T82
THE CLAROTY RESEARCH TEAM

CLAROTY

STATE OF XIoT SECURITY

Team82's analysis of vulnerabilities impacting cyber-physical systems across the Extended Internet of Things—2H 2022

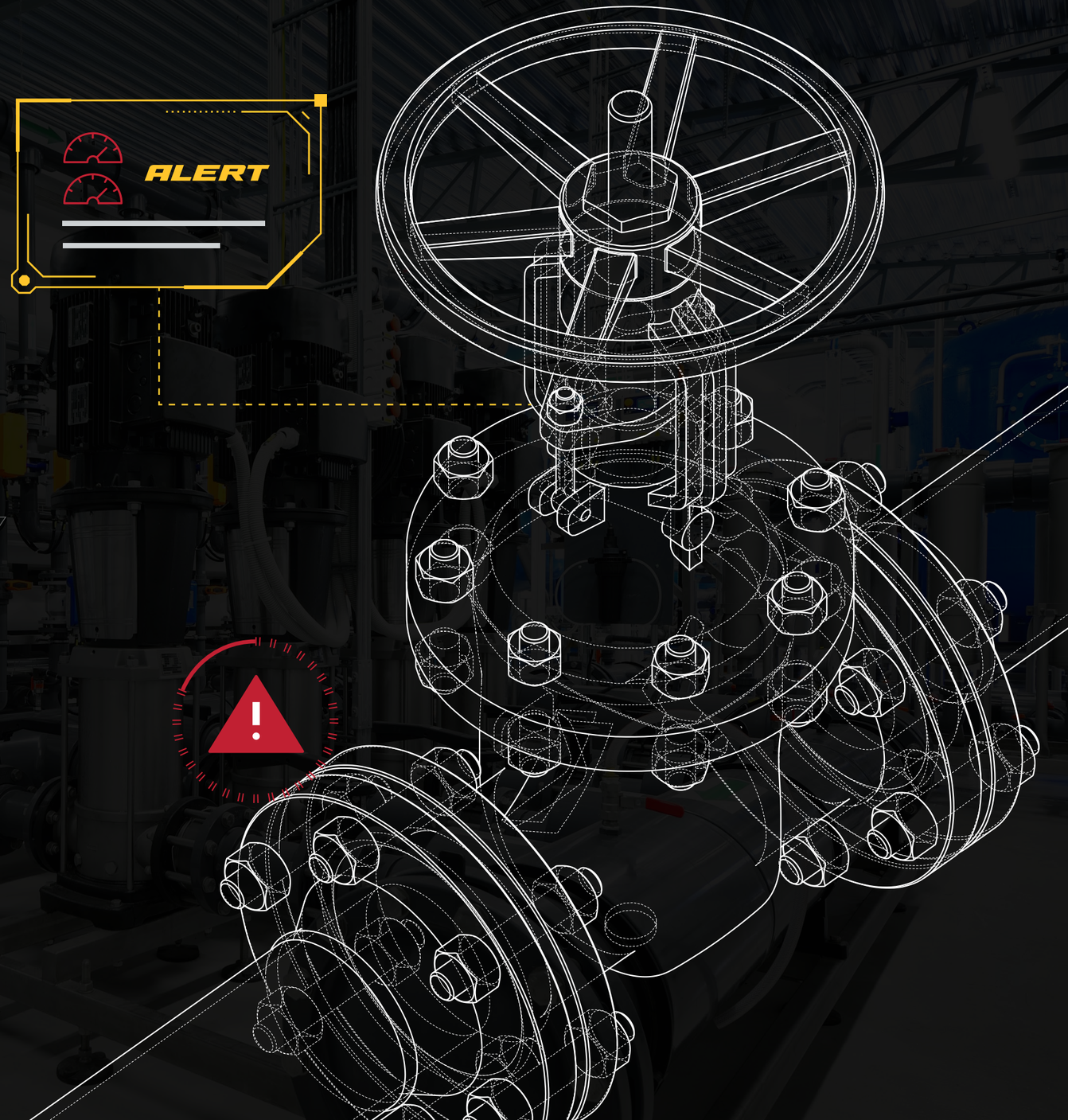
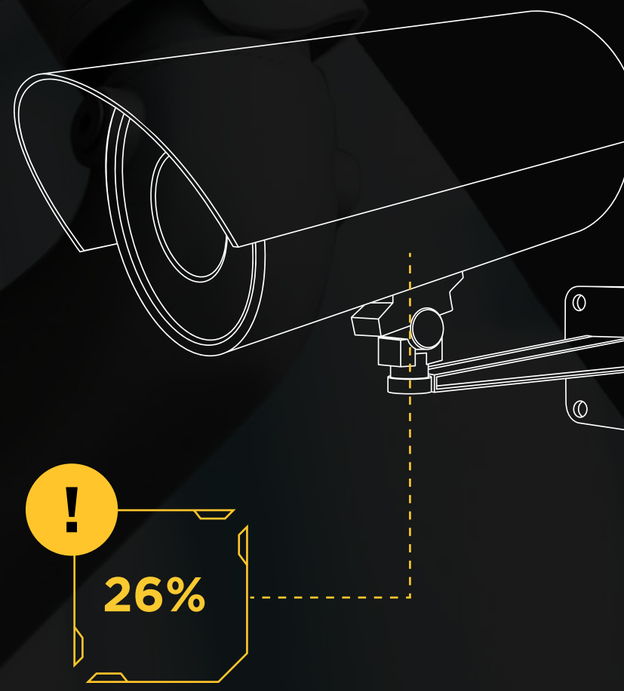
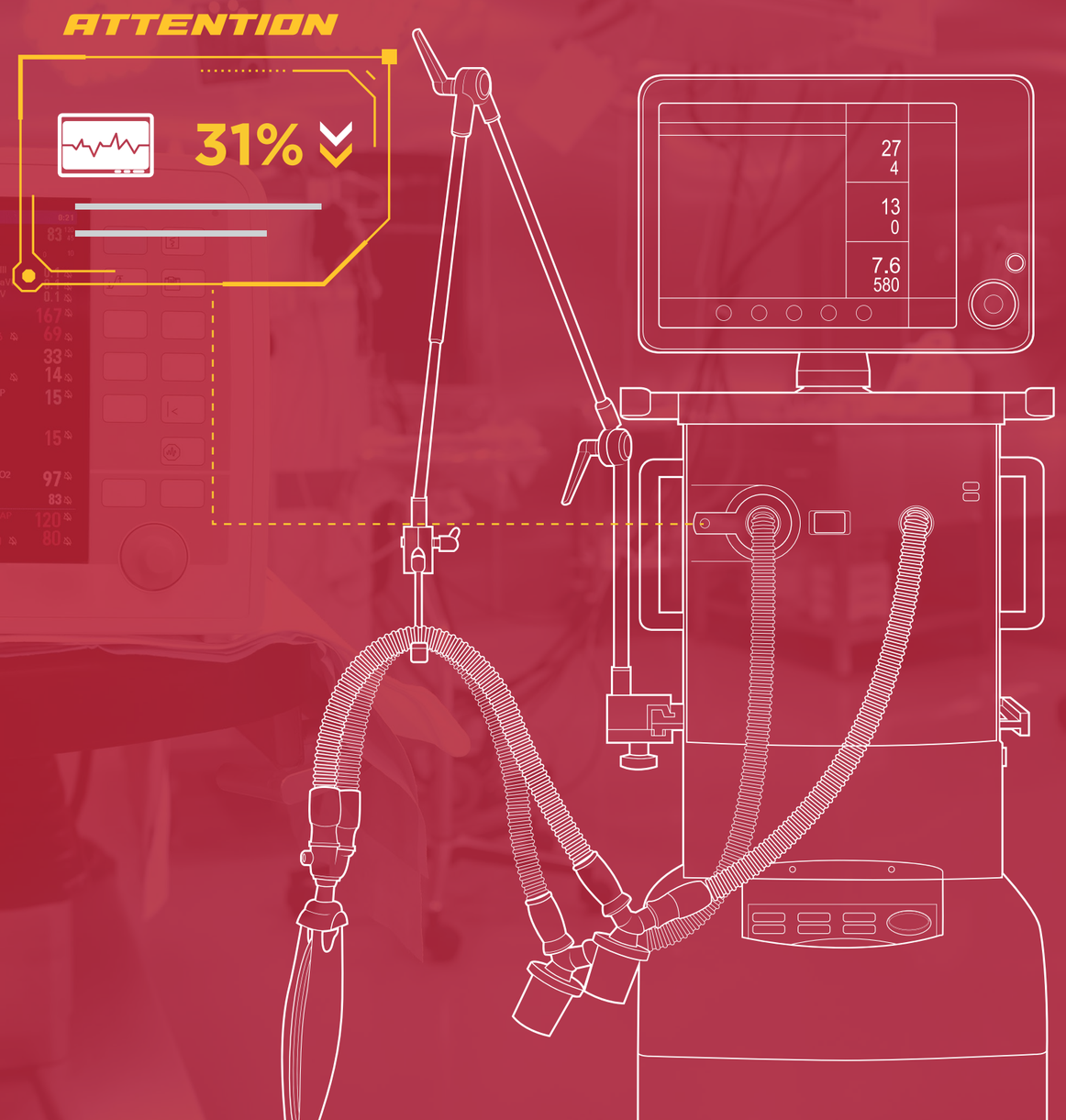


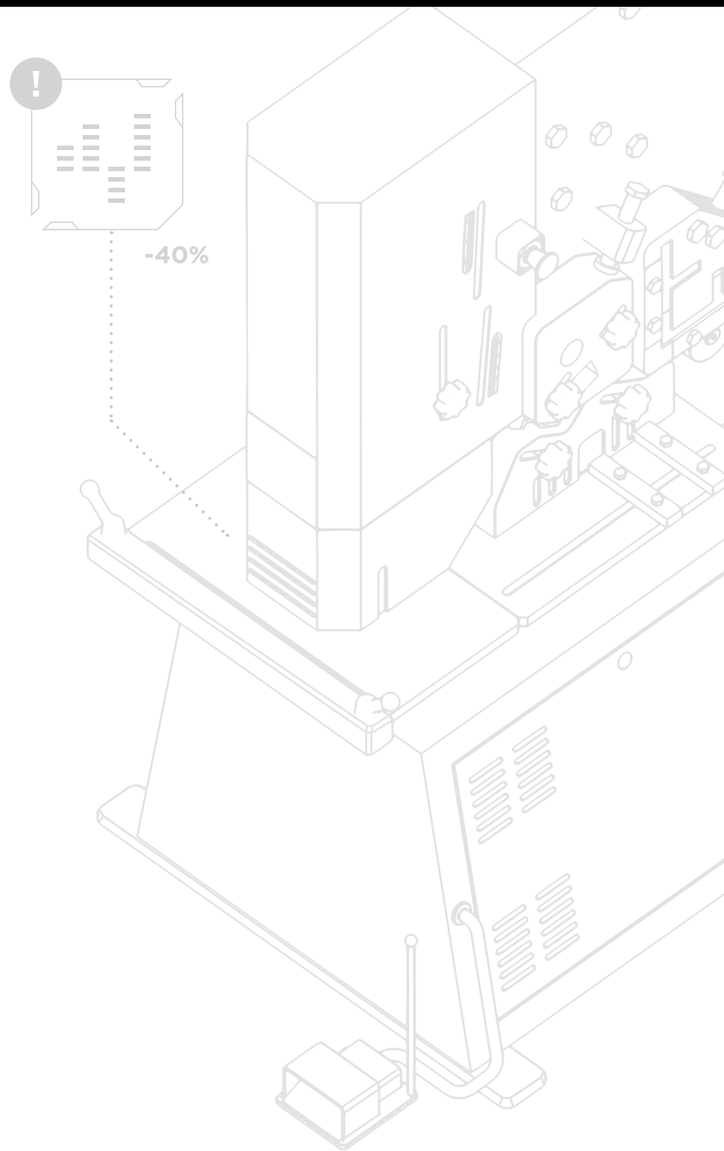
TABLE OF CONTENTS



EXECUTIVE SUMMARY



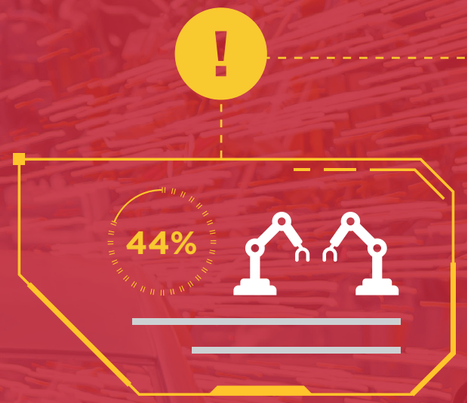
EXECUTIVE SUMMARY



Below are some of the key findings from the State of XIoT Security Report: 2H 2022.

- The State of XIoT Security Report 2H 2022 shows a second straight decline in the number of published vulnerabilities in cyber-physical systems.
- In parallel, the number of vendor-disclosed vulnerabilities has grown significantly since our first report in 2020.
- This indicates that vendors are increasing their investments in cyber-physical systems security, and improving the posture of their products and product-security programs.
- For the first time, the number of vendor self-disclosures of XIoT vulnerabilities has surpassed those of third-party security companies' research teams and independent researchers.
- Of the 688 published vulnerabilities in the 2H of 2022, 74% of those affect OT devices; OT vulnerabilities continue to dominate our dataset.
- 62% of published OT vulnerabilities affect devices at Level 3 of the Purdue Model for ICS, while one quarter of published vulnerabilities impact Level 1, or Basic Control devices, including PLCs and other controllers and sensors.
- Software-based vulnerabilities have traditionally dominated our dataset and this continues to be the case. Given the maturity of tools and awareness in the software security space, vendors are quicker to update software vulnerabilities than those found in firmware.
- The number of published IoT vulnerabilities dropped sharply after a noteworthy increase during the 1H of 2022.
- 487 published vulnerabilities in the 2H of 2022 were either assessed a critical or high-severity CVSS v3 score.
- There were 110 critical vulnerabilities in the second half of 2022, only 10 behind the peak number uncovered during the 2H of 2021.
- Team82 reported 65 vulnerabilities during the 2H 2022, and 117 throughout last year.
- 30 of those 65 vulnerabilities were assessed a CVSS v3 score of 9.5 or higher.
- 63% of published vulnerabilities in Team82's data set are exploitable over the network
- The top impacts of published vulnerabilities in the 2H 2022 are: remote code execution, denial-of-service attacks, and bypasses of security mechanisms such as authentication.
- Four of the top five CWEs in our 2H 2022 dataset are also prominent in the top five of MITRE's top 25 CWE list.
- Top mitigations recommended for published vulnerabilities in the 2H 2022 include network segmentation, secure remote access, and ransomware protection. Within OT, other mitigation strategies were traffic restriction, user and role policy implementation, and workstation hardening.

INTRODUCTION



INTRODUCTION

For more than three years, and now six of these reports, Claroty Team82 has provided biannual analyses of publicly disclosed vulnerabilities affecting operational technology (OT), internet of things (IoT) devices, and most recently, the internet of medical things (IoMT).

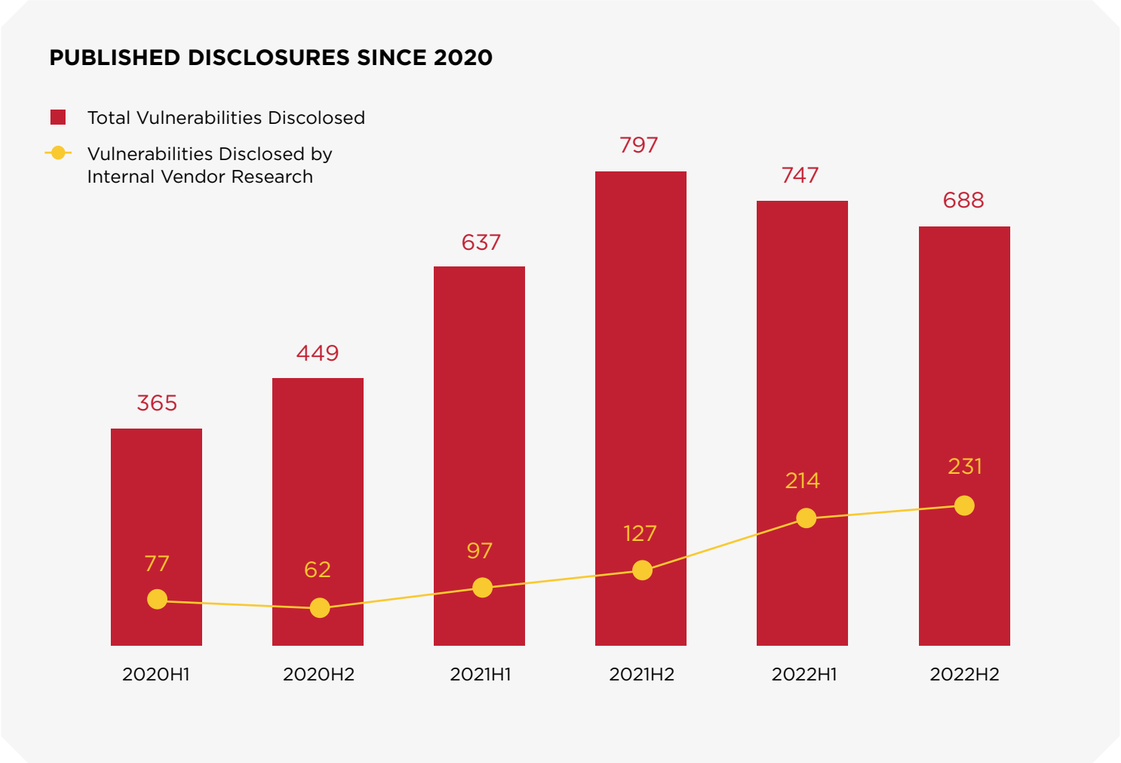
We have not only found and privately disclosed more than 400 vulnerabilities since our inception, but we've worked closely with many of the affected vendors in conveying the urgency of securing their products—and equally importantly, improving the maturity of product security teams and processes.

