Securin

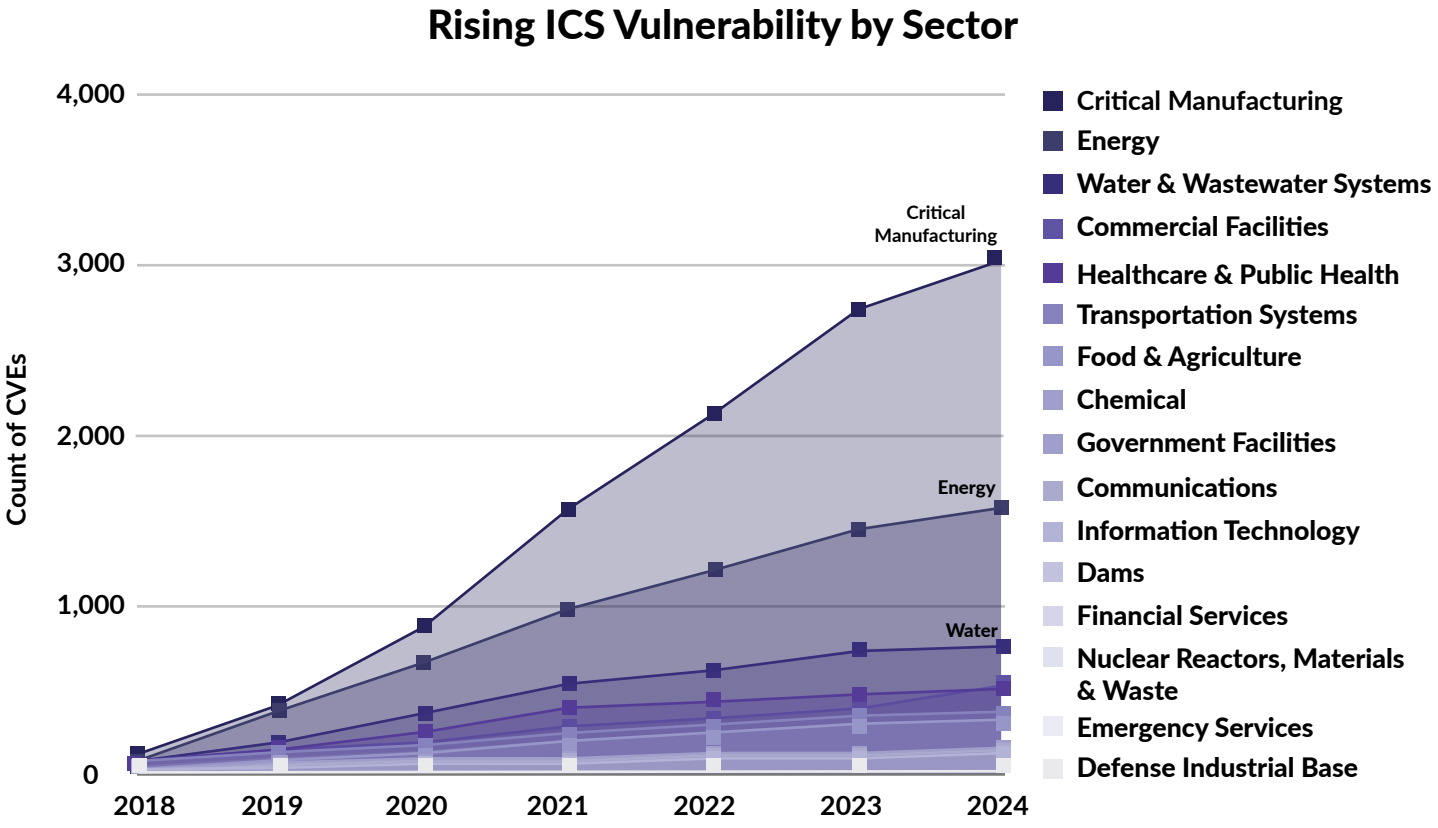
CISA Sectors
Critical Infrastructure

Overview 2024

Critical Risk Meets Critical Mass

Cyberthreats to industrial networks are a real and fast-growing challenge. An estimated 13 attacks per second[1] targeted critical infrastructure worldwide in 2023-2024 – more than 420 million hits.

As Securin research shows, this isn't an aberration, it's part of a significant global trend: vulnerabilities in Industrial Control Systems (ICS) like SCADA, HDI and medical devices are increasing, turning them into an ever-expanding attack surface that's all too easy for threat actors to exploit.



As things stand, critical manufacturing is by far the most vulnerable sector, with almost double the count of second-placed energy, followed by water and wastewater utilities in third place. With more than 3,000 vulnerabilities, software powering factories and robotics devices in the manufacturing sector can be viewed as a ticking timebomb, whether its nation state actors or cybercriminal groups, the potential for catastrophic damage is clear.

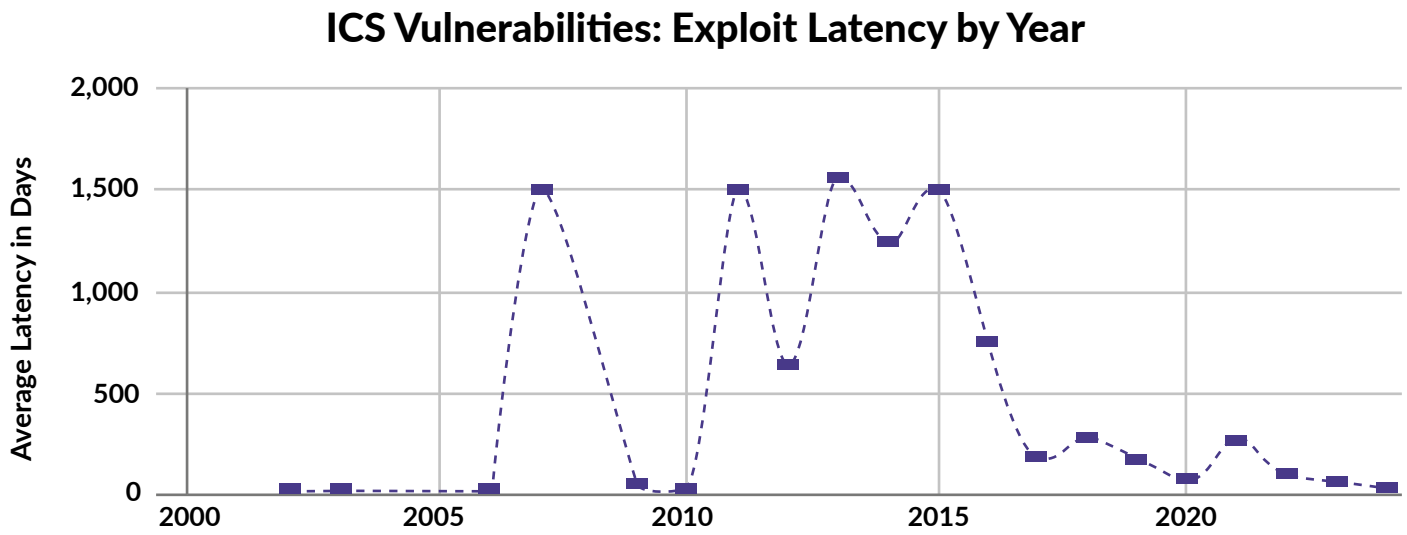
Wake Up Call

Securin research shows a clear upward trend, but the story behind it is concerning: some sectors have experienced increases in vulnerability in excess of tenfold. The nature of those vulnerabilities paints an even bleaker picture: from basic misconfigurations to public-facing applications and default credentials, it's evident that many sectors are making things far too easy for attackers.

