2025 February, 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 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/

ICS good practices, recommendations

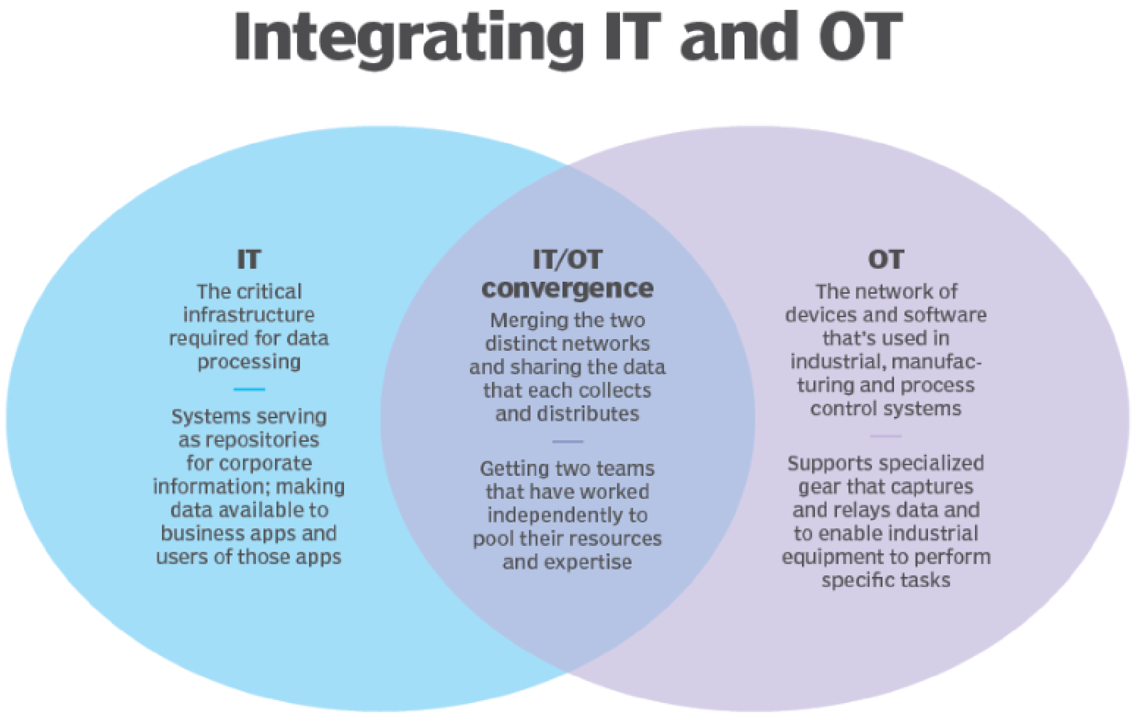
7 key OT security best practices

Operational technology forms the backbone of critical industrial control systems, underpinning everything from energy production and water supply to manufacturing and transportation. Today, these systems increasingly use edge computing to connect to IT networks, turning OT devices into powerful IoT and industrial IoT endpoints.

his connectivity, however, also makes OT vulnerable to cyber attacks that could have devastating -- and possibly even fatal -- consequences.

Organizations that rely on OT should consider adopting the following OT security best practices to manage cyber-risk.

1. Place OT security under the CISO's control
2. Identify and prioritize OT assets
3. Conduct security awareness training
4. Update and patch software regularly
5. Control network access
6. Consider a zero-trust framework
7. Deploy microsegmentation


Integrating IT and OT
IT
The critical infrastructure required for data processing
Systems serving as repositories for corporate information; making data available to business apps and users of those apps
IT/OT convergence
Merging the two distinct networks and sharing the data that each collects and distributes
Getting two teams that have worked independently to pool their resources and expertise
OT
The network of devices and software that's used in industrial, manufacturing and process control systems
Supports specialized gear that captures and relays data and to enable industrial equipment to perform specific tasks

Source and more information available on the following link:

https://www.techtarget.com/searchsecurity/tip/Key-OT-security-best-practices

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in March 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 conferences

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

IoT / OT Security Conference

OT systems are connected to the IT in the company network and supply data from sensors, for example. However, older production machines in particular are often not designed for remote access. This can compromise cybersecurity and favour cyberattacks. Management has a duty to view cybersecurity as a corporate responsibility rather than a necessary evil.

Many organisations in critical infrastructures and industrial companies underestimate the dangers that lurk here. Attacks on these sectors are on the rise. Today, it is important to protect existing infrastructures in the best possible way. For new devices, it will be crucial to consider security right from the design stage. This can also create competitive advantages.

The IoT / OT Security Conference will show you where dangers lurk and what solutions are available.

