CLAROTY

TEAM82

State of CPS Security 2025: OT Exposures

An analysis of the riskiest operational technology exposures putting critical infrastructure organizations in the crosshairs of adversaries

Introduction

Threats against operational technology (OT) within critical infrastructure sectors have taken on a decidedly aggressive tone. The Chinese are embedding offensive weapons inside American military and corporate networks. They have infiltrated telecommunications companies and internet service providers in order to spy on Americans, including the then-president-elect. The Russians, meanwhile, have made it a decades-long practice to attack the power grid in Ukraine, and the Iranians have declared all Israeli-made technology targets of their capabilities in cyberspace.

Security leaders can no longer afford to treat OT as a black box they don't understand, or believe in mythical air-gaps from the internet protecting them from any potential threat. Threat actors are investing time and resources into the targeting and exploitation of weaknesses in OT, and criminal outfits continue to aim ransomware and other extortion-based cyberattacks at enterprises in all 16 critical infrastructure sectors as defined by the Cybersecurity Infrastructure and Security Agency (CISA).

Chief information security officers (CISOs) and others responsible for OT and the protection of cyber-physical systems (CPS) have agency to act. They must understand how these critical devices are connected to the internet and prioritize defending them based on their exposures.

The data collected for this report spans a number of industries under the umbrellas of manufacturing, natural resources, and logistics and transportation.

Some of those industries include:

Food & Beverage

Pharma

Automotive

Oil & Gas

Mining

Chemical

Aviation

Rail

Maritime/Ports

940,000+

OT Devices Analyzed

270

Organizations

Those exposures include known exploited vulnerabilities (KEVs) that remain unpatched, insecure connectivity practices for OT devices that are internet-facing, the use of insecure protocols for communication between OT devices and the engineering workstations and human-machine interfaces that manage them, outdated firmware, weak configurations that can be leveraged by attackers, and a reliance on end-of-life operating systems and devices that are no longer supported by their respective vendors.

In this report, Claroty Team82 will share its findings from an analysis of close to one million OT devices, most of which are found in the manufacturing, logistics and transportation, and natural resources sectors. We will illuminate the exposures that are most coveted for exploitation by adversaries, and make recommendations that help enterprises reduce their risk.

Key Findings

Of the close to one million OT devices analyzed, Claroty Team82 found that:

12%
contain KEVs

40%
of the organizations analyzed have these assets insecurely connected to the internet

7%
of the devices are exposed with KEVs that have been linked to known ransomware samples and actors

31%
of the organizations analyzed have these assets insecurely connected to the internet

We found that **more than 12% of industrial organizations in the research had OT assets communicating with malicious domains**, demonstrating that the risk to these assets is not theoretical.

Threat Actors Strategically Targeting OT

Adversaries are targeting OT with greater frequency in the hopes of impacting national security among Western nations, as well as economic stability in those areas, and in some cases, public safety. The leverage point in an OT attack is often the inadvertent exposure of a device that is insecurely connected to the internet, including OT assets that are directly connected online rather than through some form of secure access technology.

Attackers can use this to their advantage and establish communication channels with networks inside manufacturing, logisitics and transportation, and natural resources enterprises, three industries that directly influence and impact the lives of tens of millions. Once that foothold is established, the opportunity for lateral movement on either the OT or enterprise network exists. From there, vulnerabilities or configuration weaknesses in engineering software, HMIs, or OT communication protocols are ripe for exploitation and could create an opportunity for an adversary to sabotage critical processes and potentially cause impact in the physical world.

Within the three critical sectors featured in our research, the threat to public safety or of personal injury to operators becomes more than theoretical.

The disruptive nature of these attacks enables adversaries to project a measure of power and control over critical assets, while at the same time potentially instilling chaos in society. In the Western world, we have grown accustomed to the resiliency of critical services, and disruption could degrade the public's perception of our government's ability to keep us safe.

Further complicating defenses are the well-financed state-sponsored threat actors behind this malicious activity. China, Russia, and Iran have ramped up offensive activity against Western interests.
Some examples include:

Volt Typhoon and Salt Typhoon: Both are China-linked threat actors that have infiltrated U.S. military and critical infrastructure operations.