When CISA stated in 2024 that threat actors are breaching US operational technology using "unsophisticated means", here's what that looks like in practice:

30%	**Vulnerability & Misconfiguration Exploits**	**22.8%**	**Compromised Credentials**
19%	**Spearphishing (Links & Attachments)**	**8.7%**	**External Remote Services**

Few statistics underline just how easy the sector is making it for attackers than latency – i.e. the gap between exploit publication and a CVE being published. As Securin's analysis of 41 CISA Known Exploited Vulnerabilities (KEVs) below shows, that window of time is shrinking at an alarming rate:



Looking at the latency by year, we can observe three things:

1. The trend towards a narrowing gap is likely accelerated by the adoption of "Industry 4.0" technologies. This tells us that the integration of digital technologies into manufacturing and industrial processes is making vulnerability exploits easier to write.

2. Average latency isn't so much dropping as plummeting: from **60 days in 2023 to 28 days in 2024** thus far. Attackers have an increased focus on OT and are taking less and less time to build their armory of exploits.

3. The fact that vulnerabilities from as far back as 2005-2015 continued to be exploited four years after publication tells us that attackers are all-too-aware of the presence of legacy/unpatched/end-of-life systems prominent in OT environments. They continue to exploit older vulnerabilities that are still persistent in the sector.

How bad can it get? Well…While some high-profile breaches have been marked by defenders' efforts to avert catastrophe, research indicates that only **56% of critical infrastructure organizations have ICS/OT-specific incident response**.

Why This Report?

Securin researchers analyzed **1,700 attacks on critical infrastructure targets in 2024**. Following sustained, increasing numbers of attacks over recent years, **Water & Wastewater, Energy, and Healthcare** have all been identified at the Federal Government level as sectors under intense pressure from cyberattackers. That's why we chose these three sectors as the focus for this report.

While recent years have seen increased coverage of attacks focusing on critical infrastructure, to date, there has been little in-depth analysis of why it's happening, and which vectors are being used. With this report, Securin seeks to open the conversation, look at some of the segmentation data, mapping vulnerabilities to exploits, exploits to threat actors, and bringing it all back to the core issue of weakness in software.

With so much at stake, and so much potential for catastrophe, it's time for some harsh realities to be confronted. As we'll see over the coming pages, there's a pattern. But first things first: let's start with an overview of some of the challenges.

"If it ain't broke…" The Challenge of Legacy Systems

Few sectors rely on legacy systems as much as critical infrastructure does. For those tasked with securing them, the integration of OT with IT networks has exposed previously isolated software and processes to modern threats they simply weren't designed to cope with. To compound the issue:

- 50% of defenders[3] say there's a lack of understanding of ICS/OT operational requirements among IT staff, making deeper insights into unique cybersecurity requirements harder to achieve.
- OT teams are often reluctant to update or patch legacy systems for fear of disruption or downtime. Where risk of de-stabilizing vital systems is high, simply pushing out a patch as soon as it becomes available isn't an option. Even if it was…
- There is no patch management system for ICS. Without an agent, it's impossible to detect threats as they pass through the system, all that's available is heuristics and passive scanning – and that's prone to false positives because it relies on outdated fingerprinting technology. When vulnerabilities are found, the issues around safety and process come back into play. The irony is that regulations designed to preserve safety can, in these instances, create risk because they delay patching. Between them, lack of agents and patching for ICS represent two of the greatest challenges to securing critical infrastructure.
- Resource constraints and limited budgets mean that teams often prioritize convenience or ease of use over security: default admin settings, ad hoc connections to public networks – or they're simply overwhelmed by the volumes of alerts received, with no capacity for triage and prioritization.

A Word on the Supply Chain

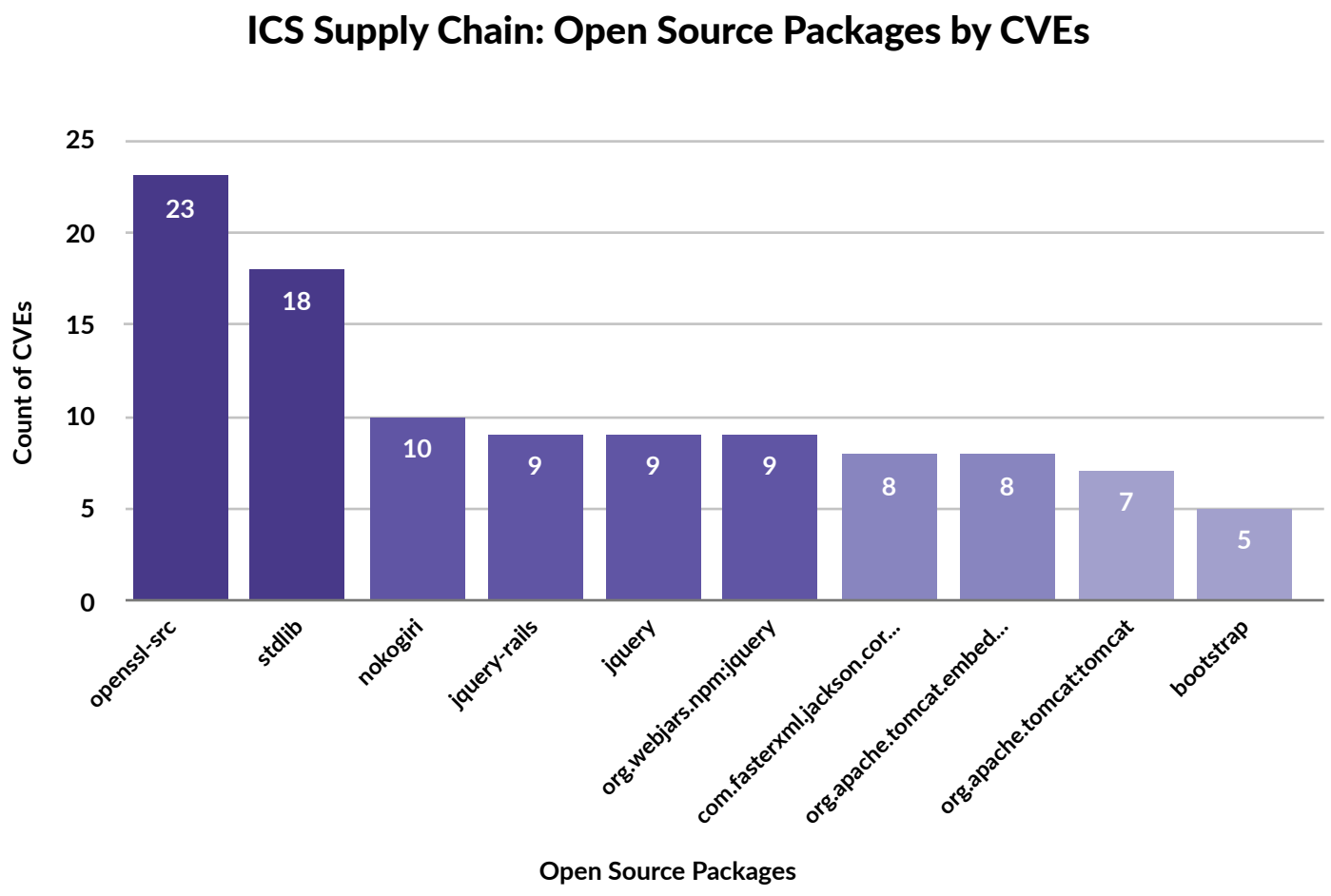
The above are all issues that – in theory, at least – can be controlled from inside the organization. Problem is, the number 1 attack vector[4] continues to be a pivot from the business IT network – so supply chain security is a crucial aspect of ICS security.

Ninety-one percent of organizations experienced at least one[5] software supply chain security (SSCS) incident in 2023. Chances are the other 9% are riding their luck: a single exploited vulnerability can trigger compromises that spread far beyond the initial point of weakness. For critical infrastructure, the results can be catastrophic.