Cham, Switzerland; 7th March 2025

More details can be found on the following website:

https://www.swissbit.com/en/company/events/iot-ot-security-conference-2025-2/

CS4CA USA Summit

As critical infrastructure continues its transition from analog to digital, the surface for cyber attacks has expanded and the resulting risks to an organization’s physical assets, people, financial liability, and reputation are increasing in frequency and potency. With this in mind, the Cyber Security for Critical Assets Summit brings together senior cybersecurity leaders from across US critical infrastructure, for 2-days of in-depth knowledge exchange, strategy planning and insight building on March 25th – 26th, 2025. This is a unique opportunity to build partnerships with senior cybersecurity executives from the country’s Oil & Gas, Energy, Utilities, Power, Water, Mining, Chemical and Transportation industries while participating in the discussions shaping the American cybersecurity landscape in 2025 and beyond.

Houston, Texas, USA; 25th – 26th March 2025

More details can be found on the following website:

https://usa.cs4ca.com/

ICS incidents

Tata Technologies hit by ransomware attack

Tata Technologies, a subsidiary of Tata Motors specializing in engineering and digital services, confirmed a ransomware attack that disrupted some of its IT systems. The attack, disclosed to the Indian Stock Exchange on January 31, 2025, impacted a limited number of IT assets, leading the company to suspend certain services as a precaution. However, Tata Technologies assured that client delivery services remained unaffected, and all disrupted systems were successfully restored.

The company is conducting a detailed investigation with cybersecurity experts to determine the root cause and implement remedial measures. Tata Technologies reaffirmed its commitment to maintaining high security standards and mitigating potential risks. The identity of the threat actors and specific attack methods have not been disclosed.

Recent reports indicate a significant rise in ransomware attacks targeting Indian organizations. Data from CyberPeace shows a 55% increase in ransomware incidents in 2024, with 98 recorded cases compared to 63 in 2023. India ranked tenth globally and sixth in Asia for ransomware threats, accounting for 5% of incidents in Asia and 3% worldwide.

The industrial sector was the most frequently targeted, accounting for 75% of attacks, while the finance sector represented 10% of cases. A notable incident in December 2024 involved Comtel, a data center operator, whose ransomware attack disrupted brokerage firms and temporarily suspended trading activities.

Tata has previously been targeted by ransomware groups. In October 2022, Tata Power suffered an attack by the Hive ransomware group, leading to the exposure of sensitive corporate and employee information.

The surge in ransomware attacks underscores the growing cybersecurity challenges faced by Indian enterprises as the country’s digital infrastructure expands. Organizations must implement robust security measures to counteract evolving threats.

The source is available on the following link:

https://www.itpro.com/security/ransomware/tata-technologies-hit-by-ransomware-attack

Book recommendation

SCADA and Power Systems

The book "SCADA and Power Systems" very lucidly brings together in one concise volume a user-friendly description to help understand the fundamentals of "Supervisory Control and Data Acquisition" (SCADA) system and its possible application functions in power system automation. The text begins with a brief history and evolution of SCADA systems followed by description of the basic functions of SCADA systems. The basic components of SCADA system from the legacy remote terminal units to the latest master control stations have also been discussed in sufficient details. The book:

- Provides strong project oriented approach to all practical aspects of SCADA systems design, project development and implementation of SCADA and Power System Automation.
- Provides an understanding of the legacy systems as well as an insight into the new technologies.
- Covers the complete chain of SCADA components and related equipment.
- Explores the SCADA communication from conceptualization to realization, including an extensive coverage of communication aspects, data communication, protocols and linking media.
- Covers substation automation in detail which forms the basis for transmission, distribution, and customer automation, distribution automation and distribution management systems, and energy management systems.

"SCADA and Power Systems" is best suited for all categories of readers; whether an Electrical Engineering student, Engineering Faculty, working professional, design engineer, and those who are working or wish to work in the challenging field of SCADA and Power System Automation Projects. Senior undergraduate and post graduate students will find it useful as an academic text book.

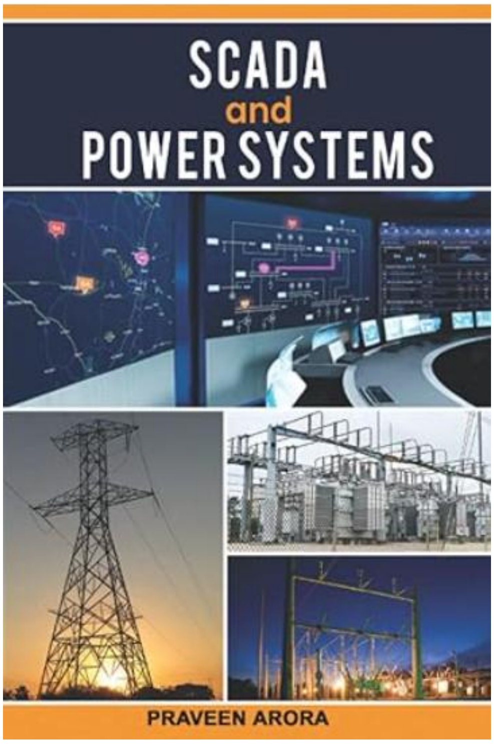
The book will also catch the attention of practitioners, fresh and experienced alike, to acquire basic knowledge of SCADA systems and application functions, which are evolving day by day, to help them adapt to the new challenges effortlessly. Written for practical application, this book is a valuable resource for professionals operating within different SCADA project stages.