While vendors such as Rockwell Automation, Siemens, Schneider Electric and others in the automation space have the resources to formalize the intake of vulnerability disclosures, rapidly triage these reports, and improve the safety of customer environments, many other companies lag behind. It's not uncommon for researchers to run into vendors that have yet to establish a product security page on their websites that includes a secure contact email address and a public PGP key to ensure the secure transfer of vulnerability information.

Happily, we can say today, however, that things are beginning to trend in the right direction.

In this edition of the *State of XIoT Security Report, 2H 2022*, you'll see evidence that vendors are embracing the need to secure cyber-physical systems, and dedicating time, people, and money to not only patching software and firmware vulnerabilities, but also product security teams overall.

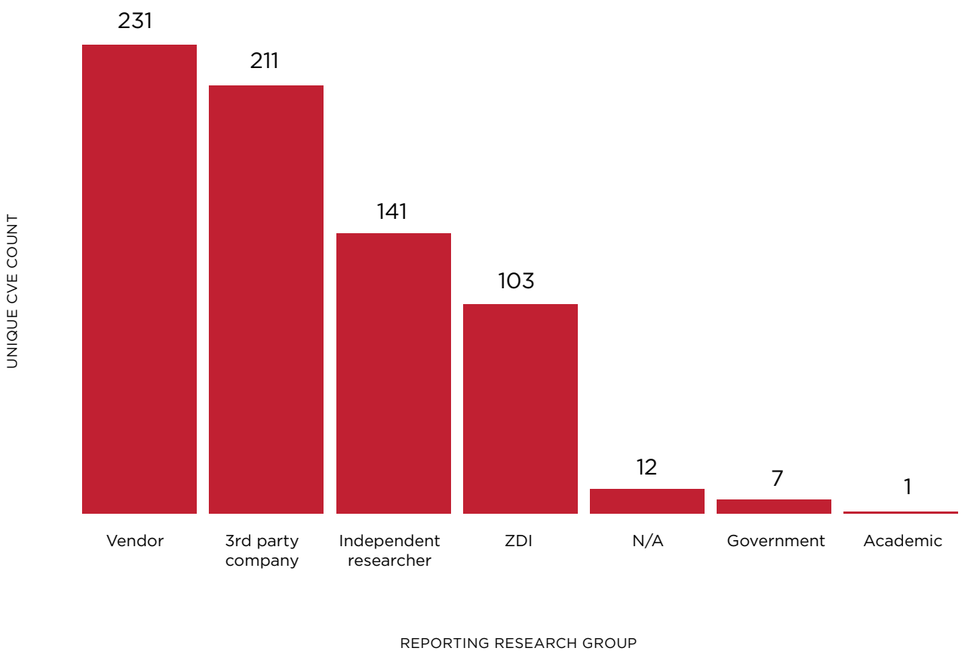
For the second consecutive report, the number of vulnerabilities affecting the Extended Internet of Things (XIoT) has dropped. After hitting a peak during the second half of 2021, we're seeing published vulnerabilities dipping while in parallel, the number of disclosures attributed to internal research and product security teams continue to climb.



In fact, for the first time, the number of published vulnerabilities attributed to vendor self-disclosures topped the numbers attributed to third-party companies.

Have researchers and vendors found all the low-hanging fruit as it relates to vulnerabilities in OT and IoT? Hardly. Our last three reports include the top three totals of published disclosures since our analyses began in 2020. But we are seeing the fruits of vendors' and researchers' labor in the steadily growing number of disclosures sourced to internal research and product security teams.

RESEARCH GROUP



From a researcher's perspective, we believe coordinated disclosures ensure that vendors are more security-aware than prior to being informed of a security issue in their product. Team82's 400-plus vulnerability disclosures track across more than 50 vendors. Three-quarters of those vendors have publicly available secure email addresses and public PGP keys. Nearly half have established product security websites where contact details and other useful information is available. The real revelation is that Team82 has tracked 11 vendors who initiated these activities after a successful coordinated disclosure with us.

All of this matters because cyber-physical systems deliver the services and things that enable our way of life. The food we eat, the water we drink, the energy that heats our homes and powers our devices, all rely on computer code somewhere. These direct links to outcomes in the physical world are putting a harsher spotlight on cybersecurity than ever before.

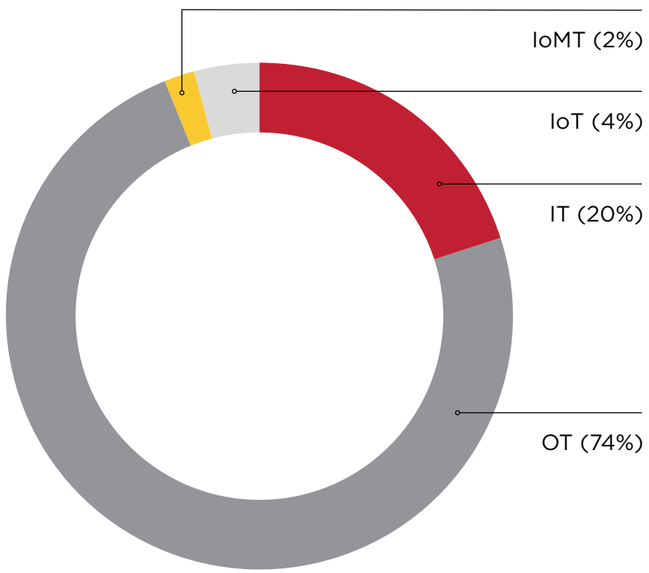
Look no further for more proof than healthcare, where politicians in the United States have recently equated secure cyber-physical systems with patient safety. For so long, cybersecurity in healthcare has almost exclusively equated to data privacy. Today, that's not enough. Hospitals and healthcare delivery organizations are connecting devices and systems online, increasing their attack surface. The ransomware epidemic, along with the COVID-19 pandemic, have been a one-two punch to the medical industry exploiting this hyperconnectivity of cyber-physical systems. This is a critical call to action to secure these systems—and others in critical infrastructure—because XIoT security matters.

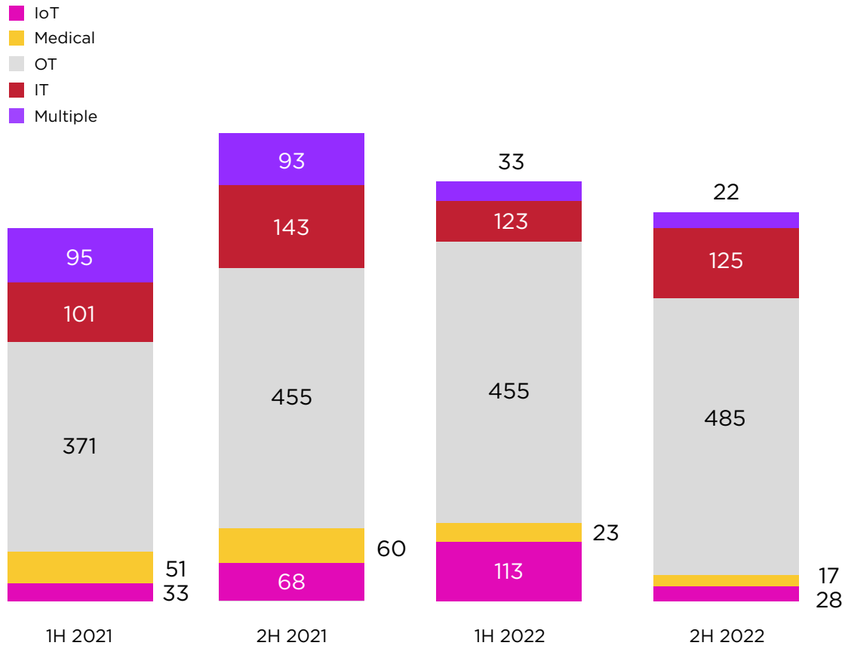
In this report, Team82 provides a contextual analysis of the vulnerabilities published during the second half of 2022. We'll look at the numbers in OT, IoT, and IoMT, what they mean, and provide insights on recommended actions that you can take within your enterprise.

Let's look at some of the other dominant trends we uncovered affecting the 2H 2022:

TRENDS

Vulnerabilities Breakdown





Published IoT and IoMT vulnerabilities in our dataset accounted for 6% of disclosures, while flaws in OT and IT-related ICS equipment accounted for 94% of published vulnerabilities in 2H 2022.

After a slight spike in published IoT vulnerabilities reported during the first half of 2022, that number has dropped back down closer to previous levels. Published vulnerabilities affecting OT continue to dominate over IoT and IoMT.

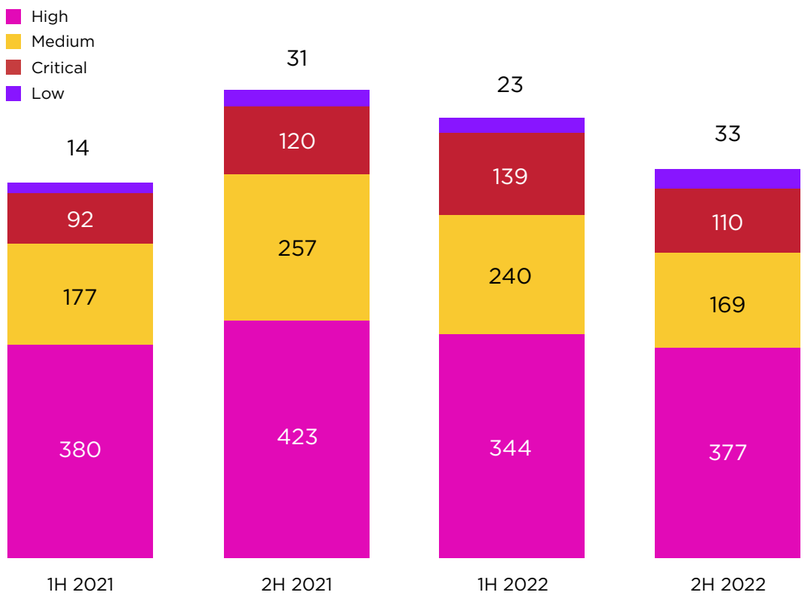
How Many, and How Critical?

During the 2H 2022, there were **688** published vulnerabilities impacting **72** industrial, healthcare, and commercial technology vendors. These overall numbers also dropped from the 1H 2022, which were 747 and 86, respectively but in the meantime, the number of OT flaws grew in the 2H 2022.

On average, there were 115 vulnerability disclosures per month during the 2H 2022. While we're seeing overall numbers trend downward, there are still a significant number of vulnerabilities being found by vendors, professional research teams, and independent researchers.

Of the 688 published vulnerabilities in 2H 2022, 487 were either assessed a critical or high-severity CVSS v3 score. There were 110 critical vulnerabilities in the second half of 2022.

VULNERABILITY SEVERITY CHANGES SINCE 2020



GLOSSARY

The State of XIoT Security Report 2H 2022 introduces a number of terms that aren't necessarily part of the day-to-day computing lexicon. We'd like to provide a snapshot of some of the important terms and concepts that shape this report.

Building Management System (BMS): Centralized computing systems that manage and regulate environmental systems such as HVAC, as well as lighting, elevators, power, and more.

Digital Imaging and Communications in Medicine (DICOM): A standardized communication protocol used in the transmission of medical images and data over the network. DICOM is the standard for many vendors' MRI and PACS systems. The standard defines how objects are encrypted in transmission.

Distributed Control System (DCS): Complex systems designed to control large industrial processes, comprising multiple controllers, I/O devices, and human-machine interfaces (HMIs). These systems are usually used in large plants, where high availability and continuous operations are required.

Extended Internet of Things (XIoT): An umbrella term encompassing cyber-physical systems connected to the internet, including devices in industrial (OT and ICS devices), healthcare (connected medical devices), and commercial environments (building management systems and enterprise IoT).

Historian: A database housing process information used for process analysis that interfaces with centralized management systems.

Human Machine Interface (HMI): An application that visualizes industrial automation processes and allows interactions between operators and controllers.

Industrial control systems (ICS): Systems and instrumentation used to operate and automate industrial processes.

Internet of Medical Things (IoMT): Connected devices and applications critical to medical and healthcare information technology.

Internet of Things (IoT): A complex network of physical things, from household automation systems to complex industrial machines, that contain embedded computers that share data over the internet.

IT/OT Convergence: A merger of information technology and operational technology OT management that integrates enterprise data systems with tools used for process control.

Operational Technology: Firmware and software that monitors physical devices critical to automation processes.

Patient Monitoring System: Devices used to monitor patients' vital signs, and alert on any changes that may indicate harm to a person's wellbeing. These systems share information with a centralized distributed monitoring system that can be accessed remotely by healthcare professionals.

Programmable Logic Controllers (PLC): A programmable controller used to automate processes, machine functions, and production lines by acting on inputs and outputs within manufacturing processes.

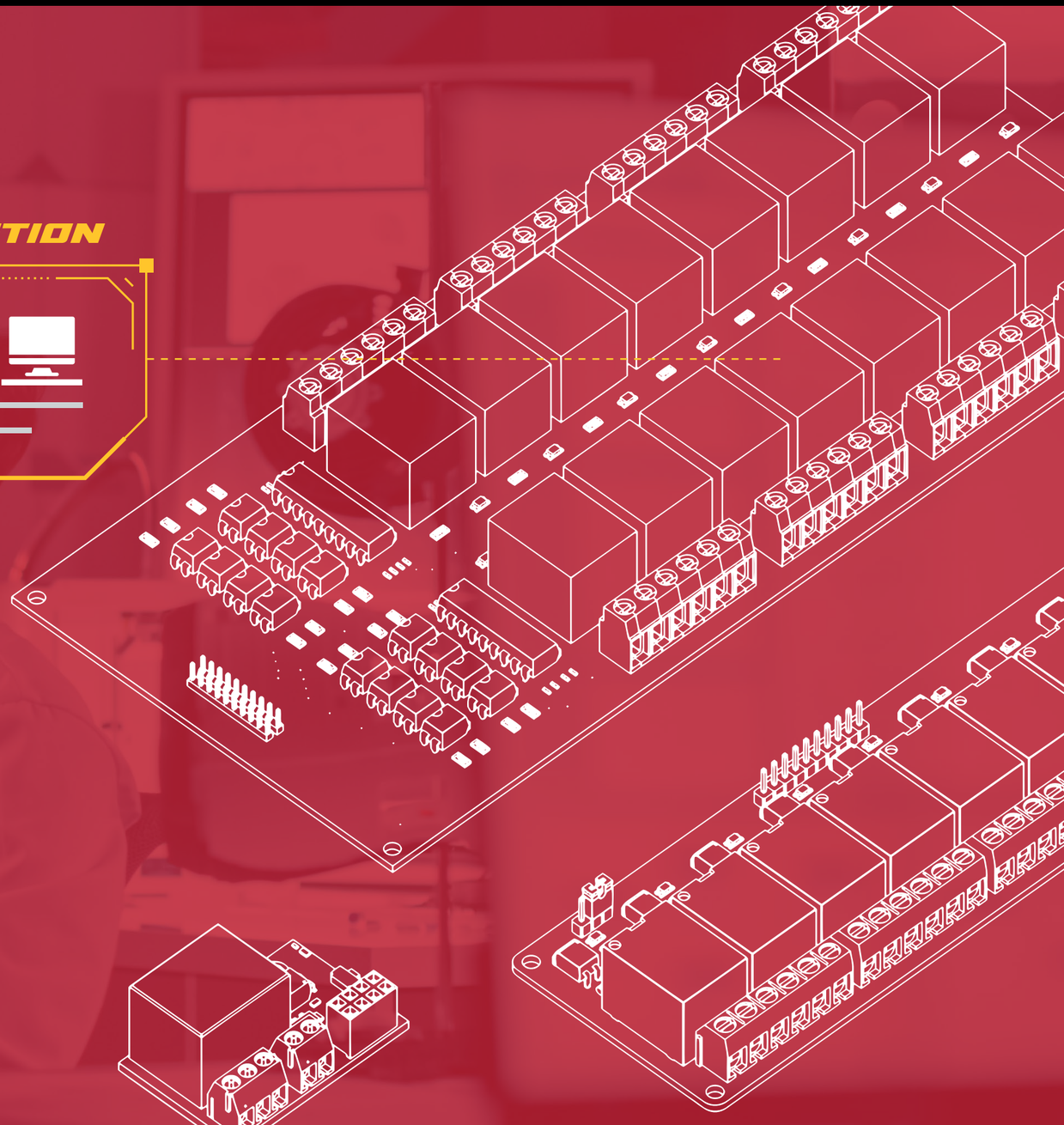
Remote Terminal Unit (RTU): An industrial field device that transmits telemetry from field devices to a SCADA or DCS.