The reality is that behind every SCADA, HMI or ultrasound machine sits a Linux or Windows OS and additional software providing services, probably using open source packages, maybe some Java or OpenSSL or jQuery…Reality dictates that, if, for example, there's a Linux vulnerability that exclusively impacts MRI machine, even the vendor themselves may be unaware of it.

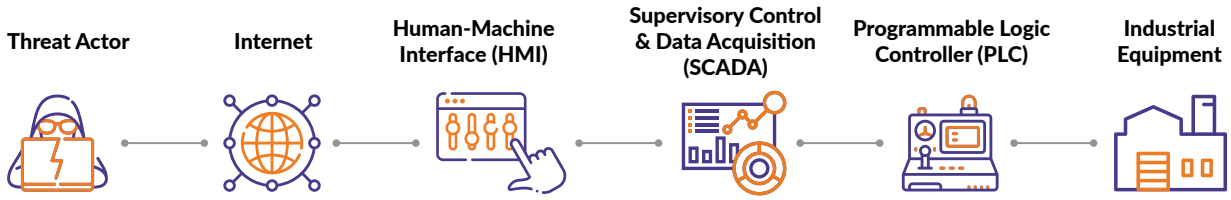
Now what?

Securin analysis reveals significant ICS supply chain exposure from software packages.



Drilling Into the Details

Vulnerabilities are escalating all the time, legacy systems are tricky to manage, you're not sure if your vendors understand that their software could be a risk for you, you can't patch on demand, and cyberattackers are having a field day.



In April 2024, the USA introduced the first high-level policy on critical infrastructure in over a decade, with the White House directive: National Security Memorandum on Critical Infrastructure Security and Resilience. CISA's FOCAL plan in September 2024 identified five priority areas, with goals ranging from addressing universal cybersecurity challenges to building defensible architecture:

1. Asset Management:

Full understanding of the cyber environment, including operational terrain and connected assets.

2. Vulnerability Management:

Proactively protect enterprise attack surface and assess defensive capabilities.

3. Defensible Architecture:

Design cyber infrastructure with an understanding that security incidents will happen and that resilience is essential.

4. Cyber Supply Chain Risk Management:

Quickly identify and mitigate risks, including from 3rd parties, posted to federal IT environments.

5. Incident Detection & Response:

Improve the ability of SOCs to detect, respond to, and limit the impact of security incidents.

While the federal government and agencies have introduced measures , the problem runs deep into individual state, local government and smaller service providers - often the organizations with the fewest resources or investment levels to cope. They might be out of sight in terms of the bigger picture, but they certainly aren't out of mind for attackers who recognize their potential as stepping stones to causing more widespread damage.

For this report, Securin analysts took a deeper look at three key sectors that have been the focus of sustained attack over recent years: Water and Wastewater, Energy, and Healthcare. What are their weaknesses? Who's attacking? What techniques are they using? Here's what we found...

Water & Wastewater Systems Sector

Vulnerable by Default? Water Gets a Wake-Up Call

Cyberattacks against US water infrastructure are increasing. The stark reality is that cyberdefenses are as weak as water.

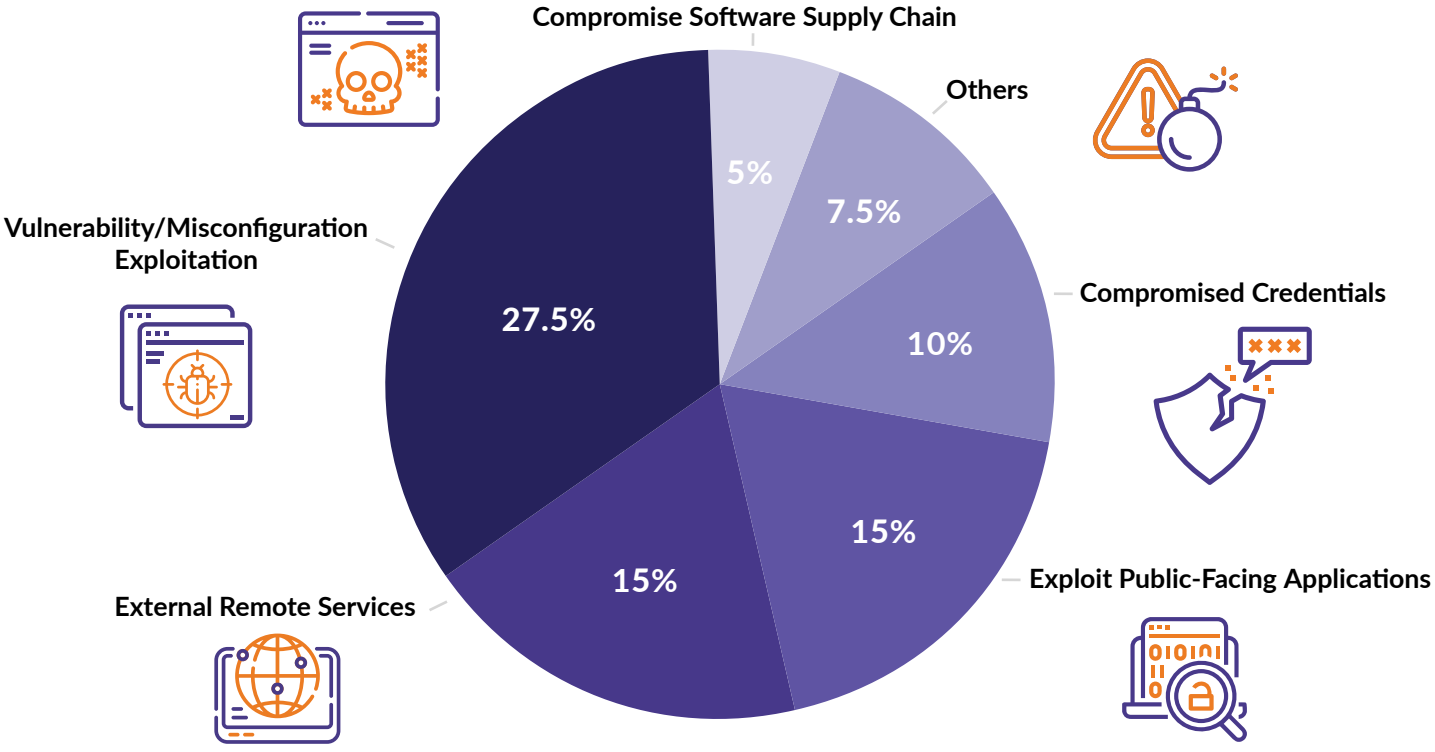
Over 70% of the water systems[7] inspected by the US Environmental Protection Agency (EPA) since September 2023 were in violation of standards meant to prevent cybersecurity breaches or other intrusions. Among the "alarming vulnerabilities at drinking water systems across the country", the EPA cited default password use, single log-ins for all staff, and access control failures.

Securin's **analysis of 75 attacks in 2024** alone shows a sector struggling to implement even basic cybersecurity hygiene. When the EPA refers to the sector as "largely non-compliant", our research shows that what that means in practical terms is failure to implement even basic hygiene:

27.5%	**Vulnerability & Misconfiguration Exploits**
15%	**Exploitation of Public-Facing Applications**
10%	**Compromised Credentials**

What we see in Securin's data is a sector defined by ad hoc connections to public networks, misconfiguration issues, vulnerability exploits and poor credential management.