Author/Editor: Mr. Praveen Arora (Author)

Year of issue: 2021

The book is available at the following link:

https://www.amazon.com/SCADA-Power-Systems-Praveen-Arora/dp/B09L4X46KY/ref=sr_1_5?dib=eyJ2IjoiMSJ9.kJBfCfR9Adu1nkwS_FXGcMI7anyJ8nTosyjMIG57cUB8GbqNZNecZ0n_TCDe_X3mDGc7OahHobR75gpz6JrQGXxWlEpsNJnJ6ovtQx3CquZGpFHZP_YxxLYrL_PxIP5adMmBSJpMRYSHDIRPmiof2vH3xuJfyjWZUw71VV3AXjN8v9XrDUBTixoKDijpOVeGE6lTDZDUPdbemSfyRExOyEc_Qyivo4m6GGC1-tBKiNTcT43zpkPw8NswP3jp7EOI1N6Fg0Pj3QVlzvkZujYdNlrje4Dn7MnV98J-M_o3kj-3rGibQdsAC1w1Le9ypuGPbaIujEni8LsXfx73Qm1YZJh6u7jzPIPlv3zXcgOkGxQ.btdU4x5u6c6omyNEgwt87ggNC2rH_C_1GWzTlot1JTM&dib_tag=se&keywords=SCADA&qid=1738595595&s=books&sr=1-5



ICS security news selection

WEF sounds alarm on software supply chain vulnerabilities, flags risks in open-source and third-party dependencies

The World Economic Forum (WEF) highlighted the growing challenge of securing software supply chains, emphasizing the rising need to safeguard against hidden dependencies. As businesses increasingly rely on third-party software suppliers and open-source solutions, they face significant hurdles in ensuring the security and integrity of their software ecosystems. Also, these challenges extend beyond IT to operational technology (OT) and industrial systems, heightening risks for critical infrastructure installations. These escalations call attention to underscoring the urgency for robust strategies to mitigate risks and protect against vulnerabilities in an interconnected digital landscape. …

Source and more information:

https://industrialcyber.co/supply-chain-security/wef-sounds-alarm-on-software-supply-chain-vulnerabilities-flags-risks-in-open-source-and-third-party-dependencies/

Critical Infrastructure Under Siege: The Top OT Threats of 2025

As we enter 2025, the operational technology (OT) cybersecurity landscape faces intensifying threats. The past year has revealed how advanced threat actors – nation-states, cybercriminal organizations, and hacktivist groups – have honed their focus on critical infrastructure, employing increasingly sophisticated tactics to exploit vulnerabilities and disrupt essential systems. …

Source and more information:

https://rmcglobal.com/critical-infrastructure-under-siege-the-top-ot-threats-of-2025/

S4x25 and BSidesICS: Where industrial cybersecurity experts converge to foster collaboration and innovation

As the industrial cybersecurity community converges in Tampa, Florida for the upcoming S4x25 and BSidesICS events, there is a palpable sense of excitement and anticipation. These gatherings offer industry experts, practitioners, and thought leaders a platform to tackle the distinct challenges faced by the industrial cybersecurity sector and prepare for rising adversarial targeting. …

Source and more information:

https://industrialcyber.co/features/s4x25-and-bsidesics-where-industrial-cybersecurity-experts-converge-to-foster-collaboration-and-innovation/

The High-Stakes Disconnect For ICS/OT Security

In the rapidly evolving domain of cybersecurity, the specific challenges and needs for Industrial Control Systems (ICS) and Operational Technology (OT) security distinctly stand out from traditional IT security. ICS/OT engineering systems, which power critical infrastructure such as electric power grids, oil and gas processing, heavy manufacturing, food and beverage processes, and water management facilities, require tailored cybersecurity strategies, and controls. This is due to the increasing attacks towards ICS/OT, their unique operational missions, a different risk surface than that of traditional IT networks, and the significant safety consequences from cyber incidents that impact the physical world. …

Source and more information:

https://thehackernews.com/2025/01/the-high-stakes-disconnect-for-icsot.html

Orthanc Server Vulnerability Poses Risk to Medical Data, Healthcare Operations

A critical vulnerability potentially affecting Orthanc servers can pose a serious risk to medical data and healthcare operations, according to a researcher.

The US cybersecurity agency CISA last week published an ICS medical advisory to inform organizations about CVE-2025-0896, a critical authentication issue discovered in Orthanc, an open source and lightweight DICOM server for medical imaging. The product is used worldwide in the healthcare and public health sector. …

Source and more information:

https://www.securityweek.com/orthanc-server-vulnerability-poses-risk-to-medical-data-healthcare-operations/

Industrial Defender 8.0 offers detailed view of OT environments

Industrial Defender announced its latest platform, Industrial Defender 8.0. This release introduces a completely redesigned risk dashboard, helping critical infrastructure and industrial operators manage security and compliance risks by assessing and prioritizing them with enhanced intelligence and risk scoring.