Store and Forward: A healthcare service where patient clinical information is stored and sent electronically to remote sites for evaluation.

Supervisory Control and Data Acquisition (SCADA): SCADA systems provide control at the supervisory level of the Purdue Model, and process and transmit data from field devices to the OT network.

TEAM82

Assessment of 2H 2022 disclosures from Claroty Team82

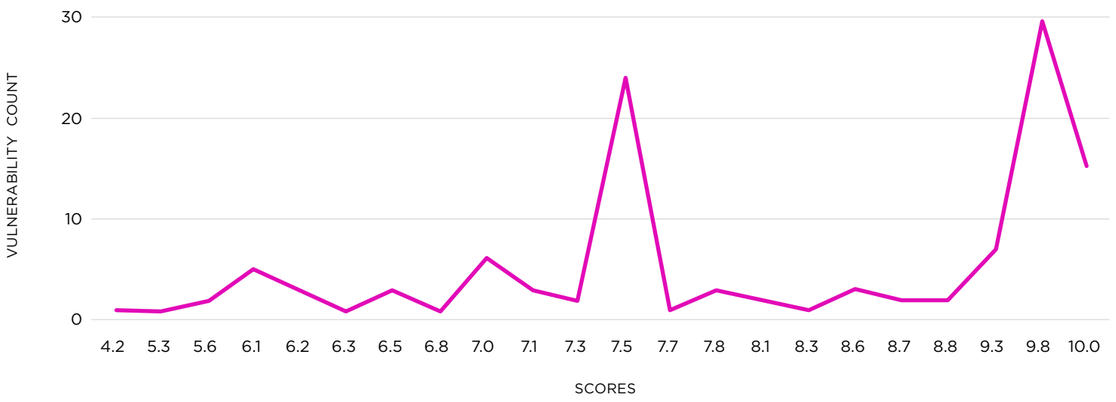


ASSESSMENT OF 2H 2022 DISCLOSURES FROM CLAROTY TEAM82

Team82 coordinated disclosures in 2022 resulted in the publication of details and remediation of 117 vulnerabilities, most of which were either assessed a critical or high-severity CVSS v3 score. Here, you can see that most of Team82's published vulnerabilities were assessed a score of 7.5 or higher, and close to half are 9.5 or higher.

While automation dominates Team82's 2H 2022 dataset of affected vendors, there are a growing number of IT and IoT vendors that entered into coordinated disclosures with Team82, and mitigated serious vulnerabilities as a result of that engagement.

SEVERITY OF TEAM82 DISCLOSURES



DISCLOSURE NUMBERS

404
Vulnerabilities disclosed since 2018

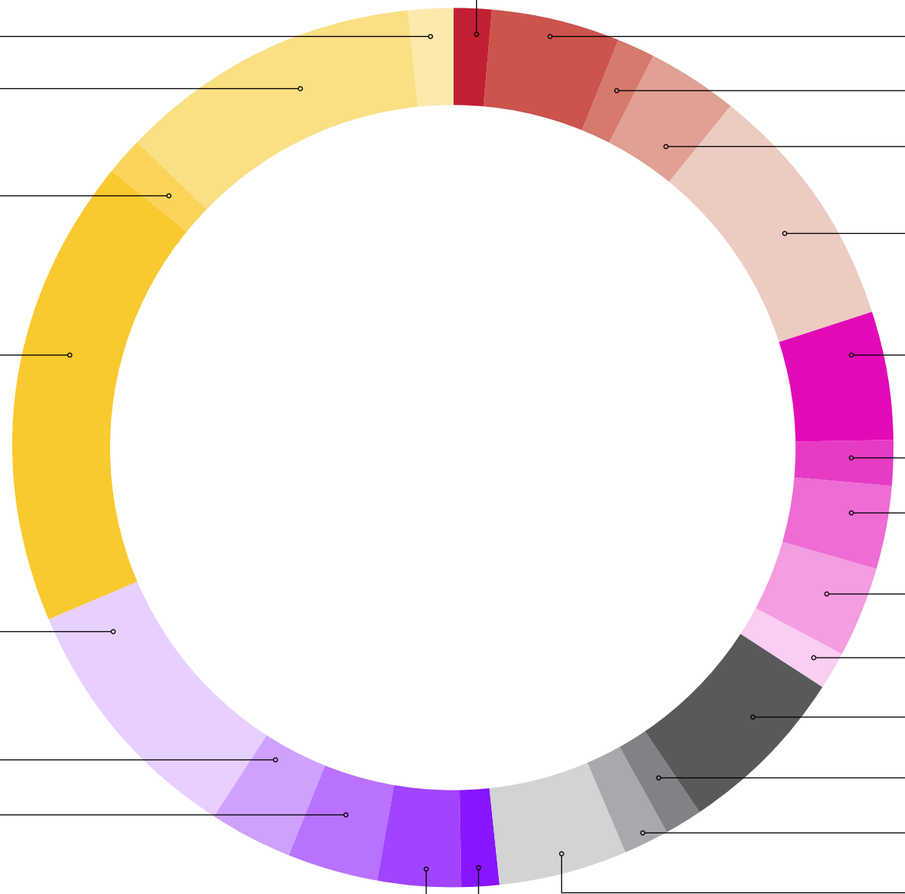
57
Affected Vendors

11
Vendors who initiated vulnerability disclosure programs or activities after a Team82 disclosure

65
Team82 disclosures in the 2H 2022

117
Total 2022 Team82 disclosures

2H 2022 AFFECTED VENDORS



Key Event: The ABCs of Securing PLCs

Team82 emphasized through a number of research endeavors in 2022 the importance of programmable logic controllers to industrial automation, and how vulnerabilities in the way they're programmed or implemented can impact processes and put safety and reliability in jeopardy. Here's a quick recap of Team82's recent PLC-related research:

HIDING CODE ON ROCKWELL PLCS:

Vulnerabilities in Rockwell Automation Logix PLCs and Studio 5000 engineering workstation applications could allow attackers to download modified code to a controller, and at the same time hide the attack from an engineering workstation. Team82 found two vulnerabilities that allowed it to decouple textual code from binary code and transfer it to the PLC, while modifying one and not the other. The end result of exploiting both vulnerabilities is the same: The engineer believes that benign code is running on the PLC; meanwhile, completely different and potentially malicious code is being executed on the PLC. Rockwell Automation released a tool to its users that detects this type of modification.

Read more >

EVIL PLC ATTACK:

This novel attack weaponizes programmable logic controllers in order to install malicious code on engineering workstations connecting to compromised PLCs. Malicious code is uploaded from the PLC to the EWS, which then would execute on other PLCs an engineer connects to. Engineering workstations are crucial crossover points between OT and corporate networks; an attacker able to execute code on an engineer's machine could rapidly compromise many systems and move laterally across either network. Products from seven leading automation vendors were vulnerable to the Evil PLC attack.

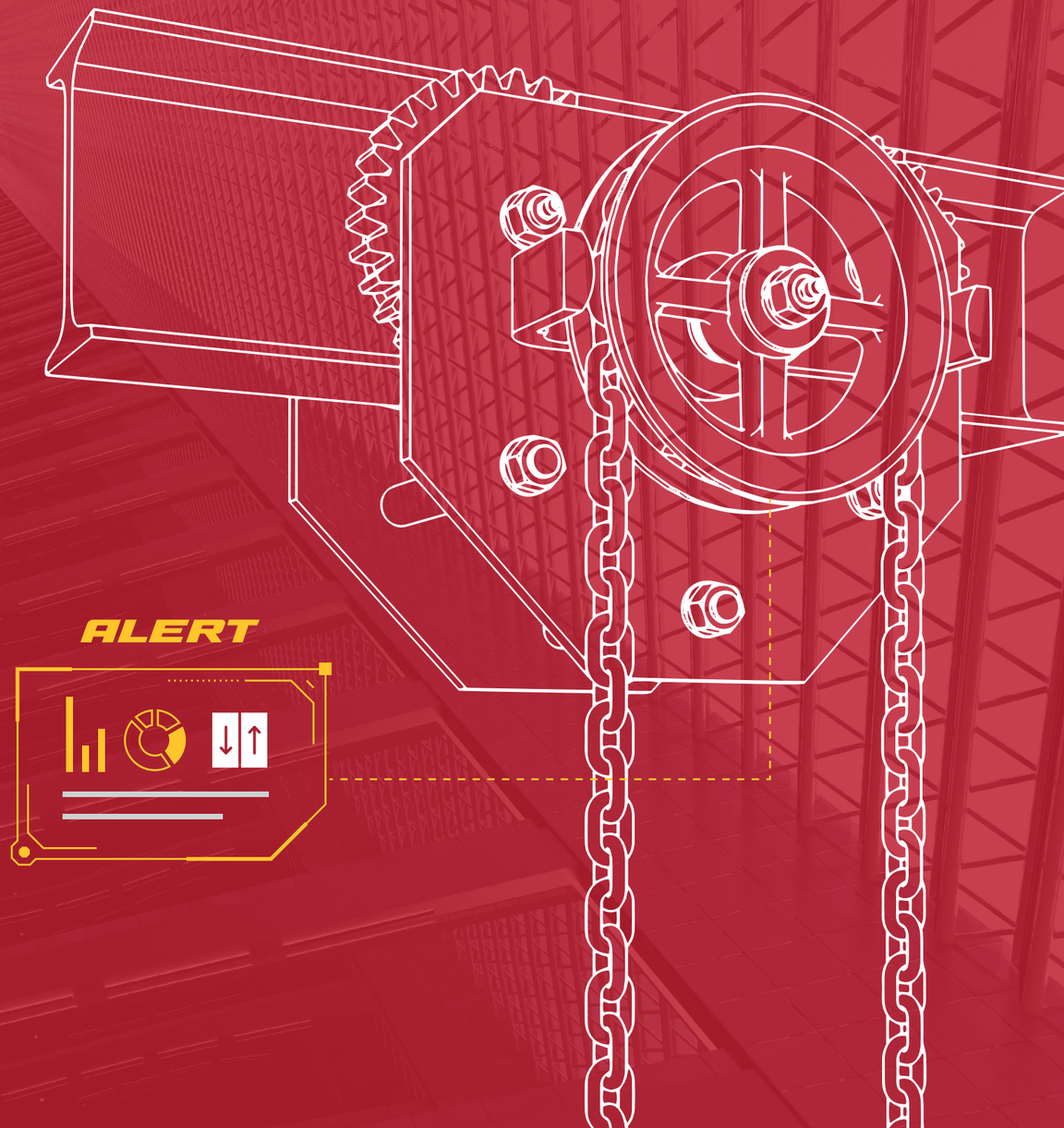
Read more >

UNCOVERING HARDCODED KEYS ON SIEMENS PLCS:

Team82 developed a method by which it could extract heavily guarded and hardcoded encryption keys embedded in Siemens SIMATIC PLCs and TIA Portal. An attacker in possession of these secret keys could execute a number of advanced attacks against any SIMATIC 1200/1500 PLC since they all shared the same key. Team82's private disclosure with Siemens resulted in a new TLS management system in TIA Portal ensuring the confidentiality of communications between Siemens PLCs and the engineering workstations. Siemens also introduced a preactivated PLC configuration password requirement, that ensures all confidential PLC configuration data are protected by default as well as predefined secure PG/HMI communication.

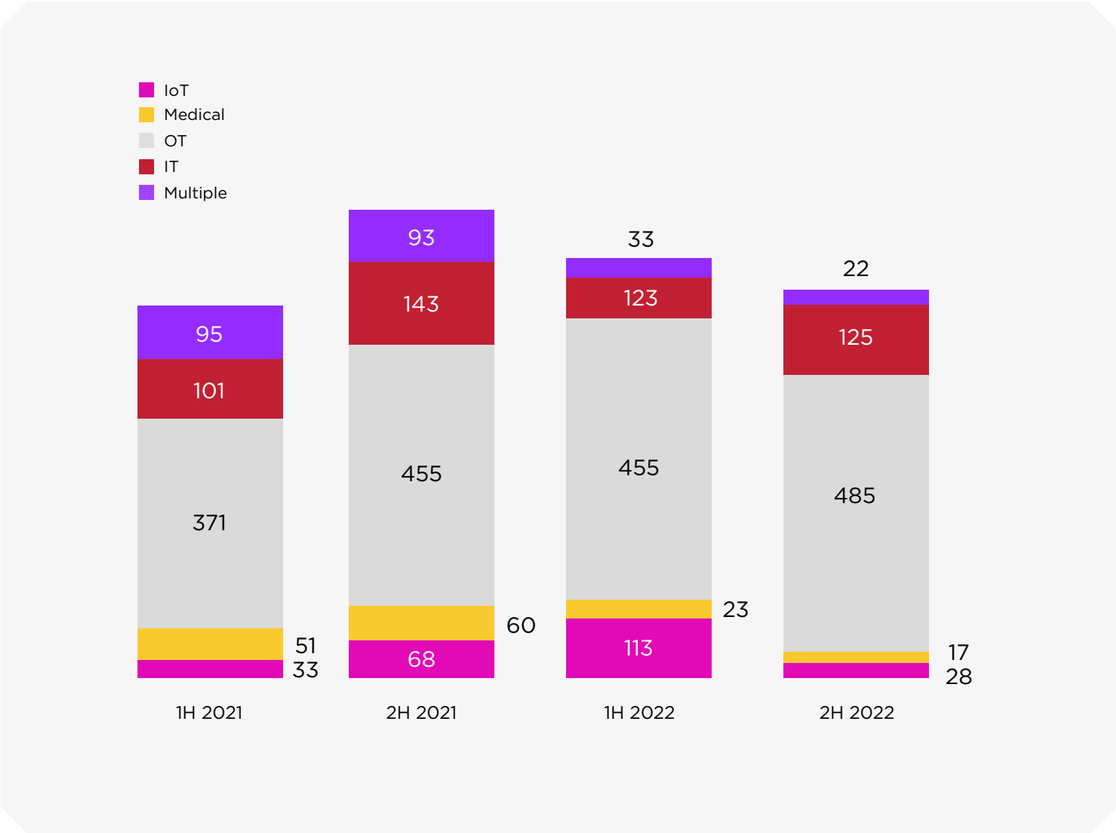
Read more >

XIoT VULNERABILITIES ASSESSMENT



ASSESSMENT OF XIOT VULNERABILITIES DISCLOSED IN 2H 2022

In the 2H 2022, we had a record number of 485 published OT vulnerabilities in our dataset, topping the previous high of 455 in the 2H of 2021 and in 1H 2022. The number of published IoT and IoMT vulnerabilities, however, dropped significantly from a combined 136 in the 1H 2022 to 45 in this report.