Initial Access Vectors Distribution (%) - Water & Wastewater Systems



The Path of Least Resistance is Wide

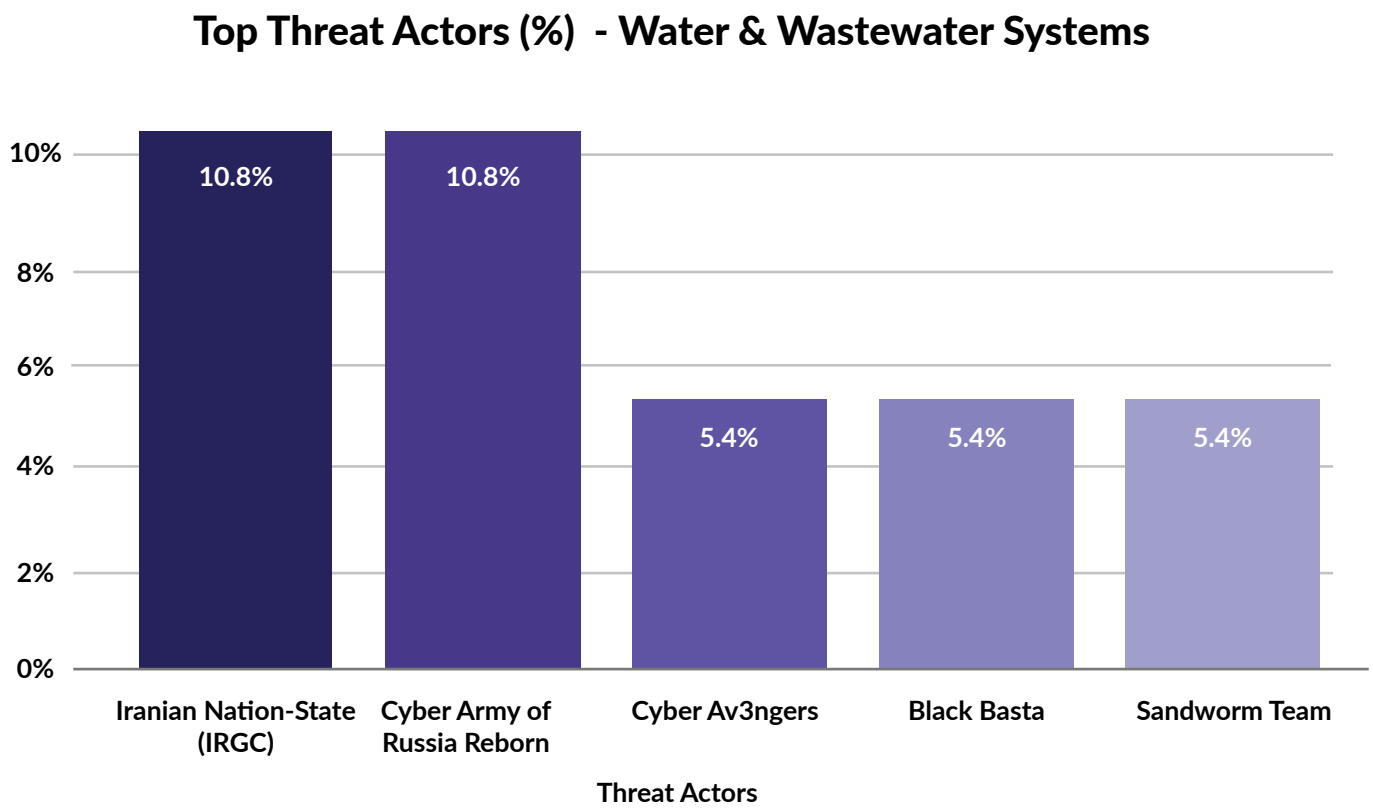
Digging a little deeper into the data, we found that water and wastewater ICS are the third-most vulnerable in 2024. We counted 800+ vulnerabilities, including:

CVE-2023-6448: The Unitronics PLC vulnerability exploited by Cyber Av3ngers to target the Municipal Water Authority of Aliquippa.

CVE-2024-6242: A high-severity bypass on Rockwell automation devices could allow unauthorized access.

Who's Attacking Water Infrastructure?

Perhaps unsurprisingly for such a vital sector, the leading threat actors targeting the United States' water and wastewater systems are nation-state – or widely believed by federal agencies to be affiliated in some way:



Among the groups that 'specialize' in targeting water infrastructure, the leading groups are all believed by US authorities to be affiliated with or directly sponsored by Iran or Russia. Research shows that these threat actors are targeting smaller utilities, presumably seeking to take advantage of limited resources.

Let's take a quick look at how they operate:

Threat Actor

The Islamic Revolutionary Guard Corps (IRGC) was behind **10.8%** of the attacks Securin analyzed. IRGC-affiliated **CyberAv3nger**s was associated with **5.4%**.

MO: Both groups have actively targeted Unitronics PLCs, mainly exploiting default port settings, along with compromised/default credentials to gain access. The Municipal Water Authority of Aliquippa in Pennsylvania was one of the utilities impacted.

Threat Actor

The Cyber Army of Russia Reborn (CARR) emerged as a significant threat late 2023/early 2024. Believed to have ties to the Kremlin's **Sandworm** group, between them, they account for **16.2%** of attacks.

MO: As with their Iranian counterparts, CARR and Sandworm exploit open ports, default passwords and compromised credentials to access SCADA and PLCs. Early in 2024, the CARR posted videos online that appeared to show it manipulating ICS software for water utilities in Abernathy and Muleshoe, TX.

Water Utilities Under Cyberattack: Some Solutions

Following several high-profile attacks, water companies have so far responded well to mitigate the potential damage. But hoping for the best is poor strategy in a threat environment where attackers only need to get lucky once, but the defenders have to stay lucky in the face of relentless persistence: Hale County Water Supply in rural Texas withstood 37,000 attempts on its firewall in four days. Its counterpart in Muleshoe Water Plant wasn't as successful, and had to take systems offline as a preventative measure.

In the wake of multiple breaches, the EPA is urging even small water systems operators to improve defenses. Many of the attacks in 2024 targeted these smaller operators – with enough success to generate concern.

With **more than 150,000 public water systems in the USA**, it's time for urgent action to mitigate weakness across IT and OT systems. Water and wastewater utilities must prioritize proactive security, and pay attention to IT and OT convergence.

We'll take a look at some actions they can take in the "Best Practices" section of this report.

Energy Sector

Vulnerable to a Fault: Is Energy Too Easy a Target?

The energy sector was the target for more than 13% of critical infrastructure cyberattacks in 2024. And it's becoming more vulnerable by the day.

With a **30% increase in CVEs since 2023**, energy is the #2 sector for ICS vulnerabilities, and the fourth most targeted critical infrastructure sector in 2024. The number of points in the US power grids that are vulnerable to cyberattack is increasing at a rate of **approximately 60 per day**.[8]

