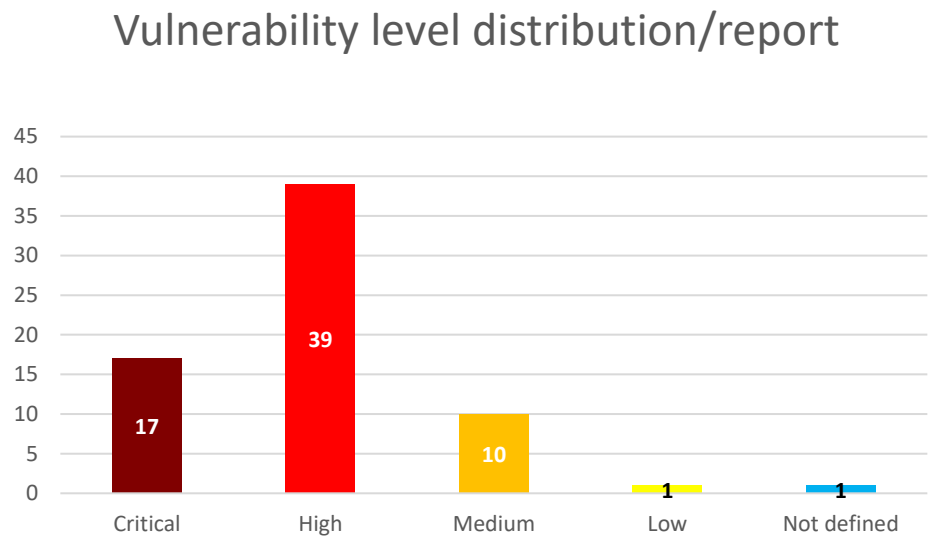
In June 2022, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:



Average number of vulnerabilities per vulnerability report in June: 2,29

The most common vulnerabilities in June:

Vulnerability	CWE number	Piece
Uncontrolled Resource Consumption	CWE-400	8
Path Traversal	CWE-22	7
Missing Authentication for Critical Function	CWE-306	7
Cleartext Transmission of Sensitive Information	CWE-319	6
Improper Access Control	CWE-284	6
Insufficient Verification of Data Authenticity	CWE-345	6
Cross-site Scripting	CWE-79	5
Use of Hard-coded Credentials	CWE-798	4
Improper Input Validation	CWE-20	4
Relative Path Traversal	CWE-23	3



ICSA-22-179-01: **ABB e-Design**

High level vulnerability: Incorrect Default Permissions.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-179-01

ICSA-22-179-02: **Omron SYSMAC CS/CJ/CP Series and NJ/NX Series**

Medium level vulnerabilities: Cleartext Transmission of Sensitive Information, Insufficient Verification of Data Authenticity, Plaintext Storage of a Password.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-179-02

ICSA-22-179-03: **Advantech iView**

Critical level vulnerabilities: SQL Injection, Missing Authentication for Critical Function, Relative Path Traversal, Command Injection.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-179-03

ICSA-22-179-04: **Motorola Solutions MOSCAD IP and ACE IP Gateways**

High level vulnerability: Missing Authentication for Critical Function.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-179-04

ICSA-22-179-05: **Motorola Solutions MDLC**

High level vulnerabilities: Use of a Broken or Risky Cryptographic Algorithm, Plaintext Storage of a Password.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-179-05

ICSA-22-179-06: **Motorola Solutions ACE1000**

Critical level vulnerabilities: Use of Hard-coded Cryptographic Key, Use of Hard-coded Credentials, Insufficient Verification of Data Authenticity.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-179-06

ICSMA-22-174-01: **OFFIS DCMTK**

High level vulnerabilities: Path Traversal, Relative Path Traversal, NULL Pointer Dereference.
https://www.cisa.gov/uscert/ics/advisories/icsma-22-174-01

ICSA-22-174-01: Yokogawa STARDOM

Medium level vulnerabilities: Cleartext Transmission of Sensitive Information, Use of Hard-coded Credentials.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-174-01

ICSA-22-174-02: Yokogawa CAMS for HIS

Medium level vulnerability: Violation of Secure Design Principles.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-174-02

ICSA-22-174-03: Secheron SEPCOS Control and Protection Relay

Critical level vulnerabilities: Improper Enforcement of Behavioral Workflow, Lack of Administrator Control over Security, Improper Privilege Management, Insufficiently Protected Credentials, Improper Access Control.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-174-03

ICSA-22-174-04: Pyramid Solutions EtherNet/IP Adapter Development Kit

Critical level vulnerability: Out-of-bounds Write.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-174-04

ICSA-22-174-05: Elcomplus SmartICS

High level vulnerabilities: Improper Access Control, Relative Path Traversal, Cross-site Scripting.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-174-05

ICSA-22-172-01: Mitsubishi Electric MELSEC Q and L Series

High level vulnerability: Improper Resource Locking.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-172-01

ICSA-22-172-02: JTEKT TOYOPUC

High level vulnerabilities: Missing Authentication for Critical Function, Insufficient Verification of Data Authenticity.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-172-02