DISCLOSURE BY THE NUMBERS

688

Published XIoT vulnerabilities in 2H 2022

72

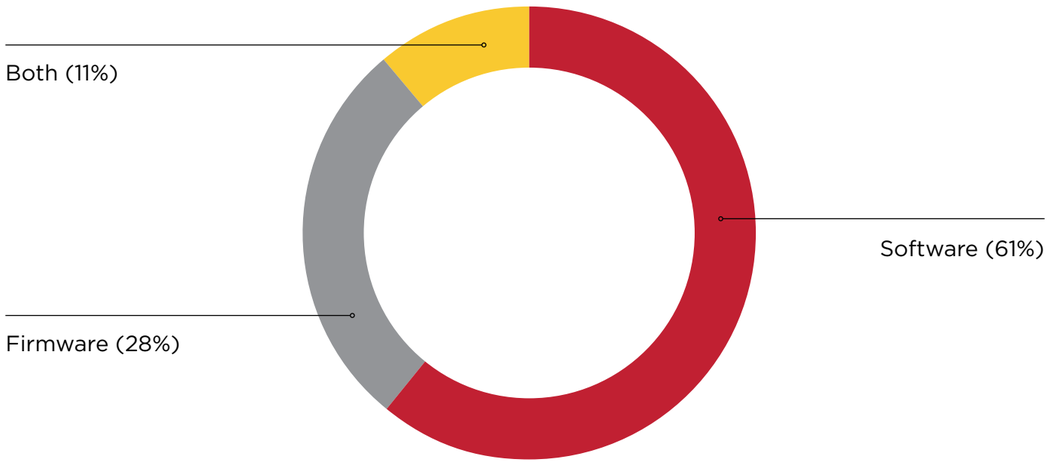
Affected Vendors in 2H 2022

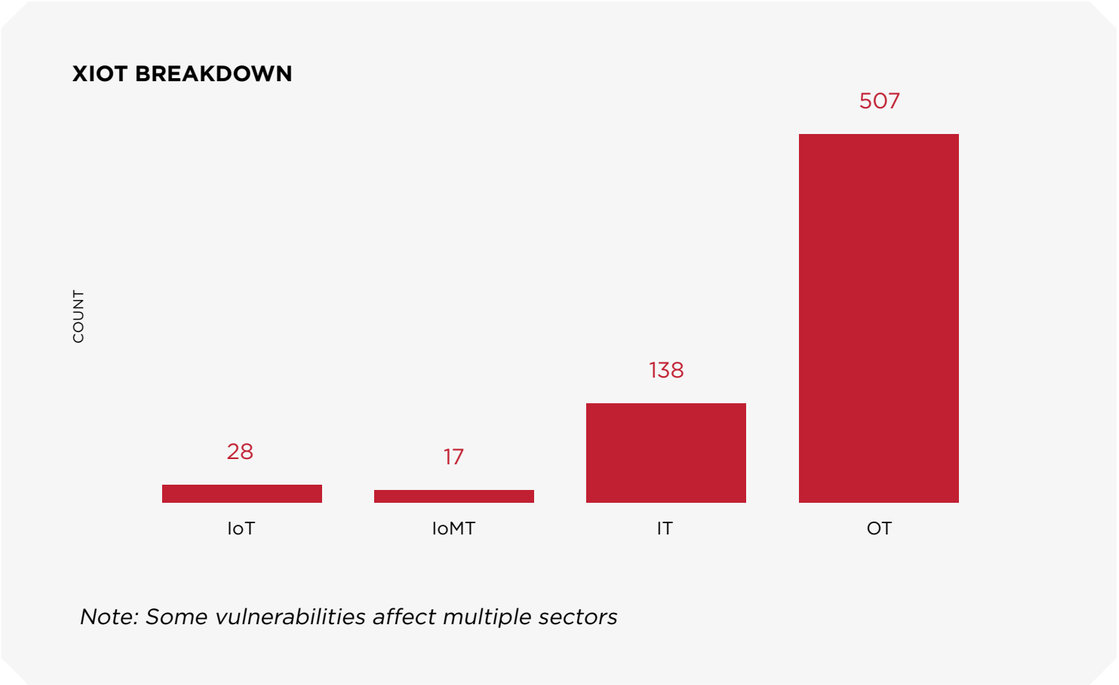
Affected XIoT Components: Software and Firmware

In the 1H of 2022, the numbers of published software and firmware vulnerabilities were almost on par with one another: 47.3% percent of disclosed vulnerabilities involved OT, IoT, or IoMT software flaws, while 46.7 were firmware-related.

In the 2H of 2022, we've reverted back to a significant number of software vulnerabilities dominating our dataset. In the past, researchers and vendors have cited challenges in researching and remediating firmware vulnerabilities; software updates are often prioritized over firmware updates given the comparative ease to test and distribute software patches.

In 2H 2022, the percentage of published software-based vulnerabilities dominates firmware.

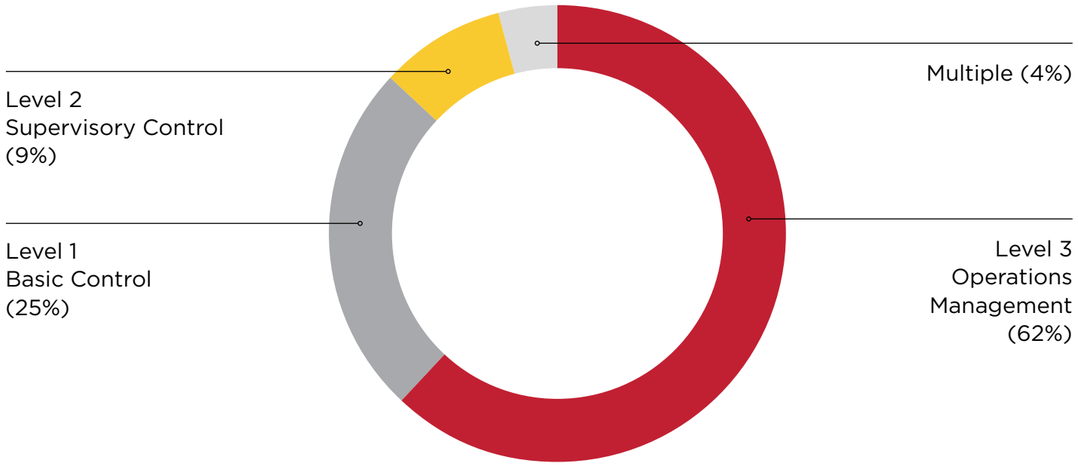




Published vulnerabilities in OT—and IT-related OT—dominate the 2H 2022 dataset.

Looking closer at the 507 published OT vulnerabilities in the 2H 2022, we see a continuing trend of a large majority of those security issues uncovered at Level 3 of the Purdue Model for ICS, the operations management level. At this level of the Purdue reference model we find devices that manage production workflows, including devices such as Historian servers and databases that collect and store process information and relay it to field devices at Levels 2 and 1, as well as the DMZ. Some of these devices, including Historian servers, can be key crossover points between the IT and OT networks, and very attractive to threat actors wishing to intercede in plant operations, for example.

In the 2H 2022, we see that 62% of published OT vulnerabilities affect Level 3, while a quarter of published vulnerabilities impact Level 1, or Basic Control devices, including PLCs and other controllers and sensors. Software-based vulnerabilities have traditionally dominated our dataset and this continues to be the case. Code-scanning tools and techniques are mature in the software security space, and are generally much easier to find for research teams and product security operations. Vendors are also quicker to update software vulnerabilities than those found in firmware.



Exploits at Levels 2 and 1 are a mix of software- and firmware-based and can allow an attacker to reach lower levels and affect the process itself, making them also an attractive, but much more difficult target to reach.

With the inability to patch over time, especially in Level 1 device firmware, it is recommended to invest in segmentation, remote access protection, and protection of the Supervisory Control level because of its links to the Basic Control level.

Key Event: GAO Comes Down on IoT/OT Insecurity within Critical Infrastructure

A U.S. Government Accountability Office report published in December scolded sector risk management agencies (SRMA) responsible for interfacing with relevant public-sector agencies and the private sector on policy development, incident management, and technical support.

The GAO report noted that while cybersecurity practices around IoT and OT devices have been implemented across the 16 critical infrastructure sectors, the SRMAs have yet to develop metrics to measure the effectiveness of those practices, nor have they conducted sector-wide risk assessments of IoT and OT environments.

While the government is careful to measure and publish statistics on key economic indicators (housing, unemployment, etc.), it has yet to do so for the security of devices that are increasingly core elements of public safety, patient care, and the continuity of key services.

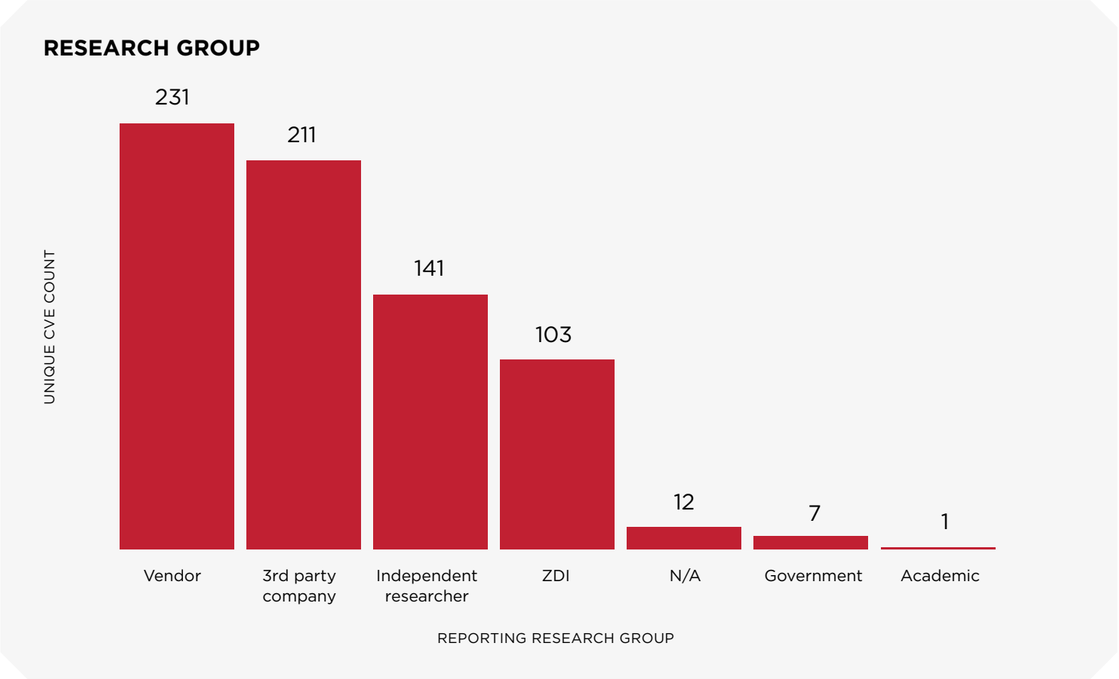
Until metrics are developed and instituted and sector-wide risk assessments that include IoT and OT happen, any investments in technology and subsequent mitigations may not be adequate to combat the true risks CI entities are facing.

Read more >

Origins of XIoT Vulnerability Discoveries

As we mentioned in the Introduction of this report, vendors are investing time, money, and people into finding and fixing vulnerabilities affecting cyber-physical systems.

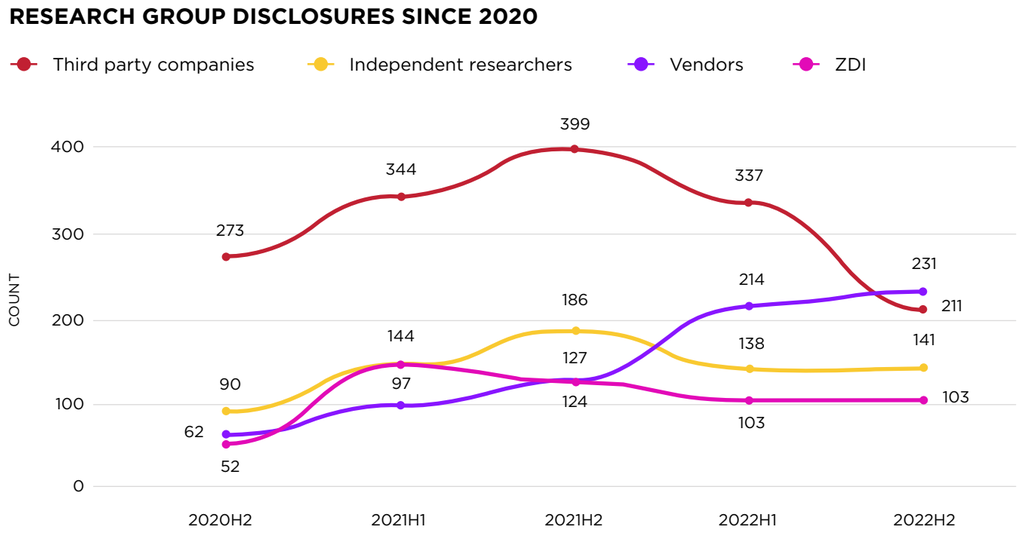
For the first time, more published vulnerabilities were attributed to vendors' product security teams than to third-party companies.



We can see here over time the changes in the numbers of published disclosures attributed to different research groups, and how in the 2H 2022 for the first time, vendors have overtaken third-parties.

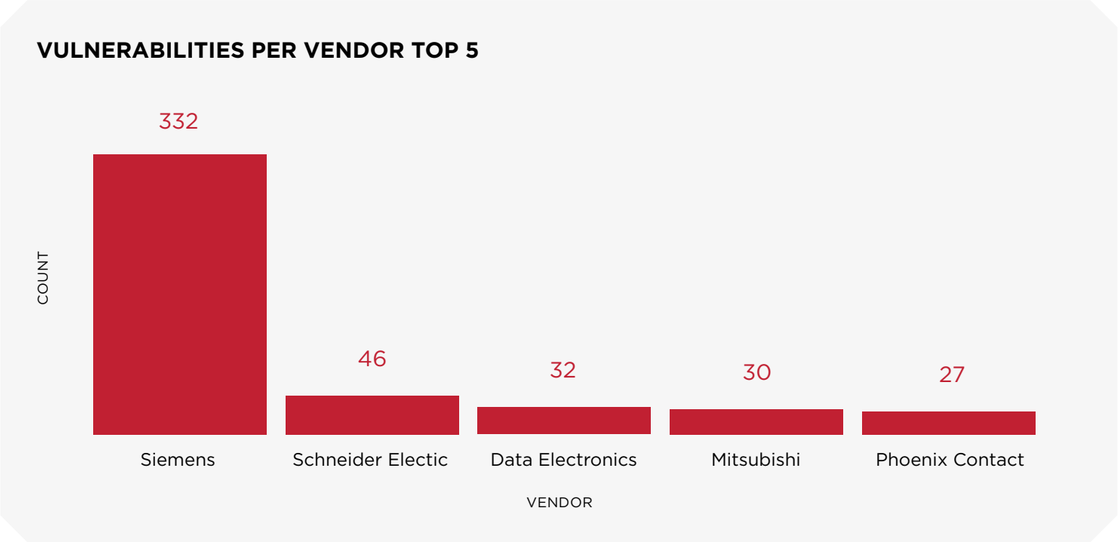
There has been a sharp increase since 2020 in vendor self-disclosures, which could be an indication that cyber-physical systems security is being prioritized by automation companies, IoT, and medical device makers.

The fact that more vendors are looking for, and finding, more vulnerabilities in their own products leads to a safer ecosystem for users in critical industries. There is also a trickle-down of security being built in natively as new products are developed, tested, and sent out into the market. These numbers may also correlate to the drop in external researchers finding vulnerabilities; the drop in the number of published vulnerabilities attributed to independent researchers could also be an offshoot of the weakening global economy. Research isn't necessarily a revenue-generating operation, and white-hats may prioritize other areas in a lagging economy.



While the number of affected vendors dropped from the 1H 2022 report from 86 to 72, the aggregate number of affected vendors for 2022 vendors did surpass the total for 2021.

Team82's dataset is dominated by automation vendors, but noteworthy is the ascension of Delta Electronics, a smart energy solution provider, and Phoenix Contact, a connection technology company, into the top 10.



72

Affected vendors in 2H 2022

158

2022 Total affected vendors, up from 147 in 2021

We should point out that a significant number of disclosed vulnerabilities for any one vendor is not a reflection of its product security or ability to scrutinize for vulnerabilities.

The opposite is likely true

- Market-leading vendors allocate ample resources to product security
- Our numbers indicate they're finding more vulnerabilities than ever before
- The age, catalog, and install base of each vendor influences the number of disclosed vulnerabilities affecting products.

Six XIoT vendors experienced first-time published disclosures in the 2H 2022; the list of first-timers is a mix of industrial and IoT vendors, primarily.

VENDORS	PRIMARY INDUSTRY
Dataprobe	IT Technology
Kingspan	Building Automation
LS ELECTRIC	Automation
MZ Automation GmbH	Automation
MiCODUS	IoT
Sequi Inc.	Industrial Security Products

Key Event: Discontinued Boa Web Server Vulnerability

Microsoft reported in November that its investigation of an electric grid intrusion first reported by Recorded Future earlier this year had a common link among affected IP addresses: the open source Boa web server, which had been discontinued in 2005.

Despite no longer being maintained, Boa is still used by IoT device vendors and in software development kits (SDKs) as a means of accessing settings consoles and sign-in prompts. Vulnerable components in the web server. Microsoft said that IP addresses affected in the attacks against portions of India's electric grid were running Boa, and many of those were IoT devices such as routers. Two vulnerabilities were uncovered allowing attackers to access files and leak other sensitive data.

The incident sheds harsh light on the security of the software supply chain. Not only are open source components often vulnerable despite being widely used across industries, but their presence is often unknown to vendors using popular SDKs, for example, and while IoT devices' patch levels may be current, the same may not be true for third-party components.