Industrial Defender 8.0 also includes updates to Industrial Defender's robust policy library, for meeting the very latest in standards and frameworks such as NERC CIP, AESCSF, OTCC, TSA Security Directives, and more. …

Source and more information:

https://www.helpnetsecurity.com/2025/02/11/industrial-defender-8-0-offers-detailed-view-of-ot-environments/

S4x25 fireside chat: Dale Peterson and Paul Griswold discuss evolution of ICS security

At the S4x25 event, Dale Peterson sat down with Paul Griswold, former chief product officer at Honeywell, for an engaging fireside chat that delved into the state of industrial control systems (ICS) security. The conversation provided candid insights into the progress made, ongoing challenges, and future directions for vendors, integrators, and asset owners within the ICS landscape. …

Source and more information:

https://industrialcyber.co/events/s4x25-fireside-chat-dale-peterson-and-paul-griswold-discuss-evolution-of-ics-security/

The High-Stakes Disconnect in ICS/OT Security

Over the last decade, incidents hitting industrial control systems (ICS) and operations technology (OT) environments demonstrate the evolution of cyber threats from mere nuisances to potentially catastrophic events. These events, such as TRISIS, CRASHOVERRIDE, Pipedream, and Fuxnet, are often orchestrated by state-sponsored groups targeting critical infrastructure, and now in many cases are also available to other non-state-sponsored threat groups. Human-operated and targeted ICS/OT ransomware incidents have also increased, posing additional concerns. …

Source and more information:

https://www.darkreading.com/ics-ot-security/the-high-stakes-disconnect-in-ics-ot-security

Australian Critical Infrastructure Faces 'Acute' Foreign Threats

Australian intelligence is projecting that foreign nations will increasingly attempt to sabotage its country's critical infrastructure.

On Feb. 19, Mike Burgess, director-general of security in charge of the Australian Security Intelligence Organisation (ASIO), delivered an annual threat assessment encompassing the many national security threats facing Australia. Among the most important, he noted, are the ways in which foreign threat actors are weaponizing artificial intelligence (AI)-enabled disinformation and deepfakes, military espionage, and attacks against critical infrastructure that could cause damage to the military, government, and social cohesion. …

Source and more information:

https://www.darkreading.com/ics-ot-security/australian-critical-infrastructure-acute-foreign-threats

Industrial System Cyberattacks Surge as OT Stays Vulnerable

Ransomware attacks on manufacturing, oil and gas, and other industrial sectors jumped significantly in 2024, as more groups emerged to target operational technology (OT); nearly a quarter of affected firms had to suspend operations.

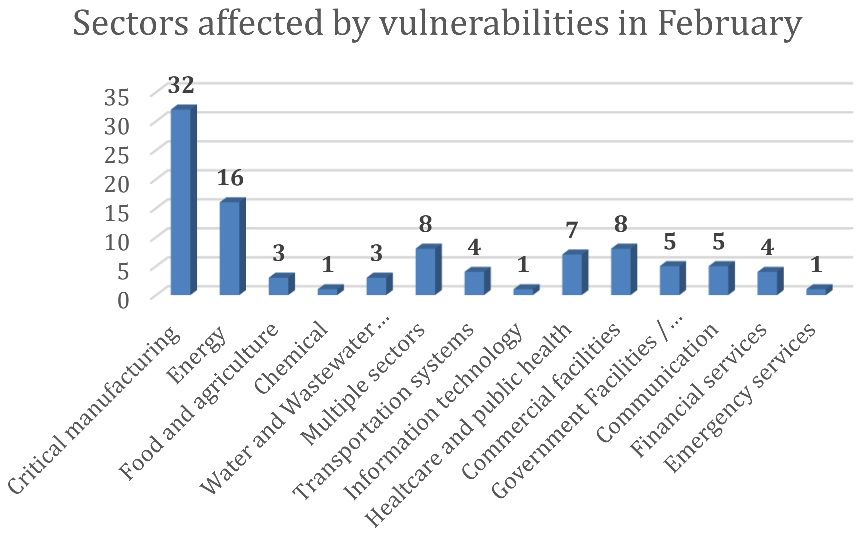
Overall, nearly 1,700 ransomware attacks successfully breached industrial organizations last year, as measured by attackers' posts on dedicated leak sites. That's an increase of 87% over the previous year, according to an OT/ICS report published by Dragos, an infrastructure security firm. The breaches led 25% of affected sites to halt operations, while 75% of attacks caused operational disruption to some degree, the company's report stated. …