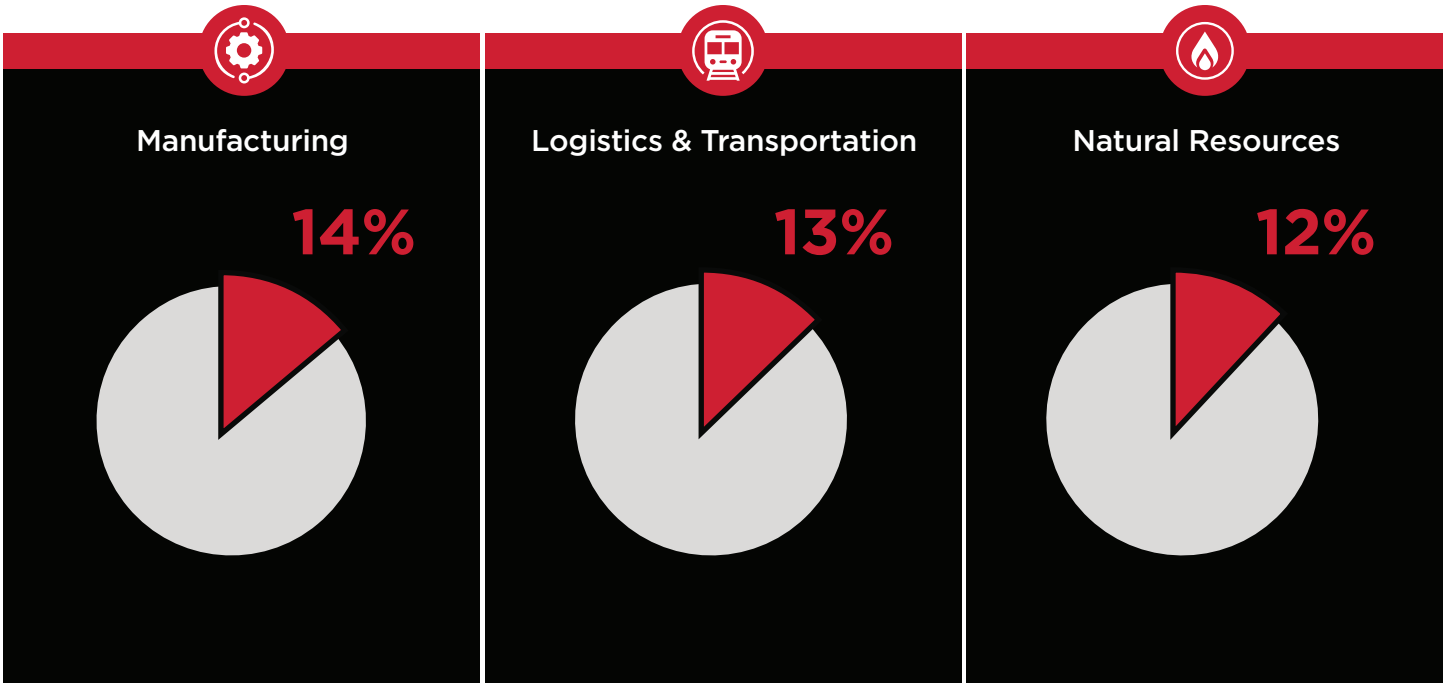
- Volt Typhoon uses native legitimate tools on systems it infiltrates by exploiting weak or default passwords for access. CISA has labeled the group's activity as disruptive or potentially destructive in the event of a major crisis or conflict with the United States.
- Salt Typhoon has been linked to breaches against U.S. internet service providers and ISP wiretap systems, allegedly exfiltrating data useful for intelligence operations.

Sandworm: Linked to Russian military intelligence, this APT is alleged to be responsible for several attacks against Ukraine's power grid dating back 10 years, as well as the destructive NotPetya malware. It is also responsible for the deployment of Industroyer and Industroyer 2, which was purpose-built malware targeting industrial equipment communicating over the IEC-104 (IEC 60870-5-104) protocol. In Ukraine, the targets were power system automation applications used in high voltage electrical substations.