IMPACT

Impact

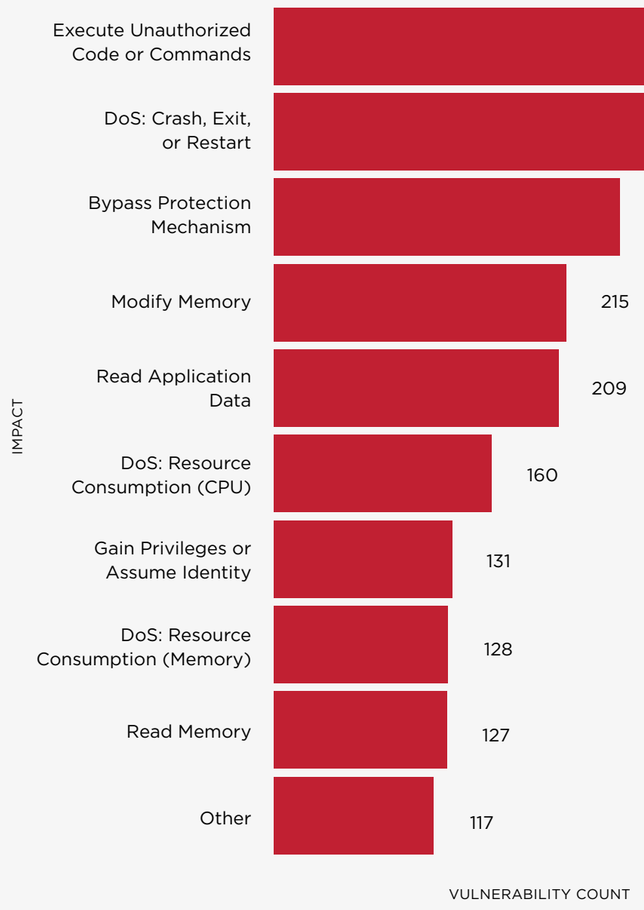
Users largely rely on two frameworks when prioritizing vulnerability remediation:

CVSS: The Common Vulnerability Scoring System is a scoring framework used to illustrate the severity and characteristics of vulnerabilities.

CWE: The Common Weakness Enumeration is a specification used to describe the cause of software and firmware vulnerabilities.

TOP 10 IMPACTS OF PUBLISHED VULNERABILITIES

There are three legs to the security model that are most applicable to XIoT devices: availability, integrity, and reliability/safety. The numbers of published vulnerabilities by impacts here affect all three areas, with the most prevalent—and severe—being the execution or unauthorized code and system crashes or restarts that could negatively affect availability and user safety.



ATTACK VECTOR DISTRIBUTION

63%
Published vulnerabilities exploitable **over the network**

30%
Published vulnerabilities that require **local access** for exploitability

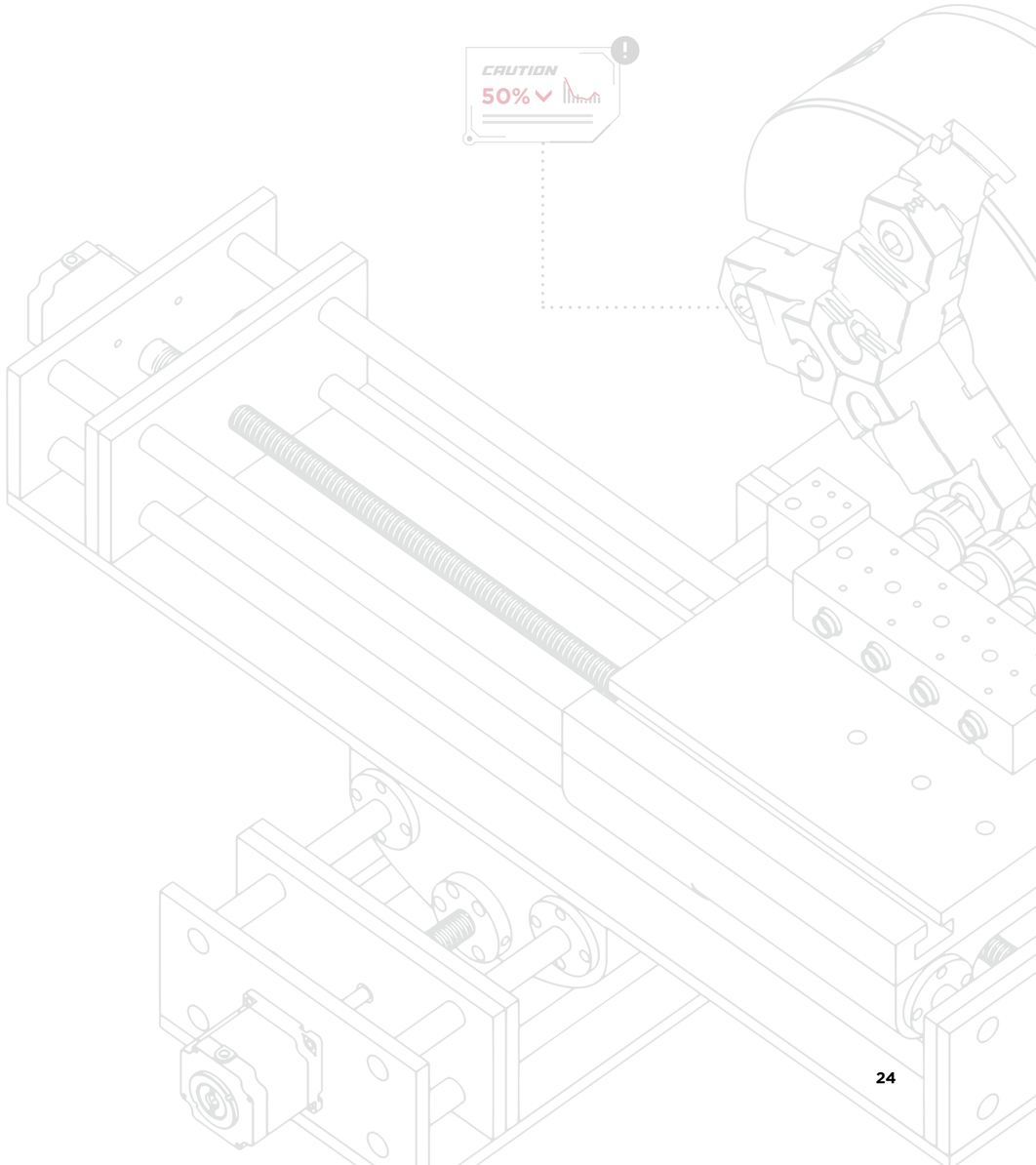
6%
Published vulnerabilities that are **adjacent**

1%
Published vulnerabilities that require **physical access** for exploitability

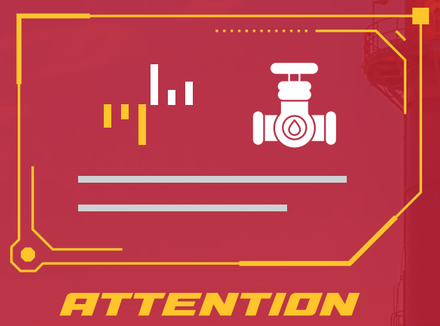
The top five most prevalent CWEs from Team82's dataset are also prominent on MITRE Corp.'s 2022 CWE Top 25 Most Dangerous Software Weaknesses list. These vulnerabilities can be relatively simple to exploit and enable adversaries to disrupt system availability and service delivery

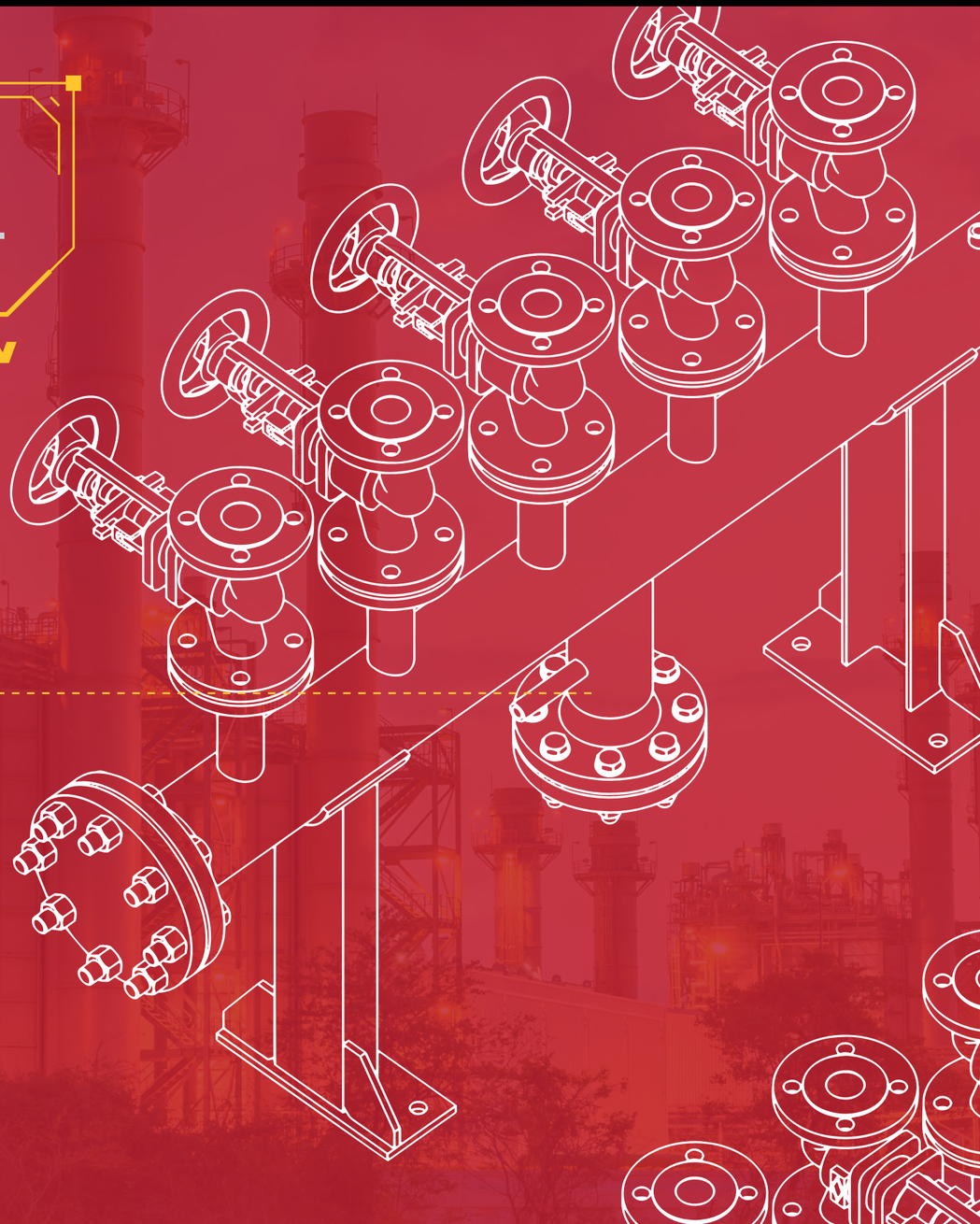
1. **CWE-787: Out-of-Bounds Write (75 published vulnerabilities in 2H 2022); No. 1 on the CWE Top 25**
2. **CWE-125: Out-of-Bounds Read (43 published vulnerabilities in 2H 2022); No. 5 on the CWE Top 25**
3. **CWE-79: Improper Neutralization of Input During Web Page Generation (39 published vulnerabilities in 2H 2022); No. 2 on the CWE Top 25**
4. **CWE-20: Improper Input Validation (36 published vulnerabilities in 2H 2022); No. 4 on the CWE Top 25**
5. **CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (27 published vulnerabilities in 2H 2022); No. 8 on the CWE Top 25**

Simple coding errors such as input validation, buffer-related memory vulnerabilities, and SQL injection continue to plague software development, and are reflected prominently in Team82's dataset and the MITRE list.



MITIGATIONS/ REMEDIATION





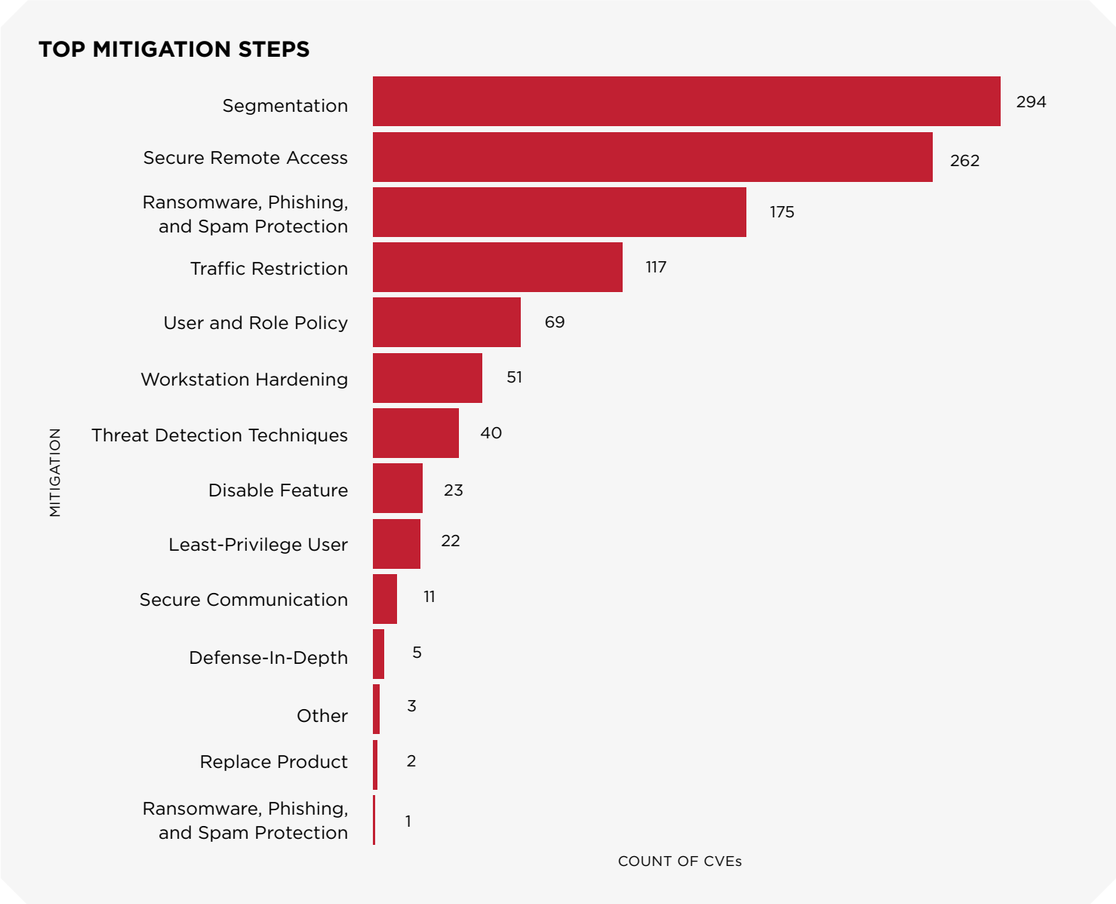
MITIGATIONS

Mitigations are often the only available remediation option given the software and firmware patching challenges we've described. In addition, many legacy ICS and medical devices may have end-of-life status and are no longer supported by the affected vendor, further placing a reliance on mitigations.

Yet despite defenders' dependence on mitigations, vendor advisories or alerts from industry groups such as ICS-CERT sometimes come up short with their defense-in-depth recommendations.

Actionable recommendations such as blocking specific ports or updating outdated protocols are important, but it should be noted that foundational practices must be in place before those recommendations are effective.

Network segmentation is an important control as air-gaps become a relic of the past and perimeters erode as enterprises move data, applications, infrastructure and services to the cloud.



Team82's data around the top mitigation steps bears this out, left. For example, network segmentation is the top step, and should be a top consideration for defenders ahead of other options on our list, including basic security hygiene such as ransomware awareness (phishing mitigations), traffic restriction, user- and role-based policies, and the principle of least privilege.

Segmentation would likely involve virtual zoning that allows for zone-specific policies that are tailored to engineering and other process-oriented functions, or alternatively separating between the public space and PHI servers in medical facilities.