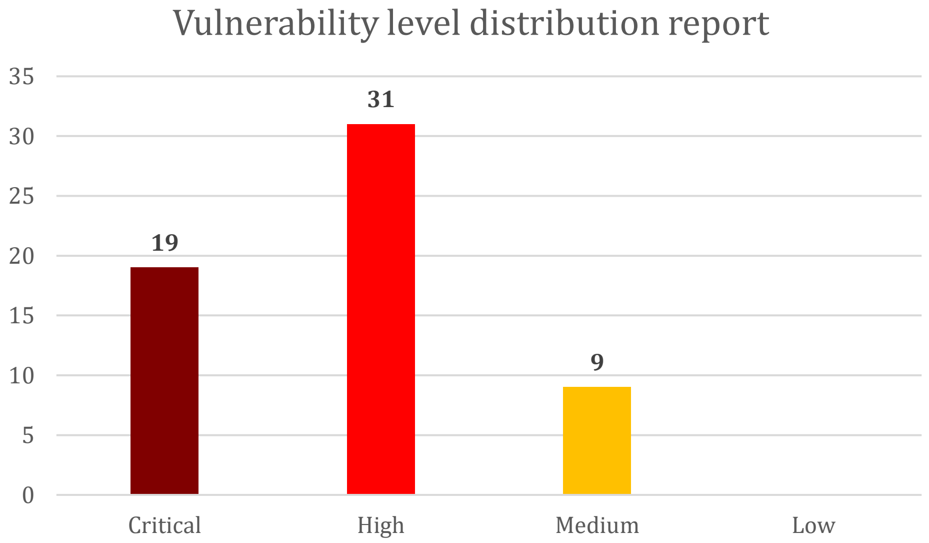
Source and more information:

https://www.darkreading.com/cyber-risk/industrial-system-cyberattacks-surge-ot-vulnerable

ICS vulnerabilities

In February 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-25-058-01: **Schneider Electric Communication Modules for Modicon M580 and Quantum Controllers**

Critical level vulnerability: Out-of-bounds Write.

Schneider Electric Communication Modules for Modicon M580 and Quantum Controllers | CISA

ICSMA-25-058-01: **Dario Health USB-C Blood Glucose Monitoring System Starter Kit Android Application**

High level vulnerabilities: Exposure of Private Personal Information to an Unauthorized Actor, Improper Output Neutralization For Logs, Storage of Sensitive Data In a Mechanism Without Access Control, Cleartext Transmission of Sensitive Information, Cross-site Scripting (XSS), Sensitive Cookie Without 'HttpOnly' Flag, Exposure of Sensitive Information Due To Incompatible Policies.

Dario Health USB-C Blood Glucose Monitoring System Starter Kit Android Application | CISA

ICSA-25-056-01: **Rockwell Automation PowerFlex 755**

High level vulnerability: Cleartext Transmission of Sensitive Information.

Rockwell Automation PowerFlex 755 | CISA

ICSMA-25-030-01: **Contec Health CMS8000 Patient Monitor (Update A)**

Critical level vulnerabilities: Out-of-Bounds Write, Hidden Functionality, Privacy Leakage.

Contec Health CMS8000 Patient Monitor (Update A) | CISA

ICSA-25-051-01: **ABB ASPECT-Enterprise, NEXUS, and MATRIX Series**

Critical level vulnerability: Use of Hard-coded Credentials.

ABB ASPECT-Enterprise, NEXUS, and MATRIX Series | CISA

ICSA-25-051-02: **ABB FLXEON Controllers**

Critical level vulnerabilities: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion'), Missing Origin Validation in WebSockets, Insertion of Sensitive Information into Log File.

ABB FLXEON Controllers | CISA

ICSA-25-051-04: **Siemens SiPass Integrated**

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

Siemens SiPass Integrated | CISA

ICSA-25-051-05: **Rapid Response Monitoring My Security Account App**

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

Rapid Response Monitoring My Security Account App | CISA

ICSA-25-051-06: **Elseta Vinci Protocol Analyzer**

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

Elseta Vinci Protocol Analyzer | CISA

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

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

Mitsubishi Electric CNC Series (Update A) | CISA

ICSMA-25-051-01: **Medixant RadiAnt DICOM Viewer**

Medium level vulnerability: Improper Certificate Validation.

Medixant RadiAnt DICOM Viewer | CISA

ICSA-24-191-01: **Delta Electronics CNCSoft-G2 (Update A)**

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

Delta Electronics CNCSoft-G2 (Update A) | CISA

ICSA-25-035-02: **Rockwell Automation GuardLogix 5380 and 5580 (Update A)**

High level vulnerability: Improper Handling of Exceptional Conditions.

Rockwell Automation GuardLogix 5380 and 5580 (Update A) | CISA

ICSA-25-044-01: **Siemens SIMATIC S7-1200 CPU Family**

High level vulnerabilities: Improper Resource Shutdown or Release, Improper Validation of Syntactic Correctness of Input.