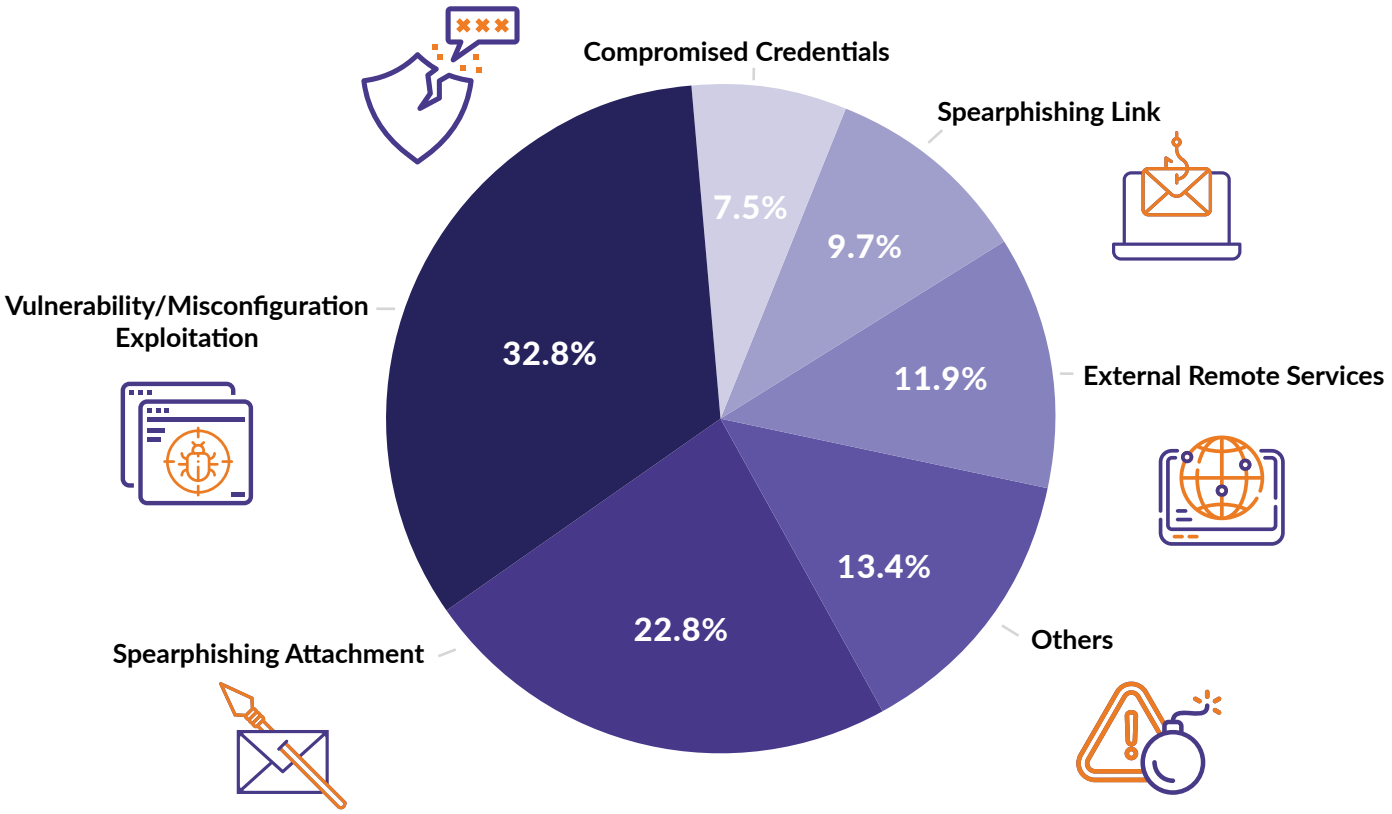
It's the kind of upward trend that no one wants to be a part of: in 2023, energy sector incidents (including power generation, water treatment and electricity production) reached a new high: **185 security incidents** were reported to the US Department of Energy.

Enter 2024, and Securin's analysis of **263 attacks** shows a sector in the spotlight for some of the world's most prominent threat groups. For such a critically important target, there's a worrying trend around energy's vulnerabilities.

Vulnerability and misconfiguration exploitation are the leading access vectors – at almost 33%

Spear phishing (using attachments & links) account for more than 25% of access vectors

Initial Access Vectors Distribution (%) - Energy



It Started with a Phish…

This year's Verizon Data Breach Investigations Report noted a **180% increase in the exploitation**[9] of vulnerabilities as the critical path to action to initiate a breach. It also found that **73% of internal breaches were due to human error**. In a world where it takes a median 60 seconds for users to fall for a phishing email, what Securin is seeing in the energy sector is a deadly combination: vulnerability and misconfiguration PLUS spear phishing. At the heart of both issues: human error, and the ease with which threat actors can leverage it to make their first move when exploiting software vulnerabilities.

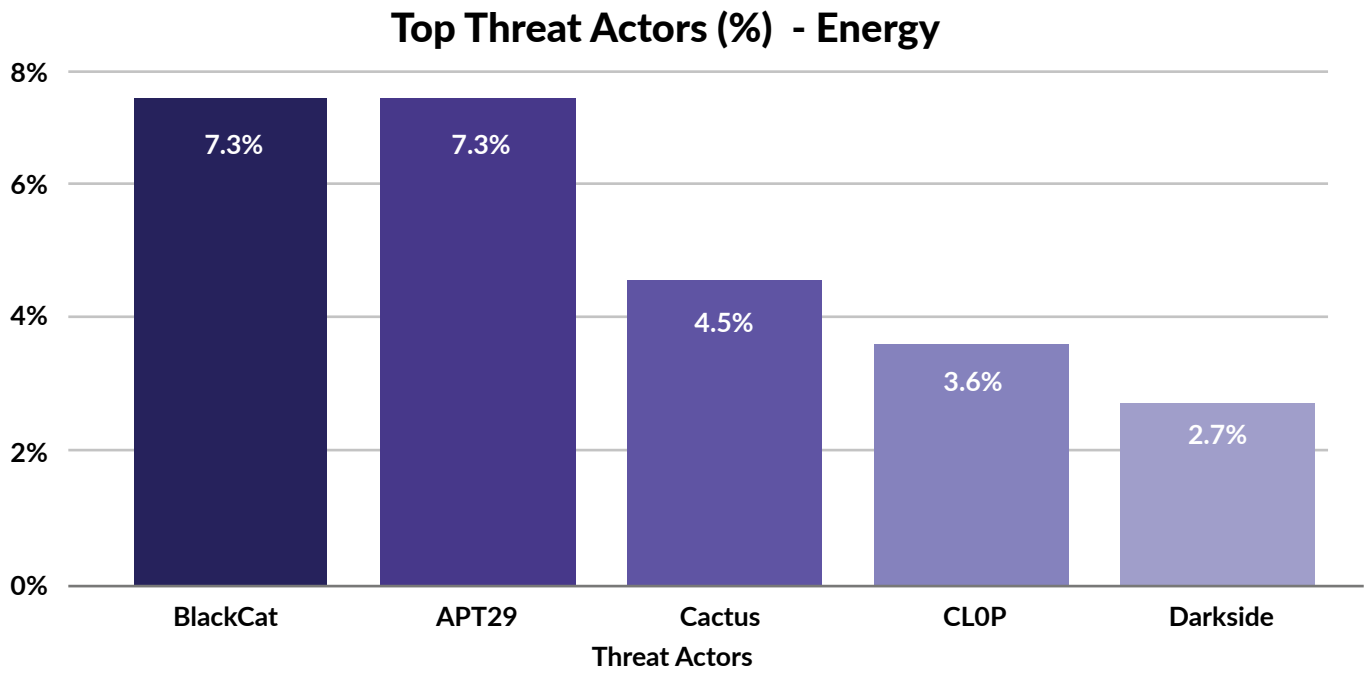
Also cause for significant concern: the combination of compromised credentials and connection to external remote services. Again, Securin's data suggests that, when it comes to cybersecurity, many energy sector systems are either too under-resourced to plug the gaps or too under-resourced to risk introducing any additional friction by eliminating default credentials, settings or access to the public internet. That's a big problem for a sector faced with **1,626 CVEs**, including:

CVE-2023-0669: The flaw behind the 2023 Hitachi Energy breach, this zero-day vulnerability in the Fortra GoAnywhere file transfer software enabled remote code execution (RCE) – and became the pathway in more than 450 incidents.

CVE-2023-28771: This command injection vulnerability in Zyxel firewalls was at the center of a co-ordinated attack on 22 Danish energy providers. Despite the availability of a patch, many companies hadn't updated.

With ICS vulnerabilities in plentiful supply, the energy sector is attracting the attention of some of the world's most prominent, persistent threat groups. Who are they and what are their methods?

Who's Attacking Energy Infrastructure?



Threat Actor

BlackCat / ALPV / Noberus: Responsible for 7.3% of the attacks analyzed by Securin, the U.S. Department of State has put a $10m bounty on this ransomware group's leaders. Significant attacks to date include energy operators in Germany, Luxembourg, and Italy.

MO: BlackCat gains initial access via stolen credentials, and has exploited known vulnerabilities such as Log4j for lateral movement.