CyberAv3ngers: Under the watch of the Islamic Revolutionary Guard Corps Cyber Electronic Command (IRGC-CEC), this APT has vowed to target any OT and enterprise technology developed in Israel. In late 2023, they targeted Unitronics' integrated HMI/PLC devices inside U.S. water facilities, and in December 2024, attacks against civilian infrastructure were disclosed using a Linux-based backdoor called IOCONTROL that has a modular configuration that allows it to be used against OT assets, including PLCs and HMIs.

Our research shows that critical sectors such as manufacturing, logistics and transportation, and natural resources have OT assets that are communicating with malicious domains, including some in China, Russia, and Iran, for example.

OT Devices Communicating with Malicious Domains



The potential for damaging attacks that either disrupt services or are destructive to critical infrastructure is real.

Therefore, cybersecurity leaders inside these organizations must inventory their highest-risk assets, and manage exposures through securing remote access, implementing network-centric controls (including segmentation), and compensating controls when necessary.

To properly do so, let's examine the data from our research, to understand the riskiest exposures we uncovered.

Quantifying the Riskiest OT Exposures

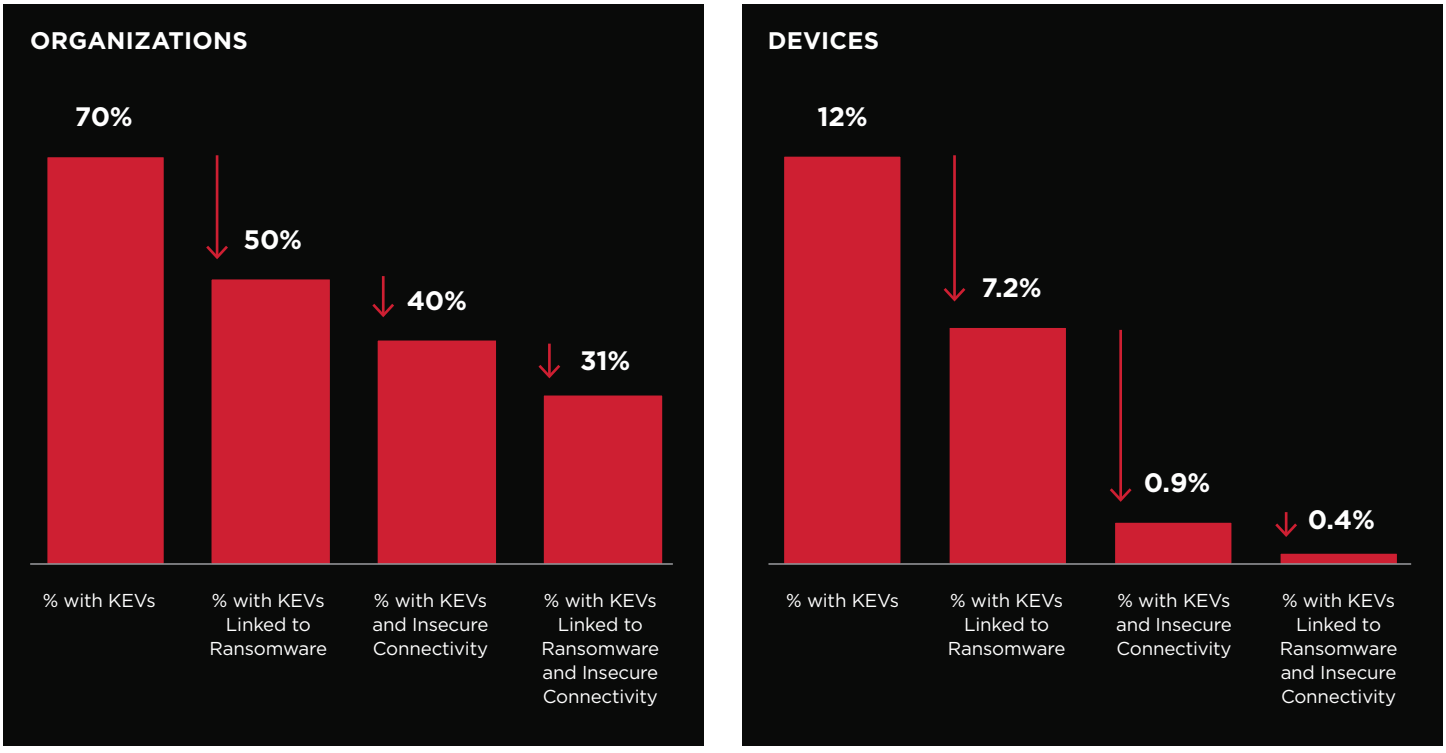
For a modern enterprise, the riskiest OT exposures cannot be measured in critical CVEs alone. Doing so would place undue burden on asset owners and operators trying to boil an ocean of unpatched vulnerabilities; fixing them at any kind of scale would be done at a tremendous human and monetary resource drain. Moreover, many of the overwhelming number of CVEs have no corresponding known exploit that could compromise the asset.