Siemens SIMATIC S7-1200 CPU Family | CISA

ICSA-25-044-02: **Siemens SIMATIC**

Medium level vulnerability: Observable Discrepancy.

Siemens SIMATIC | CISA

ICSA-25-044-03: **Siemens SIPROTEC 5**

Medium level vulnerability: Cleartext Storage of Sensitive Information.

Siemens SIPROTEC 5 | CISA

ICSA-25-044-04: **Siemens SIPROTEC 5**

High level vulnerability: Active Debug Code.

Siemens SIPROTEC 5 | CISA

ICSA-25-044-05: **Siemens SIPROTEC 5 Devices**

High level vulnerability: Use of Default Credentials.

Siemens SIPROTEC 5 Devices | CISA

ICSA-25-044-06: **Siemens RUGGEDCOM APE1808 Devices**

High level vulnerabilities: Out-of-bounds Read, Insertion of Sensitive Information Into Sent Data, Allocation of Resources Without Limits or Throttling, Integer Overflow or Wraparound, Path Traversal, Out-of-bounds Write, HTTP Request/Response Splitting.

Siemens RUGGEDCOM APE1808 Devices | CISA

ICSA-25-044-07: **Siemens Teamcenter**

High level vulnerability: URL Redirection to Untrusted Site ('Open Redirect').

Siemens Teamcenter | CISA

ICSA-25-044-08: **Siemens OpenV2G**

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

Siemens OpenV2G | CISA

ICSA-25-044-09: **Siemens SCALANCE W700**

Critical level vulnerabilities: Double Free, Improper Restriction of Communication Channel to Intended Endpoints, Improper Resource Shutdown or Release, Inadequate Encryption Strength, Race Condition, Integer Overflow or Wraparound, Out-of-bounds Write, NULL Pointer Dereference, Externally Controlled

Reference to a Resource in Another Sphere, Use After Free, Type Confusion, Improper Certificate Validation, Missing Release of Memory after Effective Lifetime, Uncontrolled Resource Consumption, Out-of-bounds Read, Inefficient Regular Expression Complexity, Incorrect Provision of Specified Functionality, Improper Check for Unusual or Exceptional Conditions, Permissive List of Allowed Inputs, Improper Input Validation, Divide By Zero, Forced Browsing, Unchecked Return Value, Truncation of Security-relevant Information, Missing Critical Step in Authentication, OS Command Injection, Excessive Iteration, Exposure of Sensitive Information to an Unauthorized Actor, Observable Discrepancy, Improper Restriction of Operations within the Bounds of a Memory Buffer, Cross-site Scripting, Injection, Improper Access Control.

Siemens SCALANCE W700 | CISA

ICSA-25-044-10: **Siemens Questa and ModelSim**

Medium level vulnerability: Uncontrolled Search Path Element.

Siemens Questa and ModelSim | CISA

ICSA-25-044-11: **Siemens APOGEE PXC and TALON TC Series**

High level vulnerabilities: Inadequate Encryption Strength, Out-of-bounds Read.

Siemens APOGEE PXC and TALON TC Series | CISA

ICSA-25-044-12: **Siemens SIMATIC IPC DiagBase and SIMATIC IPC DiagMonitor**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

Siemens SIMATIC IPC DiagBase and SIMATIC IPC DiagMonitor | CISA

ICSA-25-044-13: **Siemens SIMATIC PCS neo and TIA Administrator**

High level vulnerability: Insufficient Session Expiration.

Siemens SIMATIC PCS neo and TIA Administrator | CISA

ICSA-25-044-14: **Siemens Opcenter Intelligence**

Critical level vulnerabilities: Improper Authentication, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Deserialization of Untrusted Data, Insertion of Sensitive Information into Log File, Server-Side Request Forgery (SSRF).

Siemens Opcenter Intelligence | CISA

ICSA-25-044-15: **ORing IAP-420**

High level vulnerabilities: Cross-site Scripting, Command Injection.

ORing IAP-420 | CISA

ICSA-25-044-16: **mySCADA myPRO Manager**

Critical level vulnerabilities: OS Command Injection, Missing Authentication for Critical Function, Cleartext Storage of Sensitive Information, Cross-Site Request Forgery (CSRF).

mySCADA myPRO Manager | CISA

ICSA-25-044-17: **Outback Power Mojave Inverter**

High level vulnerabilities: Use of GET Request Method With Sensitive Query Strings, Exposure of Sensitive Information to an Unauthorized Actor, Command Injection.

Outback Power Mojave Inverter | CISA

ICSA-25-044-18: **Dingtian DT-R0 Series**

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

Dingtian DT-R0 Series | CISA

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

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

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

ICSMA-25-044-01: **Qardio Heart Health IOS and Android Application and QardioARM A100**

High level vulnerabilities: Exposure of Private Personal Information to an Unauthorized Actor, Uncaught Exception, Files or Directories Accessible to External Parties.