Threat Actor

APT29 / Cozy Bear: The group behind the **SolarWinds** supply chain breach, and believed to be Russian state-sponsored. APT 29 has a long association with cyber espionage and targeting critical industries – accounting for 7.3% of energy sector attacks.

MO: The group has evolved from password spraying and brute force techniques to targeting cloud services and accounts, often registering its own devices on compromised cloud tenants. Once a single device is compromised, the attackers escalate and expand further into the network.

Energy Sector Cyberdefense: It's Time for Positive Action

Seventy-eight percent[10] of energy professionals say that geopolitical uncertainty has made them more aware of the potential vulnerabilities in their operational technology (OT) systems. With the second most vulnerable ICS in 2024, it's time to move beyond awareness and into action.

As with the water and wastewater sector, energy's cybersecurity posture looks weak at best. Characterized by open ports, default admin settings, weak passwords, and misconfigurations – the room for improvement is clear, and we'll take a look at some of the actions and mitigation strategies in the "Best Practices" section of this report.

Healthcare & Public Health Sector

Compromised Immunity: Healthcare's Fragile Cybersecurity System

It's a tough diagnosis to accept, but with over 300 breaches in the first half of 2024 alone, cyberdefenses in the healthcare sector appear to be flatlining.

Securin research indicates that healthcare looks set to close out 2024 in the **top three most targeted sectors** for cyberattackers.

To say that it hasn't been a good year for the sector is something of an understatement: the Change Healthcare attack alone is projected to impact the health information of one in three Americans.[11] And with the 5th most vulnerable ICS environment in our analysis, an already-fragile system continues to attract attackers.

Eighty percent of healthcare institutions rely on legacy systems, often encompassing electronic health record (EHR) systems with legacy components that are difficult to manage due to complexity and the long-term nature of patient records.

We've already discussed the impact that legacy systems continue to have on critical sectors, but when you combine the old with the increasing numbers of internet-connected devices in use in modern healthcare settings, it starts looking like a ticking time bomb.

Easy Access Across Multiple Vectors

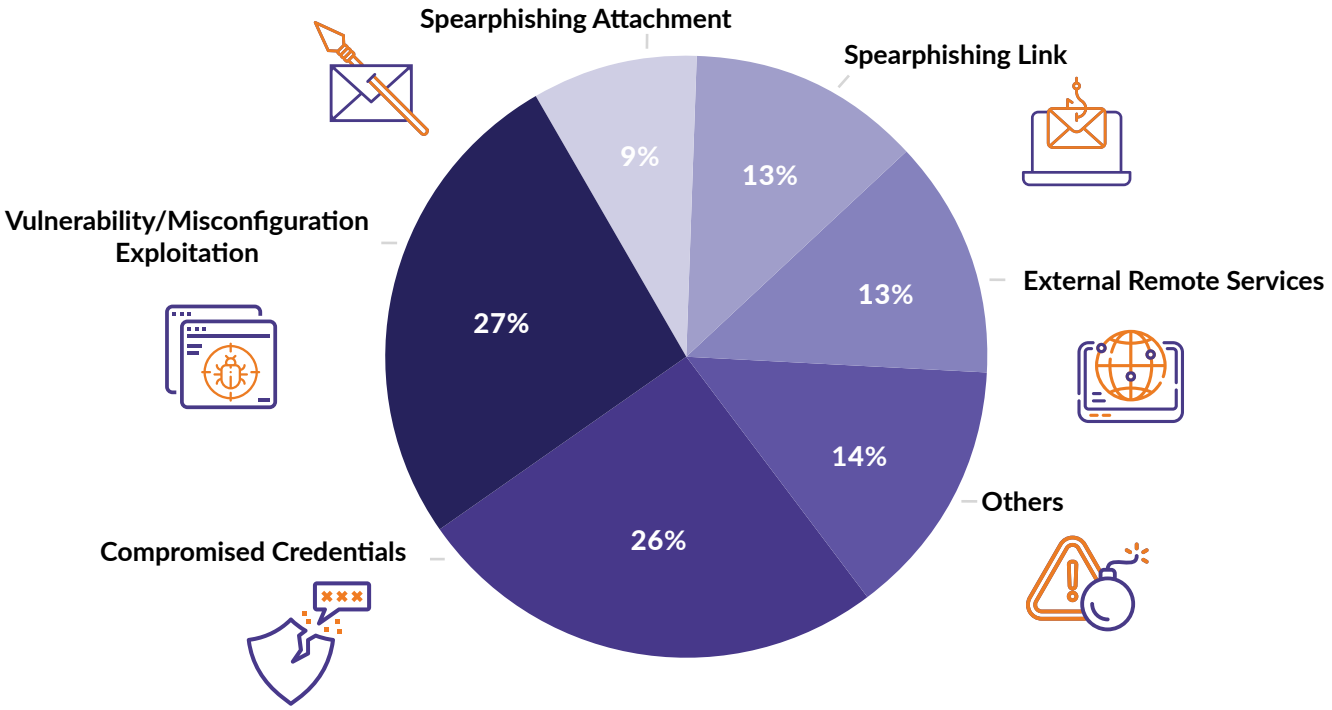
Securin analyzed **519 attacks** on the healthcare sector in 2024. The results show a sector characterized by multiple vectors that, leveraged together, have the capacity to amplify impact, or multiply opportunities for success.

Between them, compromised credentials and misconfiguration – both areas that are considered 'low hanging fruit' in theory, if not always in practice – account for more than half of initial access.

27%	Vulnerability & Misconfiguration Exploits
26%	Compromised Credentials
22%	Spear Phishing Link or Attachment

As in the other sectors we've analyzed, the prevalence of "easy pickings" in healthcare ICS and other systems likely goes a long way towards explaining the aggressive targeting of this sector, mainly by criminal gangs. On one hand, optimum scope for catastrophe promises high ransom payouts. On the other, with log-ins and credit card details a dime-a-dozen, medical records – which typically provide a near-complete picture of the individual – represent a lucrative payday. That's a picture borne out by the data around who's attacking.

Initial Access Vectors Distribution (%) - Healthcare & Public Health



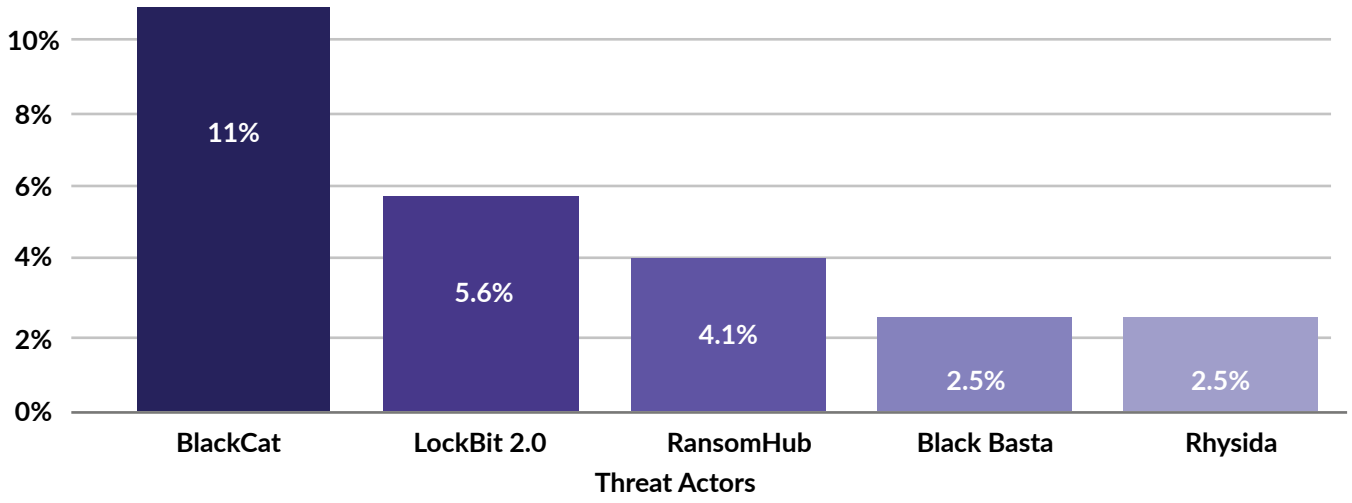
Attackers focusing on healthcare, exploitation of known vulnerabilities is a feature, including:

CVE-2018-13379: Easy to exploit, and with potential to have a wide reach, this critical flaw impacts FortiOS VPN devices, allowing attackers to steal VPN credentials and compromise VPN networks running those devices.