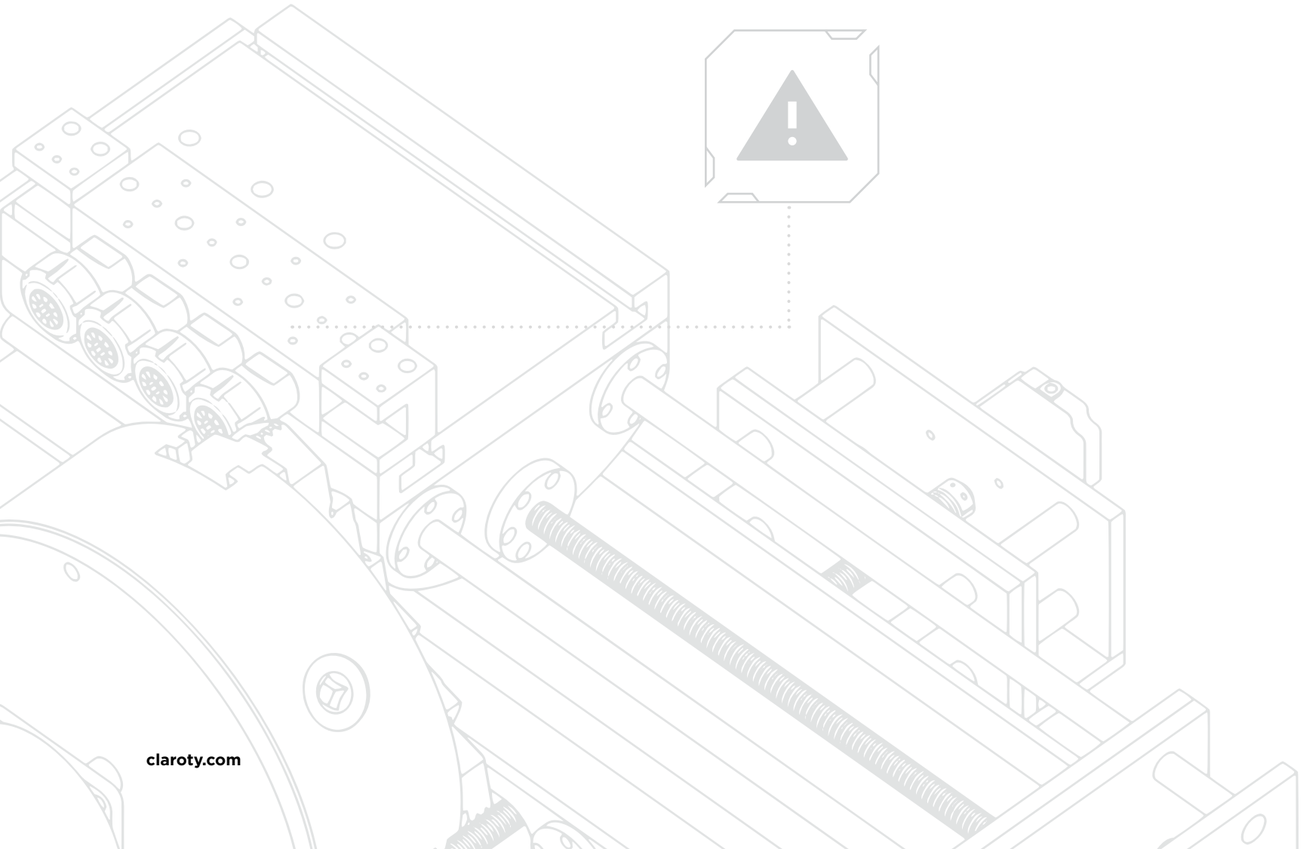
Segmentation goes hand-in-hand with secure remote access, the second most recommended mitigation. Secure remote access involves not only separating critical zones from the rest of the IT and OT networks, but also securing remote sessions through the addition of encryption, authentication, and authorization capabilities.

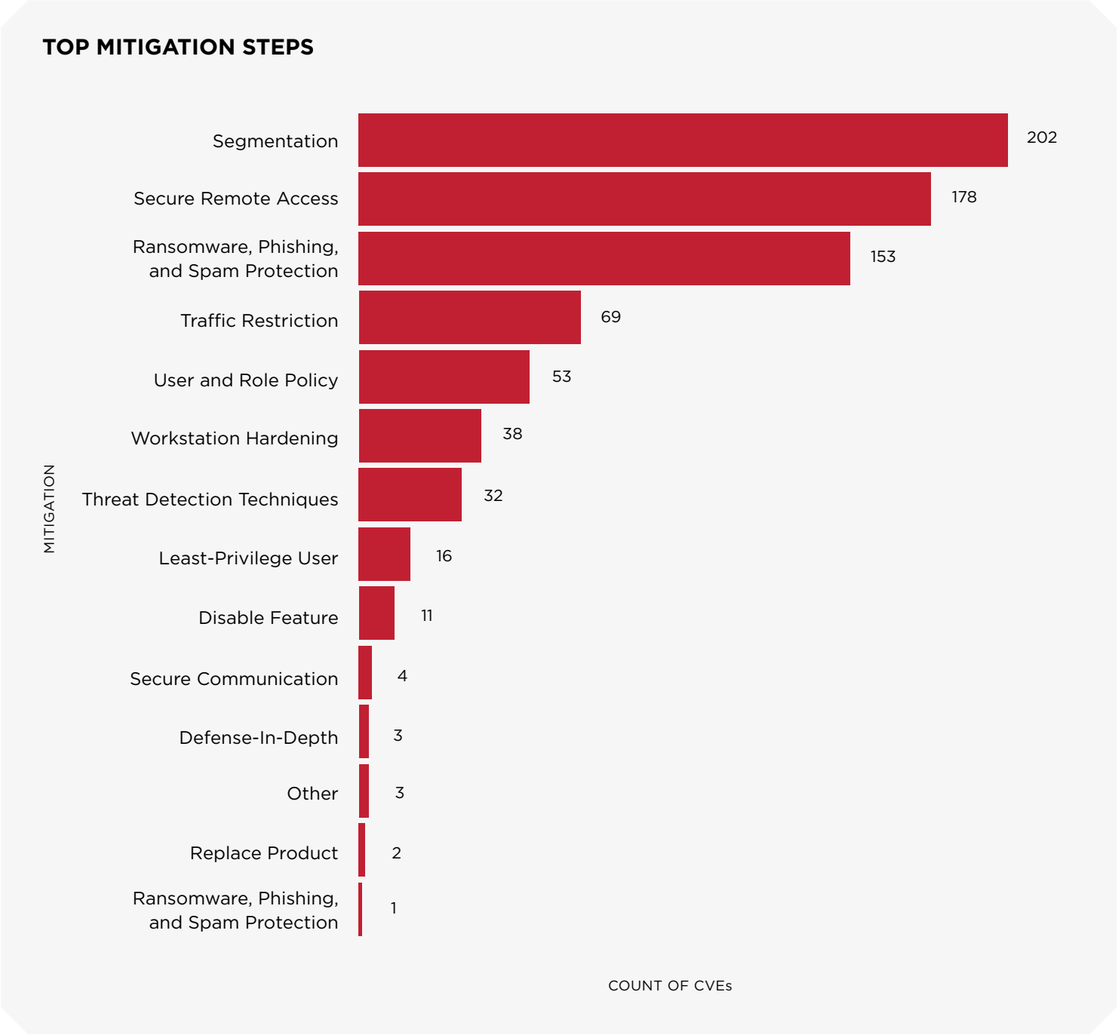
Mitigations Per XIoT Sector

OT

In OT, in addition to network segmentation, secure remote access, and ransomware protection, the other significant mitigation strategies published along with OT vulnerabilities were traffic restriction, user and role policy implementation, and workstation hardening.

Given the top CWEs that emerged in our 2H 2022 dataset around user input exploitation techniques, these additional mitigations restrict the roles of users and programs and help prevent arbitrary code execution.





IoT

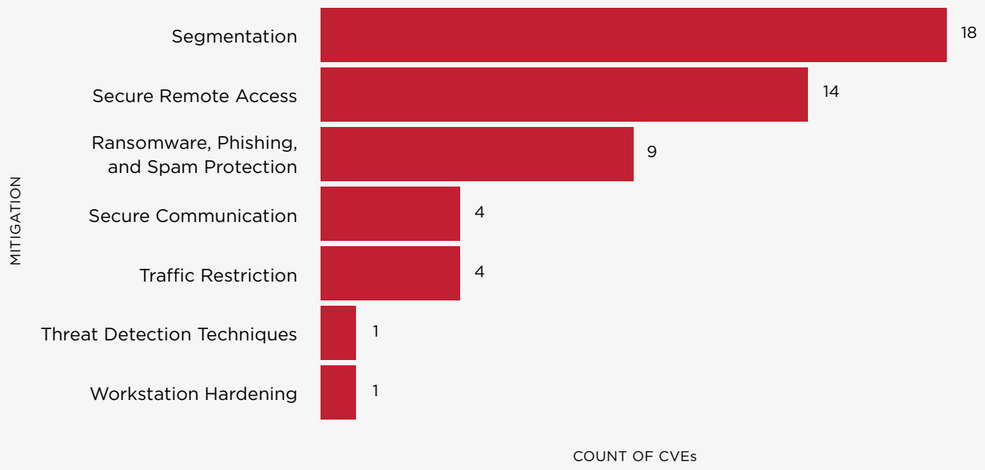
Most IoT devices are on the network, and this is an indication as to why vendors recommend mitigation techniques that could prevent network-based attacks, such as secure communication and traffic restriction, in addition to threat detection techniques and workstation hardening.

This also implies that IoT vendors are recommending organizations to use security and threat detection systems, which if done correctly will increase the overall security of their networks and devices.

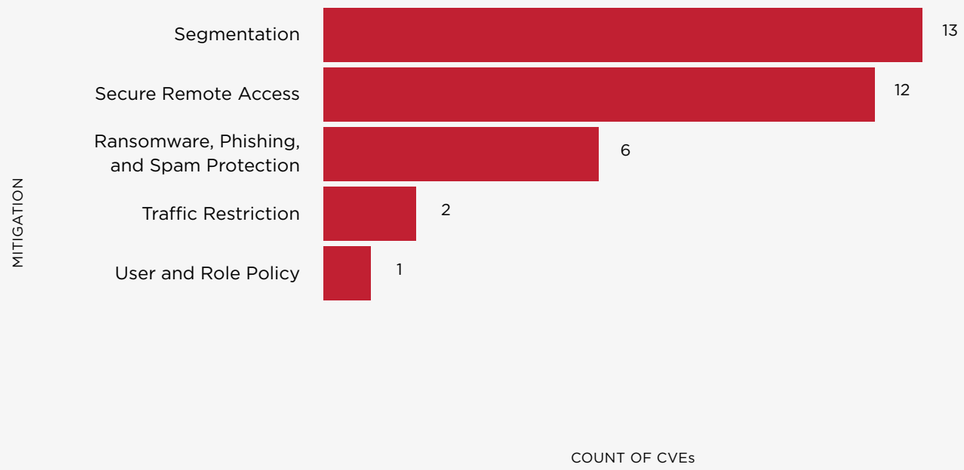
IoMT

Medical systems require high availability, therefore, adding external defensive measures such as threat detection and workstation hardening, is a good way to ensure device security, as well as preventing sensitive information being stolen by malicious actors.

TOP MITIGATION STEPS



TOP MITIGATION STEPS

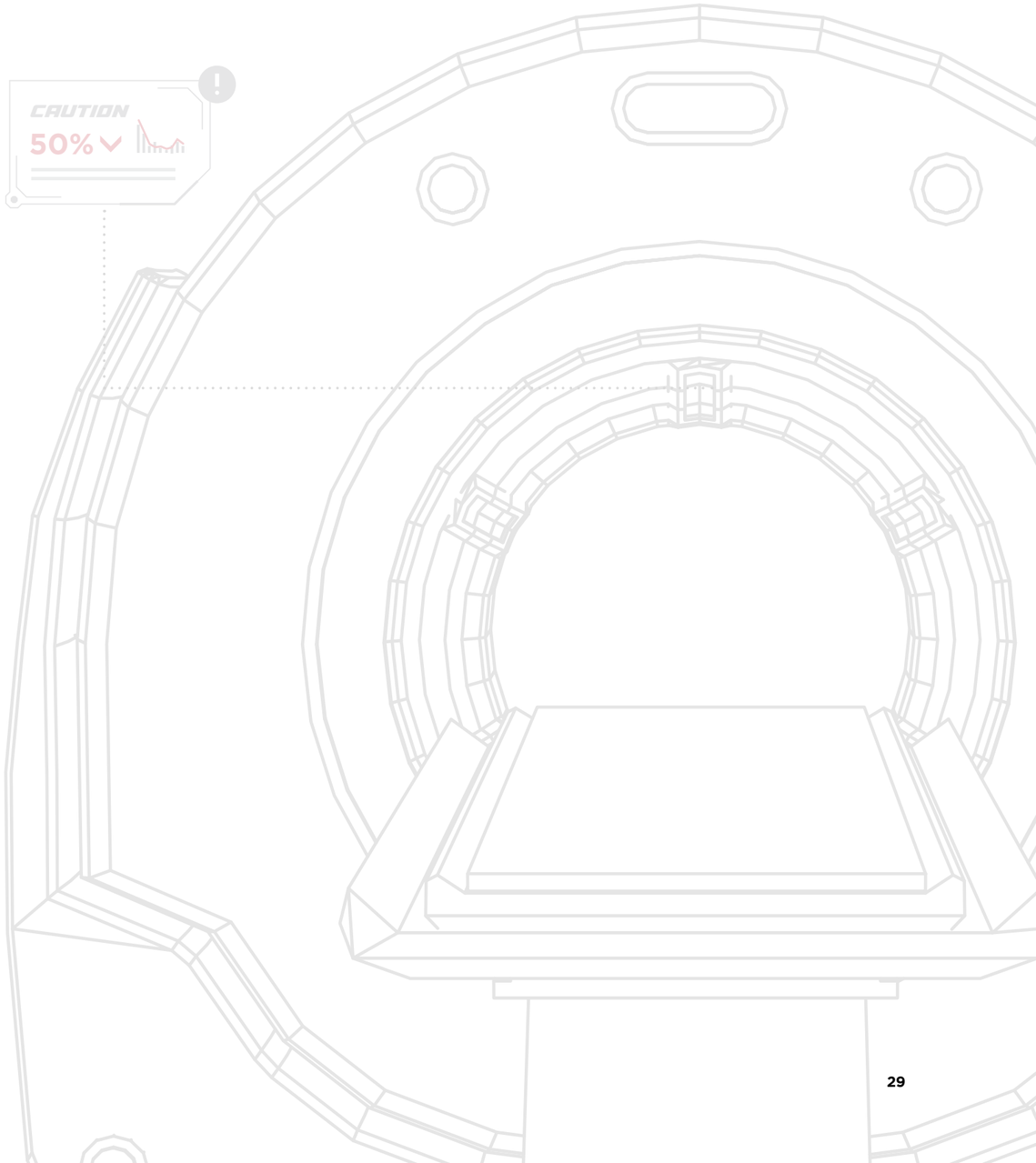


Key Event: Ransomware and Healthcare

The United States' fourth-largest hospital chain with 140 facilities, CommonSpirit Health of Chicago, suffered a ransomware attack in October that negatively impacted patient care, including surgery delays. A Texas man, for example, told *U.S. News* that his surgery scheduled for a CommonSpirit Health facility, was delayed on his doctor's recommendation until the hospital resolved its technical issues.

Meanwhile, up to 290 hospital systems were impacted by ransomware, according to security company Emisoft, which also shared further insight into the CommonSpirit attack where more than 620,000 patients' data was exposed in the attack. In other affected hospitals, critical systems that manage medication and doses were impacted and offline. Reportedly, a 3-year-old patient was given an overdose of pain medication, Emisoft said.

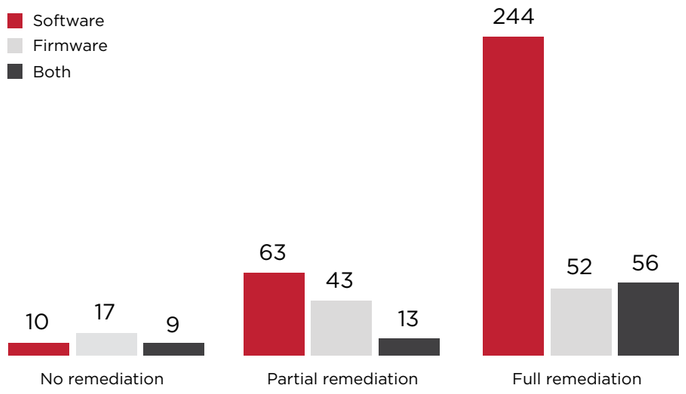
Healthcare has been the preferred target of ransomware actors, in particular since the start of the COVID-19 pandemic in 2020. Hospitals and other high-value targets are much more likely to pay an attacker's ransom demands in order to ensure continuity of care. Attackers, meanwhile, understand how vulnerable health delivery organizations are to cyberattacks, most of which still run legacy equipment retrofitted to connect online in order to provide remote patient monitoring.



Remediations

The good news is that the number of published OT vulnerabilities with partial or no remediation is dwarfed in the 2H 2022 by the availability of full remediations via software patches or firmware updates.