Qardio Heart Health IOS and Android Application and QardioARM A100 | CISA

SSA-832273: **Siemens RUGGEDCOM APE1808 Devices (Update 1.6.)**

Critical level vulnerabilities: Multiple.

SSA-832273

SSA-712929: **Siemens Industrial Products (Update 2.9.)**

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

SSA-712929

SSA-698820: **Siemens RUGGEDCOM APE1808 Devices (Update 1.5.)**

Critical level vulnerabilities: Stack-based Buffer Overflow, Session Fixation, Use of Password Hash With Insufficient Computational Effort, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Stack-based Buffer Overflow, Missing Authentication for Critical Function, Incorrect Parsing of Numbers with Different Radices, Improperly Implemented Security Check for Standard, Improper Access Control, Weak Authentication.

SSA-698820

SSA-697140: **Siemens SCALANCE and RUGGEDCOM Products (Update 1.3.)**

High level vulnerability: Improper Input Validation.

SSA-697140

SSA-398330: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1 (Update 2.3.)** **Critical** level vulnerabilities: Multiple.

SSA-398330

SSA-354569: **Siemens RUGGEDCOM APE1808 Devices (Update 1.1.)**

Critical level vulnerabilities: Missing Authentication for Critical Function, NULL Pointer Dereference, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Check for Unusual or Exceptional Conditions, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').

SSA-354569

SSA-349422: **Siemens Industrial Real-Time (IRT) Devices (Update 2.2.)**

High level vulnerability: Uncontrolled Resource Consumption.

SSA-349422

SSA-196737: **Siemens SINEC Traffic Analyzer Before V1.2 (Update 1.1.)**

High level vulnerabilities: Out-of-bounds Write, Insufficient Session Expiration, Cross-Site Request Forgery (CSRF), Insufficiently Protected Credentials, Exposed Dangerous Method or Function, Cleartext Transmission of Sensitive Information, Sensitive Cookie in HTTPS Session Without 'Secure' Attribute, Improper Input Validation.

SSA-196737

SSA-194557: **Siemens SIPROTEC 5** **(Update 1.1.)**

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

SSA-194557

ICSA-24-319-17: **2N Access Commander** **(Update A)**

High level vulnerabilities: Path Traversal, Insufficient Verification of Data Authenticity, Use of Hard-coded Cryptographic Key.

2N Access Commander (Update A) | CISA

ICSA-25-037-04: **Trimble Cityworks** **(Update A)**

High level vulnerability: Deserialization of Untrusted Data.

Trimble Cityworks (Update A) | CISA

ICSA-25-037-01: **Schneider Electric EcoStruxure Power Monitoring Expert (PME)**

High level vulnerability: Deserialization of Untrusted Data.

Schneider Electric EcoStruxure Power Monitoring Expert (PME) | CISA

ICSA-25-037-02: **Schneider Electric EcoStruxure**

High level vulnerability: Uncontrolled Search Path Element.

Schneider Electric EcoStruxure | CISA

ICSA-25-037-03: **ABB Drive Composer**

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

ABB Drive Composer | CISA

ICSA-25-037-04: **Trimble Cityworks**

High level vulnerability: Deserialization of Untrusted Data.

Trimble Cityworks | CISA

ICSMA-25-037-01: **MicroDicom DICOM Viewer**

Medium level vulnerability: Improper Certificate Validation.

MicroDicom DICOM Viewer | CISA

ICSMA-25-037-02: **Orthanc Server**

Critical level vulnerability: Missing Authentication for Critical Function.

Orthanc Server | CISA

ICSA-25-035-01: **Western Telematic Inc NPS Series, DSM Series, CPM Series**

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

Western Telematic Inc NPS Series, DSM Series, CPM Series | CISA

ICSA-25-035-02: **Rockwell Automation 1756-L8zS3 and 1756-L3zS3**

High level vulnerability: Improper Handling of Exceptional Conditions.

Rockwell Automation 1756-L8zS3 and 1756-L3zS3 | CISA

ICSA-25-035-03: **Elber Communications Equipment**

Critical level vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Hidden Functionality.

Elber Communications Equipment | CISA

ICSA-25-035-04: **Schneider Electric Modicon M580 PLCs, BMENOR2200H and EVLink Pro AC**

High level vulnerability: Incorrect Calculation of Buffer Size.

Schneider Electric Modicon M580 PLCs, BMENOR2200H and EVLink Pro AC | CISA

ICSA-25-035-05: **Schneider Electric Web Designer for Modicon**

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

Schneider Electric Web Designer for Modicon | CISA

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

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

Schneider Electric Modicon M340 and BMXNOE0100/0110, BMXNOR0200H | CISA

ICSA-25-035-07: **Schneider Electric Pro-face GP-Pro EX and Remote HMI**

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

Schneider Electric Pro-face GP-Pro EX and Remote HMI | CISA

ICSA-25-035-08: **AutomationDirect C-more EA9 HMI**

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

AutomationDirect C-more EA9 HMI | CISA

ICSA-23-299-03: **Ashlar-Vellum Cobalt, Graphite, Xenon, Argon, Lithium (Update A)** **High** level vulnerabilities: Out-of-bounds Write, Heap-based Buffer Overflow, Out-of-Bounds Read.