Instead, we offer an approach that redefines vulnerability management and prioritizes remediation not only to known exploited vulnerabilities, but by those devices containing KEVs that are also insecurely exposed to the internet, and at risk of ransomware.

For example, the total number of OT devices from this subset of data from 270 organizations with confirmed KEVs alone is more than 111,000, or 12% of our sample. That's an unwieldy number, yet not unsurprising given that more than 25% of KEVs are associated with the Windows operating system, and many HMIs and EWS run on Windows computers.

But by breaking that down to devices with confirmed vulnerabilities for which there are publicly available exploits that are linked to ransomware groups, plus insecure connectivity, that number dwindles to 3,800, or 0.4% of devices. That presents operators and administrators with a much more manageable risk calculus.

Prioritizing Device Remediation: From Unwieldy to Manageable



By taking this approach, they can consider remediation of the highest-risk devices first, where the risk of exploitation is at its greatest, and successful attacks have the greatest impact of disrupting processes in key industries such as food and beverage or oil and gas.

Within manufacturing, for example, there were more than 96,000 devices with confirmed KEVs in our dataset. These are much higher totals and percentages than logistics and transportation, yet still comparable.

Industry	Devices with Confirmed KEVs	% of Devices with Confirmed KEVs	% of Organizations with Confirmed KEVs
Manufacturing	96,387	13%	74%
Logistics & Transportation	794	1.6%	65%
Natural Resources	3,921	7%	69%

We then looked for those confirmed KEVs that were linked with ransomware. Manufacturing is consistently a top sector targeted by ransomware actors, likely because of a perceived willingness to meet ransom demands in order to resume production and minimize downtime. Within manufacturing, we found a significant percentage of devices and organizations with KEVs linked to ransomware.

Confirmed KEVs Linked to Ransomware

Industry	Devices with confirmed KEVS linked to ransomware	Percentage of overall devices with KEVs linked to ransomware	Percentage of overall organizations with KEVs linked to ransomware
Manufacturing	65,473	9.1%	61%
Logistics & Transportation	231	0.5%	42%
Natural Resources	1,478	3%	40%

As mentioned earlier, insecure connectivity opens the door to OT and enterprise networks, lateral movement, and exploitation. The riskiest behavior is directly connecting an OT device to the internet; such devices are assigned IP addresses and can be mapped by internet-scanning services such as Shodan. Attackers can use this information to find publicly accessible devices such as PLCs, and leverage password-cracking tools to break weak or default credentials.

Within our dataset, we saw the largest percentage of devices with confirmed KEVs linked to ransomware that were insecurely connected to the internet within the manufacturing sector; higher than the overall total percentages of devices in our data set.

KEVs Linked to Ransomware and Insecure Connectivity

Industry	Devices with confirmed KEVS linked to ransomware and insecurely connected to the internet	Percentage of devices with KEVs linked to ransomware and insecurely connected to the internet	Percentage of organizations with KEVs linked to ransomware and insecurely connected to the internet
Manufacturing	3,269	0.5%	43%
Logistics & Transportation	37	0.1%	19.2%
Natural Resources	393	0.7%	22.4%

The answer is to either block the internet connection or—where required—put these assets online behind a dedicated remote access solution; at a minimum a virtual private network (VPN) that encrypts communication to and from the device. Organizations are facing unprecedented demand for remote access to OT and other CPS; there are significant productivity and cost savings to be gained. But many organizations are now connecting OT assets to the public network that were not long ago isolated. In addition to operational disruption, organizations face reputational damage that is difficult to quantify, and the threat of regulatory non-compliance in the event of a breach.