CVE-2020-1472: The ZeroLogon critical vulnerability impacted Windows systems, allowing privilege elevation for attackers to gain administrator rights without authentication.

Who's Attacking Healthcare Infrastructure?

Top Threat Actors (%) - Healthcare & Public Health



Threat Actor

Lockbit 3.0's aggressive targeting of healthcare systems in 2024 exposed a deep vein of weakness in medical software and systems, including unpatched vulnerabilities in outdated software, VPNs and RDPs. Responsible for an estimated 44% of all ransomware attacks globally in 2023, the group claims to be "Completely apolitical, and only interested in money."

MO: Lockbit's favored initial access methods include exploiting public-facing applications, weak passwords / lack of MFA, phishing, and remote desktop protocol (RDP). It has been known to exploit CVEs in widely used products including Microsoft Windows Server and Exchange.

Threat Actor

RansomHub: Since February 2024, this relatively new ransomware group has attacked over 200 targets, many of them healthcare. Although not directly involved, the group claimed to have access to the data stolen from the Change Healthcare attack.

MO: Initial access is via exploitation of known vulnerabilities in services including Netlogon, ZeroLogon and Confluence. The group has been observed scanning networks and creating user accounts, phishing and password spraying.

Healthcare Sector Cybersecurity: Early Intervention Wins

As we keep seeing across the critical infrastructure sectors, older, known software vulnerabilities continue to give attackers an easy pathway into systems. Despite the availability of patches, many of these weaknesses continue to feature in attacks – underlining the critical importance of getting to grips with attack surface management and patching. Weakness in code like cross-site scripting and SQL injection continue to be introduced to code - and exploited by attackers. Years after they were first flagged, here are some old favorites that continue to be exploited:

CWEs That Have Consistently Been in the Top 10 CWE

- **CWE-79:** (Cross-site Scripting)
  - topping the list with 30,820 CVEs mapped, highlights the risk of XSS attacks in web apps
- **CWE-787:** Out-of-bounds Write
- **CWE-20:** Improper Input Validation
- **CWE-89:** Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- **CWE-200:** Exposure of Sensitive Information to an Unauthorized Actor
- **CWE-22:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

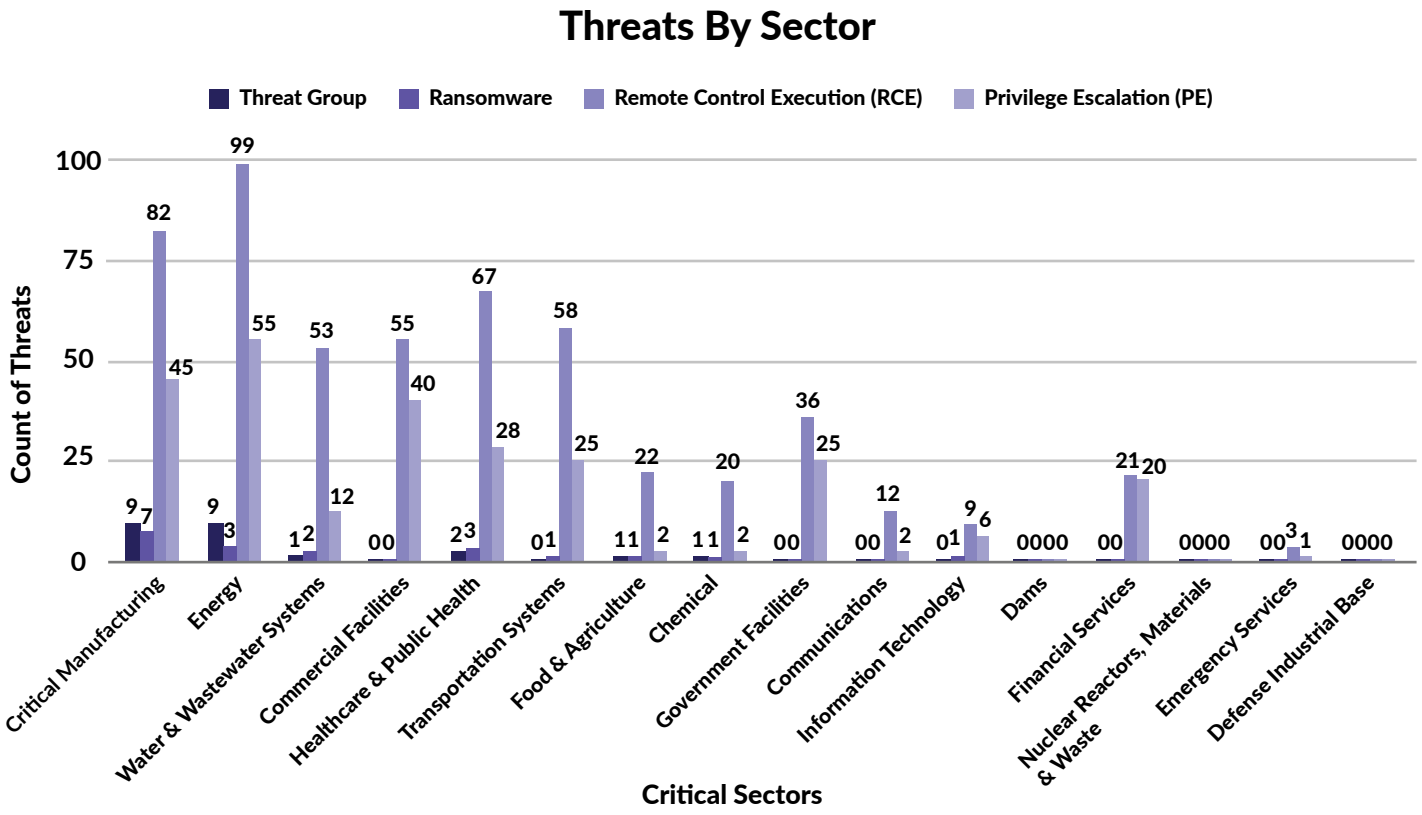
Following years of voluntary cybersecurity, many are now calling for mandatory standards for healthcare. It's time to wake up and take responsibility for monitoring and securing attack surfaces – it's no longer a nice-to-have, it's a necessity.

Where to from here? Strengthening cybersecurity with

Best Practices for Securing Critical Infrastructure

The scale of attacks is worrying, but the lack of sophistication works both ways: there are some easy wins that critical sector defenders can start with today.

First things first: a general overview of the critical infrastructure sector gives us a sense of some of the issues everyone is facing:

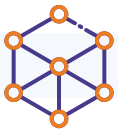


As Securin's data shows, Remote Code Execution (RCE) and Privilege Escalation (PE) are by far the most prominent threats across all critical sectors. We're not the only ones to notice: 62.4% of CISA KEVs are RCE or PE exploits, making them among the most lucrative exploits for threat actors. Both RCE and privilege escalation flaws allow attackers to take complete control of any system, execute arbitrary code, and potentially make lateral moves into sensitive data or critical infrastructure.

Bottom line: it takes around 55 days to remediate[12] 50% of critical vulnerabilities once a patch is available. As this year's Verizon DBIR put it: "If it goes into the KEV, go fix it ASAP."