Ashlar-Vellum Cobalt, Graphite, Xenon, Argon, Lithium (Update A) | CISA

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

Cybersecurity Alerts & Advisories | CISA

CERT Services | Services | Siemens Siemens global website

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

ICS alerts

CISA has published alerts in 2025 February:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2024-45195 Apache OFBiz Forced Browsing Vulnerability;
CVE-2024-29059 Microsoft .NET Framework Information Disclosure Vulnerability;
CVE-2018-9276 Paessler PRTG Network Monitor OS Command Injection Vulnerability;
CVE-2018-19410 Paessler PRTG Network Monitor Local File Inclusion Vulnerability;
CVE-2024-53104 Linux Kernel Out-of-Bounds Write Vulnerability;
CVE-2025-0411 7-Zip Mark of the Web Bypass Vulnerability;
CVE-2022-23748 Dante Discovery Process Control Vulnerability;
CVE-2024-21413 Microsoft Outlook Improper Input Validation Vulnerability;
CVE-2020-29574 CyberoamOS (CROS) SQL Injection Vulnerability;
CVE-2020-15069 Sophos XG Firewall Buffer Overflow Vulnerability;
CVE-2025-0994 Trimble Cityworks Deserialization Vulnerability;
CVE-2024-40891 Zyxel DSL CPE OS Command Injection Vulnerability;
CVE-2024-40890 Zyxel DSL CPE OS Command Injection Vulnerability;
CVE-2025-21418 Microsoft Windows Ancillary Function Driver for WinSock Heap-Based Buffer Overflow Vulnerability;
CVE-2025-21391 Microsoft Windows Storage Link Following Vulnerability;
CVE-2025-24200 Apple iOS and iPadOS Incorrect Authorization Vulnerability;
CVE-2024-41710 Mitel SIP Phones Argument Injection Vulnerability;
CVE-2024-57727 SimpleHelp Path Traversal Vulnerability;
CVE-2025-0108 Palo Alto PAN-OS Authentication Bypass Vulnerability;
CVE-2024-53704 SonicWall SonicOS SSLVPN Improper Authentication Vulnerability;
CVE-2025-23209 Craft CMS Code Injection Vulnerability;
CVE-2025-0111 Palo Alto Networks PAN-OS File Read Vulnerability;
CVE-2025-24989 Microsoft Power Pages Improper Access Control Vulnerability;
CVE-2017-3066 Adobe ColdFusion Deserialization Vulnerability;
CVE-2024-20953 Oracle Agile Product Lifecycle Management (PLM) Deserialization Vulnerability;
CVE-2024-49035 Microsoft Partner Center Improper Access Control Vulnerability;
CVE-2023-34192 Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability;
Links and more information:
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Five Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA

CISA Partners with ASD’s ACSC, CCCS, NCSC-UK, and Other International and US Organizations to Release Guidance on Edge Devices
CISA—in partnership with international and U.S. organizations—released guidance to help organizations protect their network edge devices and appliances, such as firewalls, routers, virtual private networks (VPN) gateways, Internet of Things (IoT) devices, internet-facing servers, and internet-facing operational technology (OT) systems.
Links and more information:
CISA Partners with ASD’s ACSC, CCCS, NCSC-UK, and Other International and US Organizations to Release Guidance on Edge Devices | CISA

Trimble Releases Security Updates to Address a Vulnerability in Cityworks Software
CISA is collaborating with private industry partners to respond to reports of exploitation of a vulnerability (CVE-2025-0994) discovered by Trimble impacting its Cityworks Server AMS (Asset Management System). Trimble has released security updates and an advisory addressing a recently discovered deserialization vulnerability enabling an external actor to potentially conduct remote code execution (RCE) against a customer’s Microsoft Internet Information Services (IIS) web server.
Links and more information:
Trimble Releases Security Updates to Address a Vulnerability in Cityworks Software | CISA

CISA and FBI Warn of Malicious Cyber Actors Using Buffer Overflow Vulnerabilities to Compromise Software
CISA and the Federal Bureau of Investigation (FBI) have released a Secure by Design Alert, Eliminating Buffer Overflow Vulnerabilities, as part of their cooperative Secure by Design Alert series—an ongoing series aimed at advancing industry-wide best practices to eliminate entire classes of vulnerabilities during the design and development phases of the product lifecycle. “Eliminating Buffer Overflow Vulnerabilities” describes proven techniques to prevent or mitigate buffer overflow vulnerabilities through secure by design principles and best practices.
Links and more information:
CISA and FBI Warn of Malicious Cyber Actors Using Buffer Overflow Vulnerabilities to Compromise Software | CISA