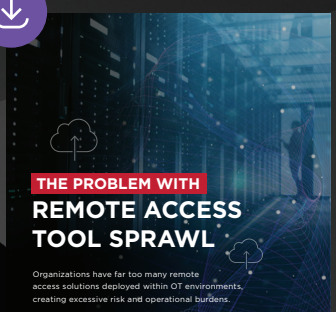
Even then, however, some organizations are throwing excessive remote access technology at the problem. Research from Team82 published in September 2024 showed that 55% of organizations in our data set had four or more remote access tools in the OT environment; 33% of organizations had six or more. Many of these tools were found to be non-enterprise-grade security products; 79% of organizations have more than two of these non-enterprise-grade tools installed on devices running on the OT network, creating risky exposures and additional operational costs.

55%

of organizations in our data set had four or more remote access tools in the OT environment

33%

of organizations had six or more



Recommendations

While many OT security projects start in the asset inventory phase, a catalog of the assets in and of themselves doesn't drive down cyber risk. We recommend an exposure management approach to risk reduction that prioritizes OT devices most at risk for exploitation.

Exposure Management

An exposure management approach provides enterprises with a dynamic model for risk mitigation, one that strategically addresses the riskiest OT assets and looks beyond simply remediating the most critical CVEs.

Exposure management requires a more focused approach to mitigating risk, and includes scoping, discovering, prioritizing, validating, and mobilizing phases. We think it's critical to leverage this framework and apply it to the context of OT.

Scoping

In asset-intensive enterprises, **scoping** should be focused around determining the assets that are essential for the execution of critical business processes, such as production lines. By scoping based upon business impact, security practitioners can dramatically reduce the denominator of assets that need to be continuously inspected for cyber risks.

Discovery

Discovery focuses on achieving a robust asset inventory of devices in the scope of interest. What we've learned is that getting a detailed inventory requires a data-driven rubric of collection methods, with the ultimate goal of gaining sufficient detail to drive vulnerability prioritization efforts.

A CVSS-focused vulnerability management program potentially ignores other exposures that introduce greater risk to the organization.

- Known exploited vulnerabilities (KEVs)
- Legacy and end-of-life software and firmware
- Default or weak, guessable passwords
- Overextended privileged access
- Inadequate or insecure system configurations
- Lack of policy enforcement
- Insecure connectivity of CPS assets to the internet

Prioritizing

While **prioritizing** risks takes vulnerabilities into account, it also expands the definition of risk to include misconfigurations and risky conditions, like default credentials. Enrichment with known exploits, exploit prediction scoring system, and business impact assessments can both focus on the most consequential impacts to production, but also further narrows the effort to risks that are exploitable today.

Validating

While many exposures may exist, an attacker may not actually be able to exploit them. The ports may be closed, or a firewall may be blocking traffic from an at-risk system. That's why **validating** the attack path is an important step in focusing remediation efforts on the assets that are both high risk and exposed.

Mobilization

Mobilization is a critical step of the exposure management cycle to ensure integration into existing enterprises workflows to drive peer collaboration for activities like patching, changing passwords, or reconfiguring the infrastructure to eliminate risk.

About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. 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. To learn more, visit claroty.com.

About Team82

Team82, the research arm of cyber-physical systems (CPS) protection company Claroty, is an award-winning group of researchers known for threat research, OT and medical protocol analysis, and discovery and disclosure of industrial, healthcare, and commercial vulnerabilities. Committed to strengthening CPS cybersecurity and equipped with the industry's most extensive testing lab, the team works closely with leading vendors to evaluate the security of their products. As of January 2025, Team82 has discovered and disclosed more than 640 vulnerabilities. Learn more at claroty.com/team82.

CLAROTY

TEAM82