ICSA-22-172-03: Phoenix Contact Classic Line Controllers

Critical level vulnerability: Insufficient Verification of Data Authenticity.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-172-03

ICSA-22-172-04: Phoenix Contact ProConOS and MULTIPROG

Critical level vulnerability: Insufficient Verification of Data Authenticity.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-172-04

ICSA-22-172-05: Phoenix Contact Classic Line Industrial Controllers

Critical level vulnerability: Missing Authentication for Critical Function.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-172-05

ICSA-22-172-06: Siemens WinCC OA

Critical level vulnerability: Use of Client-side Authentication.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-172-06

ICSMA-22-167-01: Hillrom Medical Device Management

High level vulnerabilities: Use of Hard-coded Password, Improper Access Control.

https://www.cisa.gov/uscert/ics/advisories/icsma-22-167-01

ICSA-22-167-01: AutomationDirect C-More EA9 HMI

High level vulnerabilities: Uncontrolled Search Path Element, Cleartext Transmission of Sensitive Information.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-01

ICSA-22-167-02: AutomationDirect DirectLOGIC with Serial Communication

High level vulnerability: Cleartext Transmission of Sensitive Information.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-02

ICSA-22-167-03: AutomationDirect DirectLOGIC with Ethernet

High level vulnerabilities: Uncontrolled Resource Consumption, Cleartext Transmission of Sensitive Information.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-03

ICSA-22-167-04: Siemens Mendix SAML Module

High level vulnerabilities: Improper Restriction of XML External Entity Reference, Cross-site Scripting.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-04

ICSA-22-167-05: Siemens EN100 Ethernet Module

High level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-05

ICSA-22-167-06: Siemens Apache HTTP Server

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

https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-06

ICSA-22-167-07: Siemens SINEMA Remote Connect Server

Low level vulnerability: Improperly Implemented Security Check for Standard.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-07

ICSA-22-167-08: Siemens SICAM GridEdge

Critical level vulnerabilities: Missing Authentication for Critical Function, Resource Leak.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-08

ICSA-22-167-09: Siemens SCALANCE LPE9403 Third-Party Vulnerabilities

Critical level vulnerabilities: Path Traversal, Improper Initialization, Allocation of Resources Without Limits or Throttling, Race Condition, Improper Preservation of Permissions, Incorrect Permission Assignment for Critical Resource, Exposure of Sensitive Information to an Unauthorized Actor, Path traversal.
https://cwe.mitre.org/data/definitions/281.html

ICSA-22-167-10: Siemens SCALANCE XM-400 and XR-500

Medium level vulnerability: Improper Validation of Integrity Check Value.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-10

ICSA-22-167-11: Siemens Xpedition Designer

High level vulnerability: Incorrect Permission Assignment for Critical Resource.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-11

ICSA-22-167-12: Siemens Spectrum Power Systems

High level vulnerability: Use of Hard-coded Credentials.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-12

ICSA-22-167-13: Siemens Teamcenter

Critical level vulnerability: Use of Hard-coded Credentials.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-13

ICSA-22-167-14: Siemens OpenSSL Affected Industrial Products

High level vulnerability: Infinite Loop.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-14

ICSA-22-167-15: Siemens Teamcenter Active Workspace

Medium level vulnerability: Cross-site Scripting.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-15

ICSA-22-167-16: Siemens SCALANCE LPE 4903 and SINUMERIK Edge

High level vulnerability: Out-of-bounds Write.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-16

ICSA-22-167-17: Siemens SINEMA Remote Connect Server

Critical level vulnerabilities: Use of Incorrectly-Resolved Name or Reference, Use of Uninitialized Resource, Uncontrolled Resource Consumption, Integer Overflow or Wraparound, Improper Encoding or Escaping of Output, Exposure of Resource to Wrong Sphere, Cryptographic Issues, Cross-site Scripting, Missing Authentication for Critical Function, Insufficient Verification of Data Authenticity, Improper Input Validation, Insertion of Sensitive Information into Log File, Improper Access Control, Obsolete Feature in UI, Internal Asset Exposed to Unsafe Debug Access Level or State, Incorrect User Management, Omission of Security-relevant Information, Command Injection.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-17

ICSA-22-132-06: Siemens SIMATIC WinCC (Update A)

High level vulnerability: Insecure Default Initialization of Resource.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-06

ICSA-22-132-10: Siemens Desigo PXC and DXR Devices (Update A)

Critical level vulnerabilities: Special Element Injection, Uncontrolled Resource Consumption, Use of Password Hash with Insufficient Computational Effort, Insufficient Session Expiration, Observable Discrepancy, Improper Restriction of Excessive Authentication Attempts, Sensitive Cookie in HTTPS Session Without 'Secure' Attribute, Uncaught Exception.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-10

ICSA-22-132-13: Siemens Industrial Devices using libcurl (Update A)

High level vulnerability: Use After Free.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-13

ICSA-22-132-16: Siemens Teamcenter (Update A)

High level vulnerabilities: Stack-based Buffer Overflow, Improper Restriction of XML External Entity Reference.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-16

ICSA-22-104-06: Siemens PROFINET Stack Integrated on Interniche Stack (Update A)