REMEDIATION BY FIRMWARE/SOFTWARE 2H 2022



76%

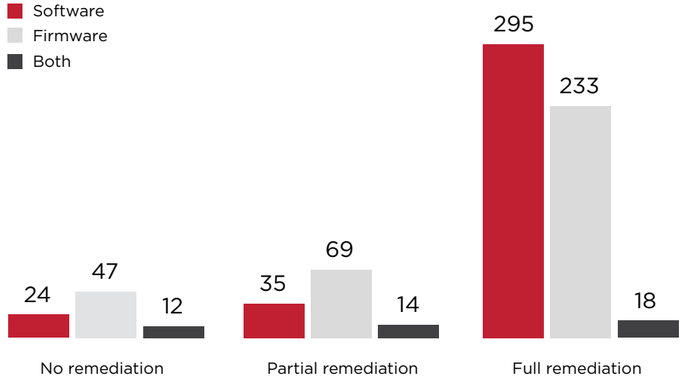
of fully remediated vulnerabilities are software based. Emphasizing the ease of patching software over firmware.

63%

of partially or unremediated vulnerabilities when exploited, could result in remote code execution or in denial-of-service

In the 1H 2022, full remediations via firmware updates were almost on par with software patches, but the trend has reversed itself in the second half of the year.

REMEDIATION BY FIRMWARE/SOFTWARE 1H 2022



54%

of fully remediated vulnerabilities are software based. Emphasizing the ease of patching software over firmware.

62%

of partially or unremediated vulnerabilities when exploited, could result in remote code execution or in denial-of-service

REMEDIATION BY THE NUMBERS

64% | **439 TOTAL**

Published vulnerabilities with full remediation: All products are patched and updated

21% | **143 TOTAL**

Published vulnerabilities with partial remediation: Not all affected products have a publicly available fix

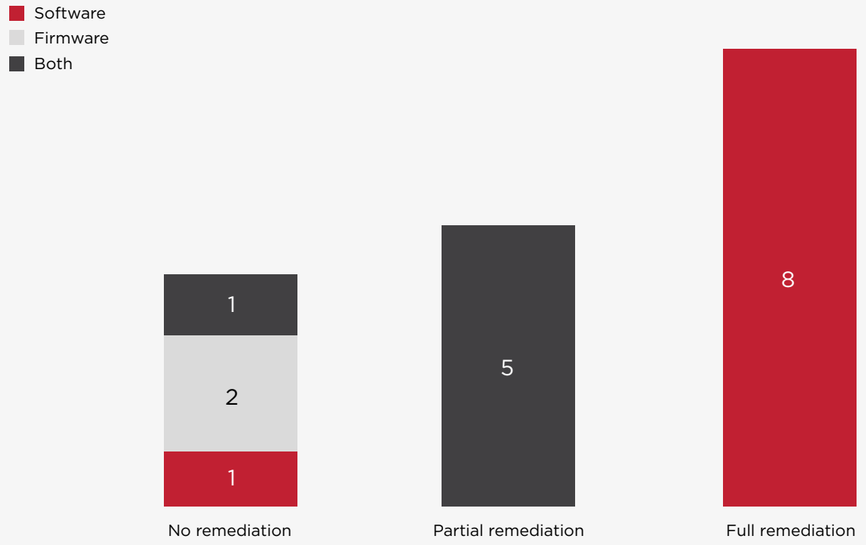
15% | **104 TOTAL**

No remediation: Product—including end-of-life—remains unpatched and without published mitigations

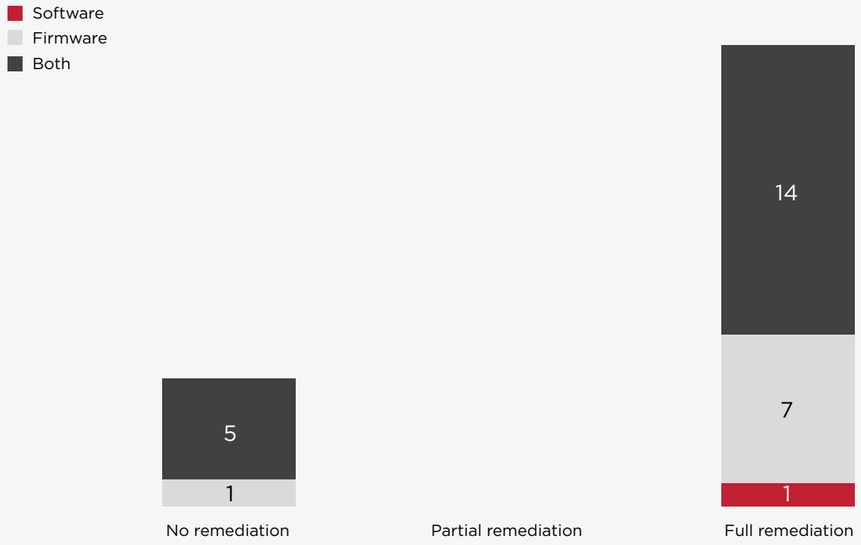
While the number of published internet of medical things vulnerabilities dropped in the 2H of 2022, the gap between full and partial remediation is much closer than in OT.

Full remediation of IoT vulnerabilities in both software and firmware tripled the number of published vulnerabilities with no available remediation.

REMEDIATION BY FIRMWARE/SOFTWARE OF IOMT VULNERABILITIES



REMEDIATION BY FIRMWARE/SOFTWARE OF IOT VULNERABILITIES



End-of-Life Products

End-of-life OT products can be vulnerable to security threats because the affected vendor no longer supports the product. These systems are often used in critical infrastructure, making them a target for malicious actors. Organizations that plan on using EOL OT products should have a plan in place for identifying and mitigating potential vulnerabilities in order to protect against potential attacks.

17

2% of the 688 published vulnerabilities in 2H 2022 that affect end-of-life OT products

0

Number of published vulnerabilities in 2H 2022 that affect end-of-life IoT and IoMT products

END-OF-LIFE EXPLOITABILITY

69%

Percentage of published vulnerabilities allow an attacker to carry out remote code execution or denial-of-service attacks

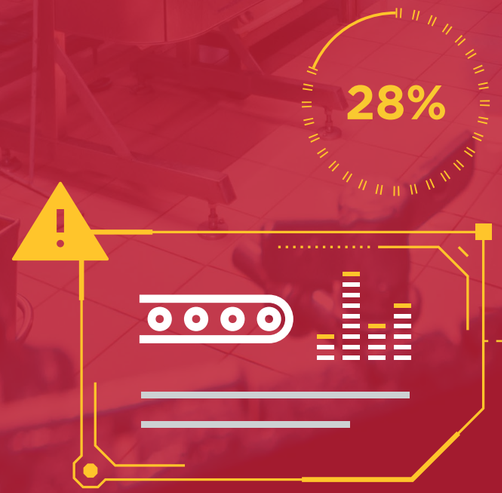
65%

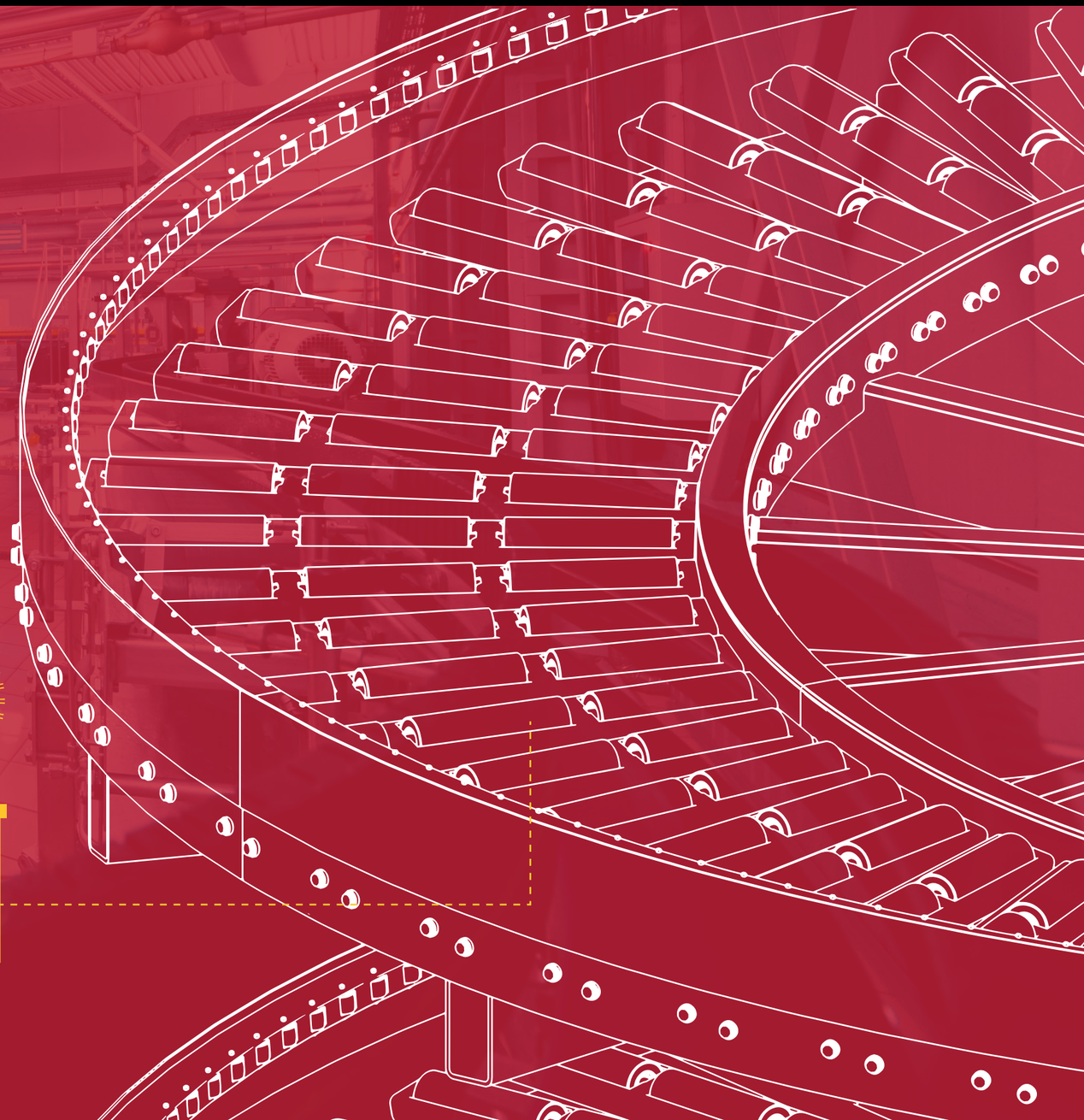
Percentage of published vulnerabilities exploitable via a network-based attack vector

12%

Percentage of published vulnerabilities without mitigation advice from the affected vendor

TRENDS TO WATCH





TRENDS TO WATCH IN 2023

Healthcare Cybersecurity is Patient Safety

The American Hospital Association has said it. And now, legislators have said it: Cybersecurity is patient safety.

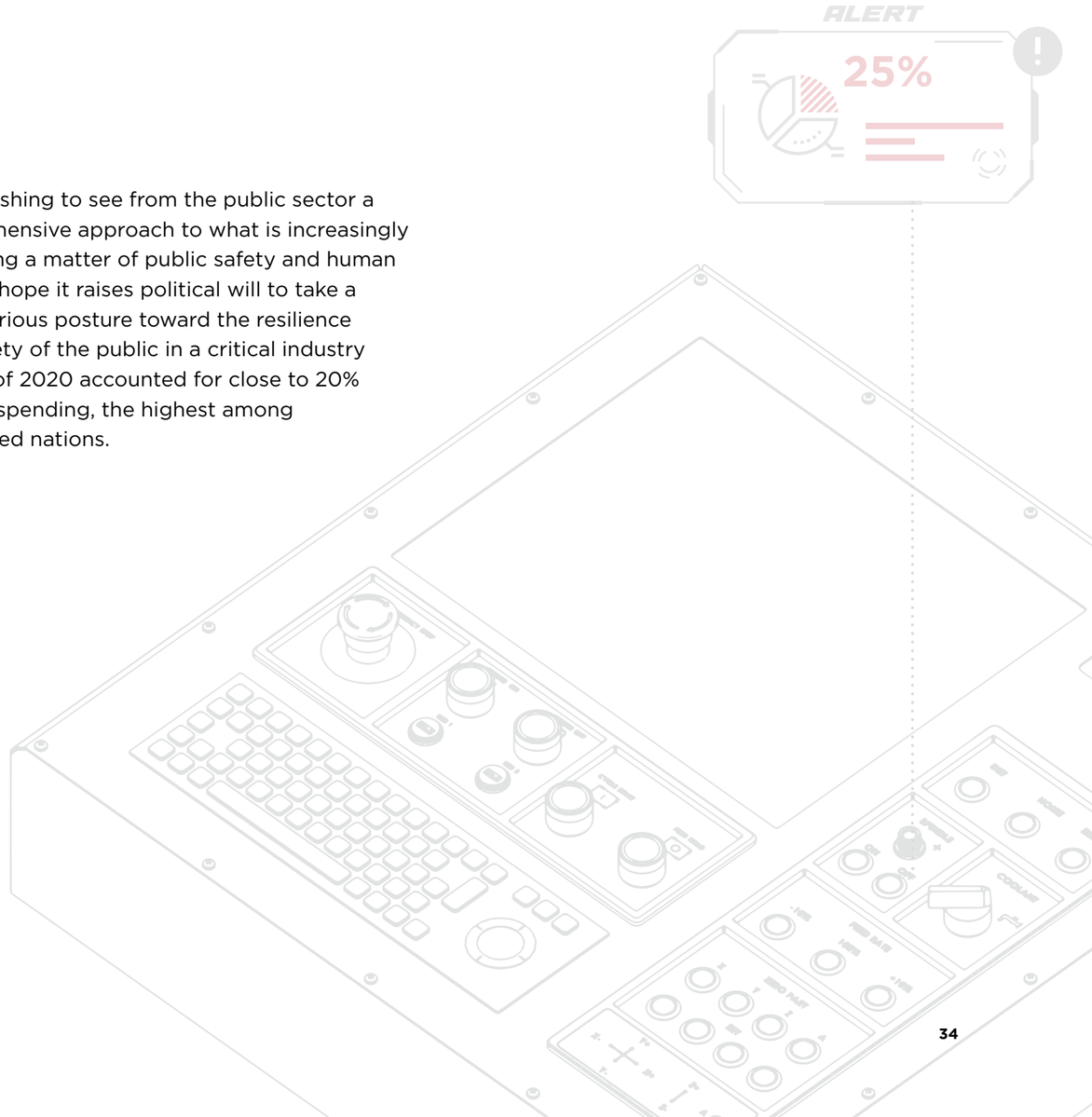
That was an important takeaway from a 2022 paper from Sen. Mark Warner (D, VA.). The paper puts cybersecurity on par with patient safety, and stresses that it can no longer be solely a data privacy concern.

"It has become readily apparent that the way that cybersecurity is treated by those in the healthcare sector needs to change. Cybersecurity can no longer be viewed as a secondary concern; it must become incorporated into every organization's—from equipment manufacturers to health care providers—core business models," the paper said. "Changing the healthcare sector's posture toward cybersecurity will require significant effort and resources from both the public and private sector."

Resource-strapped healthcare delivery organizations should be encouraged to see concrete incentives as proposed options for addressing legacy systems, for example, with a "Cash-for-Clunkers" type of buy-back program in order to upgrade to current, supported software and firmware at the heart of connected medical devices. This could be used to nudge manufacturers toward modular equipment design that supports minimum cybersecurity hygiene requirements.

The paper also supports incentives for the inclusion of SBOMs—a supplied list or inventory of software components—for every piece of software and healthcare equipment within healthcare. This aligns with a pre-market approval proposal in the PATCH Act and coupled with continuous vulnerability management, improves the quality of an HDO's asset inventory and management capabilities.

It's refreshing to see from the public sector a comprehensive approach to what is increasingly becoming a matter of public safety and human life. We hope it raises political will to take a more serious posture toward the resilience and safety of the public in a critical industry that as of 2020 accounted for close to 20% of GDP spending, the highest among developed nations.



Bringing XIoT to the Cloud

Cloud-based analysis of OT and IoT data brings a wealth of pros and cons, starting with improved understanding of process efficiency, for example, counterweighted by a significantly enhanced attack surface.