How do you fix problems you don't know you have? And what actions should you take when you do?

Best Practices for Proactive Cybersecurity in Critical Infrastructure



1. Gain Visibility

Start with a comprehensive IT/OT asset inventory and security assessment to identify critical vulnerabilities across your industrial control systems and connected infrastructure. Monitor products nearing their end of life (EOL) or end of support (EOS) – neglecting this can leave systems vulnerable to exploitation by threat actors. Leverage External Attack Surface Management (EASM) to continuously discover, inventory, and assess internet-facing assets and shadow IT that could provide attackers entry into your OT environment.

2. Get Your Priorities Right

Prioritization is critical, especially for legacy systems: identify attacker pathways and use Vulnerability and Threat Intelligence to determine exploitable risk. This involves assessing which vulnerabilities are most likely to be targeted, based on threat actor tactics, techniques and procedures (TTPs), as well as evaluating the severity and potential impact on critical systems. By focusing on the most likely attack vectors, organizations can allocate resources more effectively and mitigate the highest-risk vulnerabilities first.

3. Segmentation

Prioritize implementation of network segmentation using industrial firewalls and unidirectional gateways to create secure zones between IT/OT environments.
If legacy systems must be used, separate them from the main network to prevent widespread compromise during cyberattacks. Using modular systems will allow you to deploy isolated shutdowns and incremental upgrades.

4. Control Access

Establish robust access control policies, including privileged access management for SCADA systems, multifactor authentication (MFA) for remote connections, and perform regular access reviews.

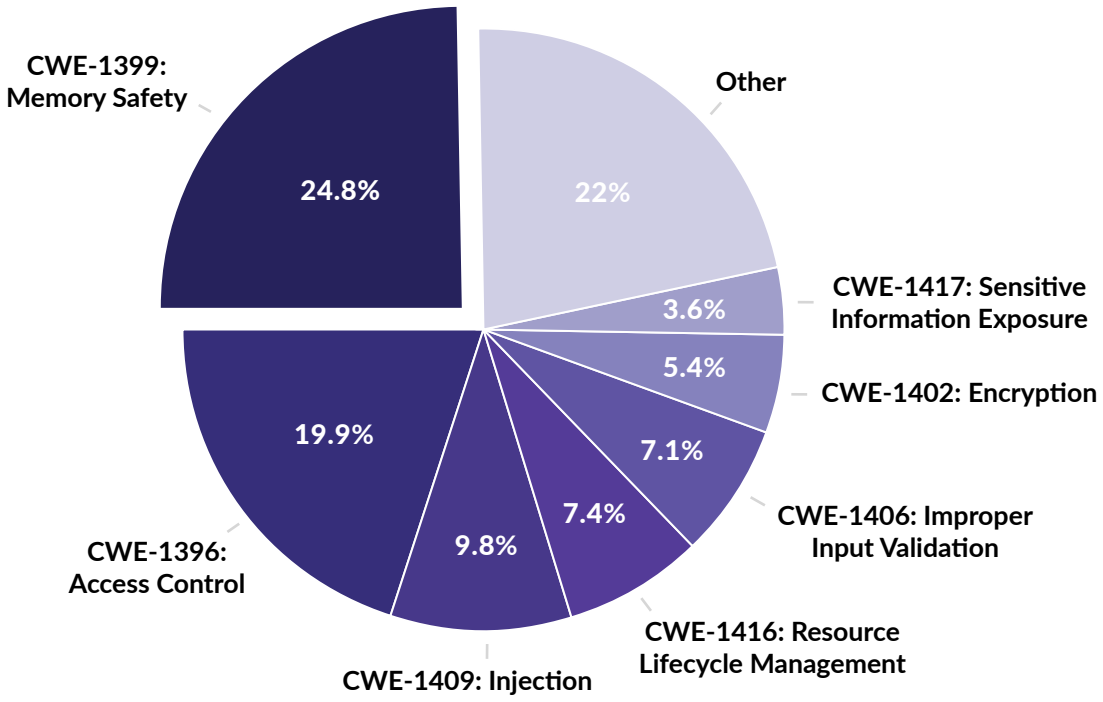
5. Build Resilience

Create incident response playbooks specifically for OT disruptions, including offline backups of PLC configurations, and regular tabletop exercises. Incident response plans help organizations minimize incident impact, reduce downtime, and protect critical assets.

6. Go Multilayered

Implement a multi-layered security approach that considers legacy systems. Choose tailored cybersecurity solutions that are compatible with older systems, and use network security barriers, intrusion detection, prevention systems, and robust antivirus software.

Know Your Attack Surface:
Top 3 ICS Weaknesses by Category



#1 CWE 1399 - Memory Safety (24.8%)

CISA estimates that this class of vulnerability is responsible for about 70% of all security vulnerabilities in software. Attackers can exploit it to execute arbitrary code and buffer overflow attacks such as the “Heartbleed” attacks impacting HMI/SCADA and ICS running vulnerable versions of OpenSSL. Securin research from earlier in 2024 shows that this class of weakness contributes over 25% of CISA’s Known Exploited Vulnerabilities (KEVs) – and, as the graph below shows, this trend tracks for ICS.

#2 CWE 1396 - Access Control (19.9%)

Access control issues are dominant - and dangerous - in ICS appliances, due to the increased connectivity brought by IT/OT convergence, which integrates operational technologies with IT networks. Weak or misconfigured access controls expose critical OT systems to unauthorized access, making them vulnerable to attacks such as privilege escalation, ransomware and remote exploitation.

#3 CWE 1409 - Injection (9.8%)

Injection issues are critical for ICS appliances, particularly in the context of IT/OT convergence, because they allow attackers to manipulate control commands or data flows. ICS devices often process unvalidated inputs, making them susceptible to SQL, command, or code injection attacks. These vulnerabilities can enable attackers to alter operational parameters, disrupt processes, or exfiltrate sensitive data.

References

1 **Security Today:** https://securitytoday.com/articles/2024/01/29/world-critical-infrastructure-suffered-13-cyber-attacks-every-second-in-2023.aspx

2 **SANS State of ICS/OT Cybersecurity 2024:** https://www.sans.org/white-papers/sans-2024-state-ics-ot-cybersecurity/

3 **SANS State of ICS/OT Cybersecurity 2024:** https://www.sans.org/white-papers/sans-2024-state-ics-ot-cybersecurity/

4 **SANS State of ICS/OT Cybersecurity 2024:** https://www.sans.org/white-papers/sans-2024-state-ics-ot-cybersecurity/

5 **Tech Target:** https://www.techtarget.com/esg-global/wp-content/uploads/2024/05/Infographic-Software-Supply-Chain-May-2024.pdf

6 **Congressional Research Service:** https://crsreports.congress.gov/product/pdf/IF/IF12716

7 **EPA:** https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities

8 **North American Electric Reliability Corporation:** https://www.nerc.com

9 **Verizon Data Breach Investigations Report:** https://www.verizon.com/business/resources/reports/dbir/

10 **DNV Energy Cyber Priority 2023:** https://www.dnv.com/publications/energy-cyber-priority-2023/

11 **HIPAA: H1 2024 Healthcare Data Breach Report:** https://www.hipaajournal.com/h1-2024-healthcare-data-breach-report/

12 **Verizon Data Breach Investigations Report:** https://www.verizon.com/business/resources/reports/dbir/

About Securin

At Securin, we empower teams and organizations to minimize their business risk with our comprehensive range of offensive cybersecurity solutions. These solutions are carefully crafted to be intuitive, adaptable, and scalable, catering to organizations of all sizes in today's ever-changing digital landscape. Securin's human-augmented intelligence approach to cybersecurity empowers organizations to thrive by proactively addressing emerging threats and uncertainties, ensuring their security.

Follow Us On

Securin
securin.io