Medium level vulnerability: Uncontrolled Resource Consumption.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-06

ICSA-22-104-07: Siemens Mendix (Update A)

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

https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-07

ICSA-22-069-01: Siemens RUGGEDCOM Devices (Update B)

Medium level vulnerability: Inadequate Encryption Strength.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-01

ICSA-22-041-07: Siemens Solid Edge, JT2Go, and Teamcenter Visualization (Update C)

High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Out-of-bounds Write, Heap-based Buffer Overflow, Out-of-bounds Read.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-07

ICSA-21-257-06: Siemens SIMATIC CP (Update A)

Medium level vulnerability: Cleartext Storage of Sensitive Information.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-257-06

ICSA-21-222-07: Siemens SIMATIC CP (Update A)

High level vulnerabilities: Out-of-Bounds Read, Use After Free.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-222-07

ICSA-21-194-07: Siemens Industrial Products LLDP (Update B)
Critical level vulnerabilities: Classic Buffer Overflow, Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-194-07

ICSA-21-131-03: Siemens Linux-based Products (Update H)
High level vulnerability: Use of Insufficiently Random Values.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-131-03

ICSA-20-105-08: Siemens KTK, SIDOOR, SIMATIC, and SINAMICS (Update C)
High level vulnerability: Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-105-08

ICSA-20-042-04: Siemens PROFINET-IO Stack (Update H)
High level vulnerability: Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-042-04

ICSA-20-014-03: Siemens SCALANCE X Switches (Update B)
High level vulnerability: Missing Authentication for Critical Function.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-014-03

ICSA-20-014-05: Siemens TIA Portal (Update E)
High level vulnerability: Path Traversal.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-014-05

ICSA-17-285-05: Siemens BACnet Field Panels (Update A)
High level vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Path Traversal.
https://www.cisa.gov/uscert/ics/advisories/ICSA-17-285-05

ICSA-22-165-01: Johnson Controls Metasys ADS ADX OAS Servers
High level vulnerabilities: Unverified Password Change, Cross-site Scripting.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-165-01

ICSA-22-165-02: Meridian Cooperative Meridian
High level vulnerability: Improper Access Control.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-165-02

ICSA-22-165-03: Mitsubishi Electric MELSEC-Q/L and MELSEC iQ-R
High level vulnerability: Improper Input Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-165-03

ICSA-22-160-01: Mitsubishi Electric Air Conditioning Systems
High level vulnerabilities: Use of a Broken or Risky Cryptographic Algorithm, Exposure of Sensitive Information to an Unauthorized Actor, Channel Accessible by Non-Endpoint.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-160-01

ICSA-21-334-02: Mitsubishi Electric MELSEC and MELIPC Series (Update C)

High level vulnerabilities: Uncontrolled Resource Consumption, Improper Handling of Length Parameter Inconsistency, Improper Input Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-334-02

ICSA-22-154-01: Vulnerabilities Affecting Dominion Voting Systems ImageCast X

Not defined: Improper Verification of Cryptographic Signature, Mutable Attestation or Measurement Reporting Data, Hidden Functionality, Improper Protection of Alternate Path, Path Traversal: '../filedir', Execution with unnecessary privileges, Authentication Bypass by Spoofing, Incorrect Privilege Assignment, Origin Validation Error.
https://cwe.mitre.org/data/definitions/346.html

ICSA-22-153-01: Carrier LenelS2 HID Mercury access panels

Critical level vulnerabilities: Protection Mechanism Failure, Forced Browsing, Classic Buffer Overflow, Path Traversal, OS Command Injection.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-153-01

ICSA-22-153-02: Illumina Local Run Manager

Critical level vulnerabilities: Execution with unnecessary privileges, Path Traversal, Unrestricted Upload of File with Dangerous Type, Improper Access Control, Cleartext Transmission of Sensitive Information.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-153-02

ICSMA-22-151-01: BD Pyxis

High level vulnerability: Not Using Password Aging.
https://www.cisa.gov/uscert/ics/advisories/icsma-22-151-01

ICSMA-22-151-02: BD Synapsys

Medium level vulnerability: Insufficient Session Expiration.
https://www.cisa.gov/uscert/ics/advisories/icsma-22-151-02

ICSA-22-151-01: Fuji Electric Alpha7 PC Loader

High level vulnerability: Stack-based Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-151-01

ICSA-22-139-01: Mitsubishi Electric MELSEC iQ-F Series (Update A)

High level vulnerability: Improper Input Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-139-01

ICSA-22-090-04: Mitsubishi Electric FA Products (Update A)

High level vulnerabilities: Use of Password Hash Instead of Password for Authentication, Use of Weak Hash, Cleartext Storage of Sensitive Information, Authentication Bypass by Capture-replay.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-04

ICSA-20-245-01: Mitsubishi Electric Multiple Products (Update D)

High level vulnerability: Predictable Exact Value from Previous Values.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-245-01

ICSA-20-212-02: Mitsubishi Electric Factory Automation Engineering Software (Update B)
High level vulnerability: Permission Issues.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-212-02

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

https://ics-cert.us-cert.gov/advisories

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

In June 2022, ICS-CERT has not published alerts.