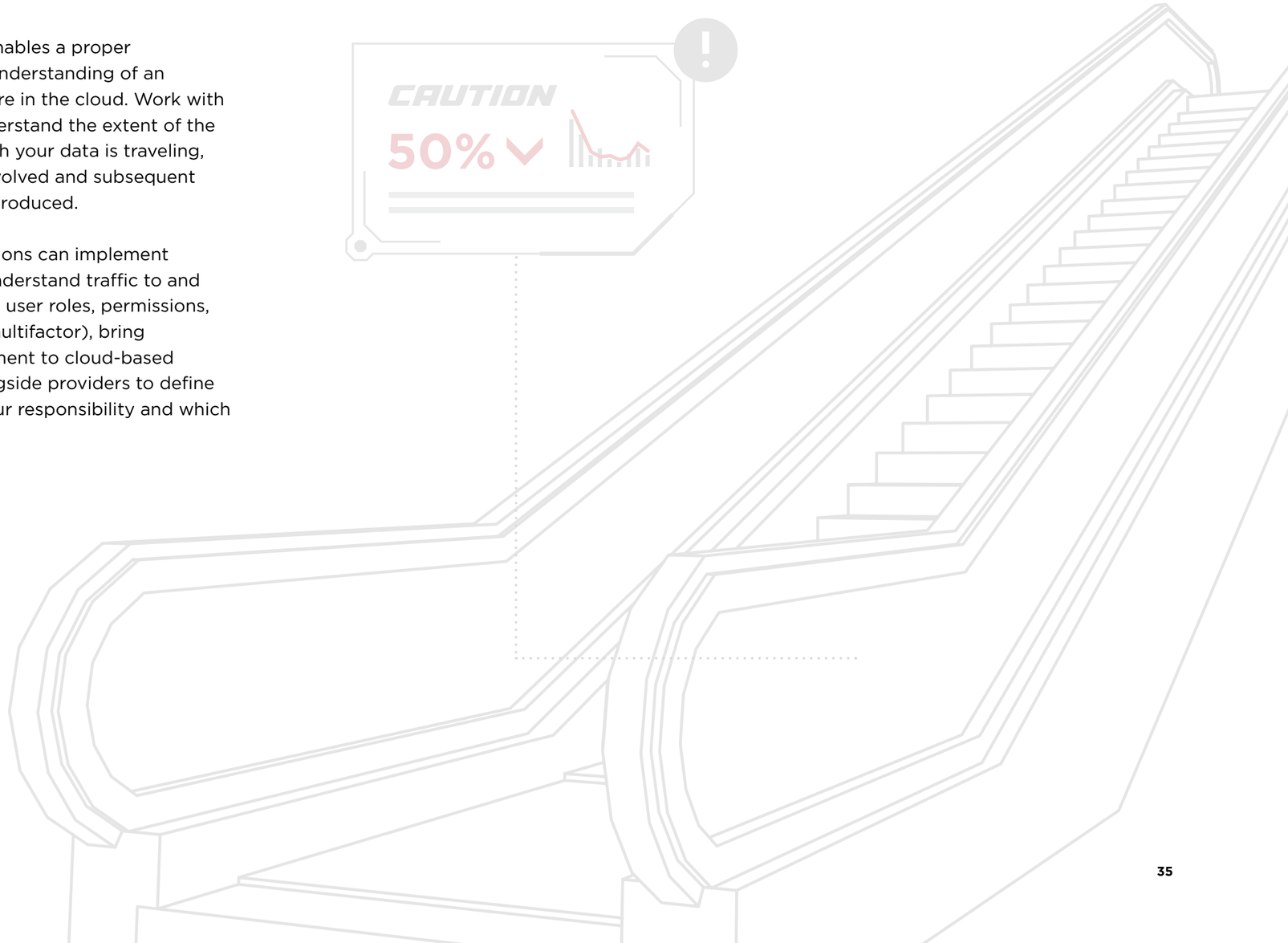
The data collected by OT and IoT device sensors and sent to a cloud-based architecture of servers, storage, and processing capabilities can turn your plant into a well-oiled machine, but it can also exacerbate the loss of air gapped networks and expose sensitive information to anyone with access to cloud-based storage, for example.

Security analysts responsible for cybersecurity of cyber-physical systems must understand these inherent risks and mitigate them.

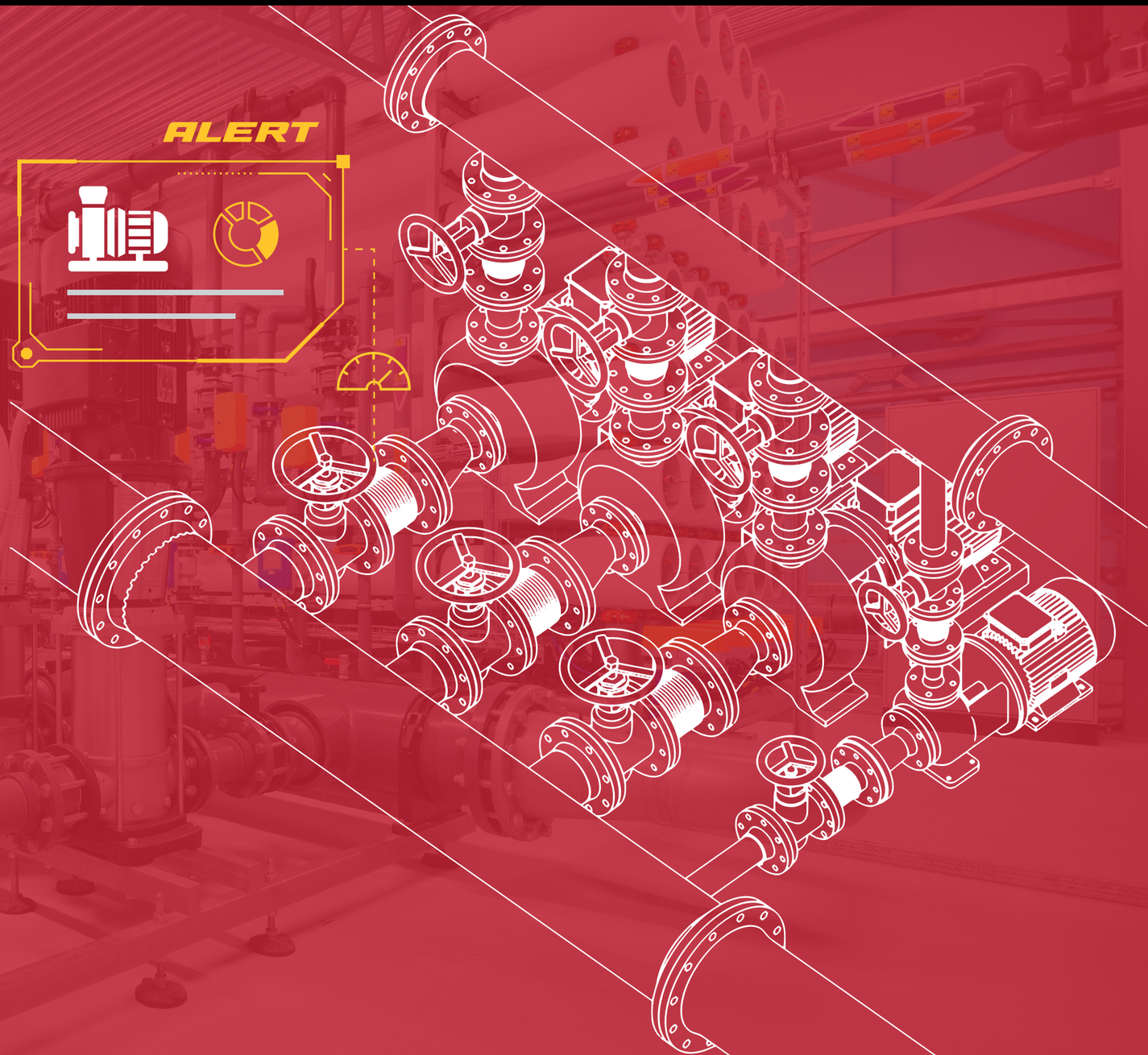
First, asset visibility should be a top priority—the most severe challenge to cybersecurity. Accurate asset inventories are difficult to achieve as new devices and data are added to the cloud, especially when trying to baseline what expected network behavior looks like in order to understand whether deviations pose a threat to the business.

Asset visibility then enables a proper risk assessment and understanding of an organization's exposure in the cloud. Work with your providers to understand the extent of the infrastructure on which your data is traveling, the physical assets involved and subsequent multi-tenancy risks introduced.

From there, organizations can implement monitoring tools to understand traffic to and from the cloud, define user roles, permissions, and authentication (multifactor), bring vulnerability management to cloud-based assets, and work alongside providers to define which controls are your responsibility and which are the provider's.



RECOMMENDATIONS



RECOMMENDATIONS

Team82 recommends these security measures in response to vulnerability trends we're sharing in this report.

Network Segmentation

Segmentation is far and away the champion of XIoT mitigation recommendations. Within OT networks, segmentation has been a security fixture as operators use it to limit external—and internal—access to critical systems and resources.

Air-gapped networks have been the de facto security practice to keep field devices and management systems clear of external connections. However, it's rapidly losing favor as OT, medical devices, and embedded systems running IoT devices are connected to the internet and managed via the cloud.

Users are urged to virtually segment assets, and prioritize segmentation:

- Segment networks virtually and configure them in such a way they can be managed remotely.
- Create zone-specific policies that are tailored to engineering and other process-oriented functions.
- Reserve the ability to inspect traffic and OT, Medical and IoT specific protocols in order to detect and defend against anomalous behaviors.

RECOMMENDATIONS

Secure Remote Access

Remote administration of XIoT devices is commonplace for internal security analysts and network managers, as well as for third-party contractors and vendors. Strategically, organizations must carefully manage privileges to medical devices, industrial control systems—in particular, field devices and systems at management levels of the Purdue Model for ICS—and other XIoT systems.

Secure remote access that streamlines access to internal employees and third parties, extends a zero-trust approach to privileges, and offers auditing and response capabilities is a must to reduce mean-time-to-repair.

Security practitioners are encouraged to do the following:

- Use a zero-trust implementation to help reduce downtime, ensure availability and service delivery.
- Verify VPN versions are patched and up to current versions
- Monitor remote connections, particularly those to OT networks, ICS devices, critical medical equipment, e-PHI servers and critical IoT devices.
- Enforce granular user-access permissions and administrative controls following the principle of least privilege.

RECOMMENDATIONS

Manage Risk from the Cloud

Process efficiency is a dominant business reason to connect XIoT devices and systems to the internet and manage them from the cloud. Doing so brings enhanced analytics that improve operational efficiency and usability; it also carries risk that must be managed.

Many XIoT devices, especially those within OT, are no longer air-gapped and therefore have a much larger attack surface. Threat actors may see an opportunity to target vulnerabilities exposed by connectivity at scale.

Risk management in cloud managed OT networks can be broken down into several security aspects, right, security practitioners and ICS companies should do the following:

Data Security: Encryption and Secure Communication

- Verify XIoT devices' cloud support protocols, such as MQTT or HTTPS via Web Client/ REST. Within OT, for example, these are used to exchange data between PLCs and the cloud.
- Use security mechanisms, such as encryption and signing of data and communication with X.509 certificates or hardware-based encryption.

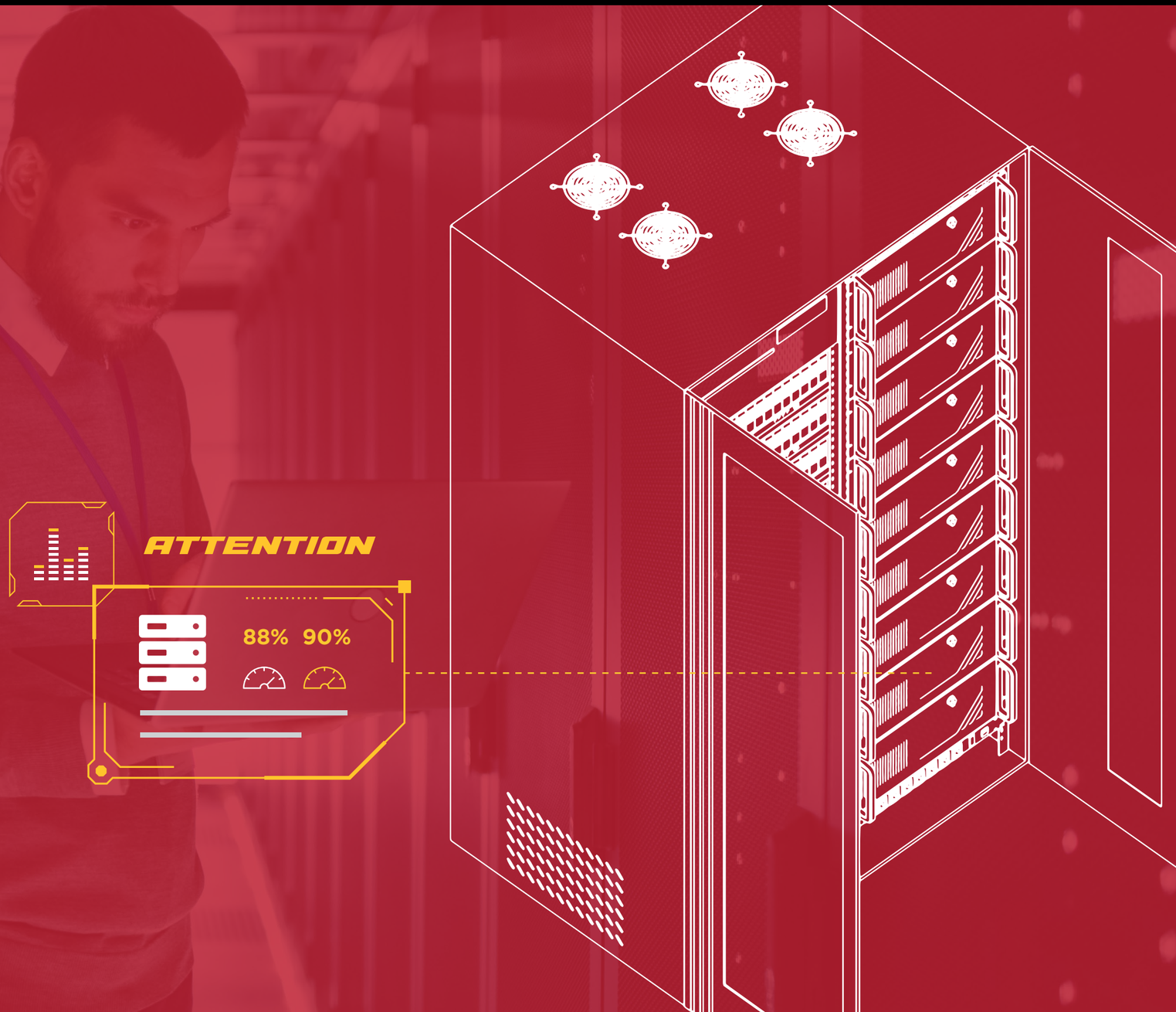
Authentication and Identity Management

- Add and enforce multi-factor authentication.
- Strengthen credentials, especially passwords to secure remote connections.
- Use granular user and role-based access control policies.

Defining Responsibilities

- Adhere to a shared responsibility model and define a line between an organization's and the cloud provider's responsibilities.

ABOUT THE STATE OF XIoT SECURITY REPORT



ABOUT THE STATE OF XIoT SECURITY REPORT 2H: 2022

Claroty Team82's biannual State of XIoT Security report is a deep examination and analysis of connected device vulnerabilities disclosed during the second half of 2022 affecting industrial, healthcare, and commercial products.

Throughout this report, you'll learn about vulnerabilities impacting industrial control systems, the internet of medical things (IoMT), building automation systems, and enterprise internet of things (IoT) devices that sustain our lives and enable innovation across business and critical infrastructure sectors.

Recognizing the critical need to understand the XIoT risk and vulnerability landscape, Team82 developed an automated collection and analysis tool that ingests vulnerability data from trusted open sources, including the National Vulnerability Database (NVD), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), CERT@VDE, MITRE, and industrial automation vendors Schneider Electric and Siemens.

About Claroty

Claroty empowers industrial, healthcare, and commercial organizations to secure all cyber-physical systems in their environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com.

About Team82

Team82, the research arm of XIoT cybersecurity company Claroty, is an award-winning group of researchers known for its development of proprietary threat signatures, OT protocol analysis, and discovery and disclosure of industrial, healthcare, and commercial vulnerabilities.

Fiercely committed to strengthening XIoT security and equipped with the industry's most extensive testing lab, the team works closely with leading industrial vendors to evaluate the security of their products. As of December 2022, Team82 has discovered and disclosed more than 400 vulnerabilities.

For more information, visit: https://claroty.com/team82/

ACKNOWLEDGEMENTS

The primary author of this report is Bar Ofner, security researcher at Claroty.

Contributors include: Rotem Mesika, threat and risk group lead, Nadav Erez, vice president of data, Sharon Brizinov, director of research, Amir Preminger, vice president of research, Chen Fradkin, data scientist, and Moran Zaks and Yuval Halaban, security researchers. Special thanks to the entirety of Team82 for providing exceptional support to various aspects of this report and research efforts that fueled it.

T82
THE CLAROTY RESEARCH TEAM

CLAROTY