OT Security Insights

2024

paloalto NETWORKS | SIEMENS

Table of Contents

Key Findings

Exploitation of remote services:
This was the most common tactic in OT networks, accounting for **20%** of incidents, with attackers frequently leveraging outdated protocols like SMBv1 to gain initial access and move laterally.

Aging vulnerabilities:
61.9% of exploit triggers in OT networks were linked to CVEs aged **6 to 10 years**, indicating that legacy systems remain a significant vulnerability.

Manufacturing at high risk:
The manufacturing sector accounted for **82.7% of internal exploit attempts**, demonstrating the significant risks posed by OT systems and internal network vulnerabilities, especially through lateral movement and persistence techniques.

Unknown malware challenge:
79.92% of detected malware in OT networks was classified as "**Unknown**," underscoring the growing challenge of identifying and mitigating novel or evolving threats.

Widespread exposure of OT devices:
Cortex Xpanse® captured approximately **46.2 million observations** of OT devices in 2023, identifying over **1.25 million unique IP addresses** and over **4.53 million unique device fingerprints** associated with OT application servers exposed to the public internet, revealing a substantial attack surface that adversaries can exploit.

Executive Summary

This whitepaper, a collaborative effort by Palo Alto Networks and Siemens, explores the escalating cybersecurity risks associated with SCADA and OT devices exposed on the public internet. As the convergence of information technology (IT) and operational technology (OT) accelerates, the attack surface for critical infrastructure expands, making these systems increasingly vulnerable to cyberattacks with potentially severe operational and physical consequences.

In 2023, over **1.25 million SCADA and OT devices** were found to be exposed to the internet, a significant risk that could allow cyberattacks to directly impact essential services. The study highlights that **enhanced fingerprinting techniques**, introduced in **March–April 2023**, dramatically improved the identification of these exposed devices, particularly SCADA and building control systems. This advancement provided better visibility into the global distribution of vulnerable devices, emphasizing the need for more robust security practices in OT environments.

The analysis of **51,000 OT firewalls**, using Palo Alto Networks **App-ID™**, revealed substantial malware and exploit activity in OT networks. Mapped to the **MITRE ATT&CK® Matrix for ICS**, key attack tactics identified include **Initial Access**, **Lateral Movement**, and **Privilege Escalation**, which were frequently used to target OT systems. These findings underscore how attackers gain footholds in critical infrastructure. The geographical and industry-specific analysis further showed that sectors such as **manufacturing**, **energy**, and **retail** are particularly at risk, with **poor network segmentation** and misconfigurations expanding their attack surfaces.

The whitepaper concludes that, to mitigate these risks, organizations must strengthen security controls, improve network segmentation, and implement continuous monitoring. A proactive, adaptive approach to OT security is critical to safeguarding against the growing complexity of cyberthreats targeting critical infrastructure systems.

Key definitions for the purposes of this paper:

- **OT network**—an identified network where a firewall logged any OT traffic.
- **OT traffic**—any traffic logs tagged as OT per Palo Alto Networks App-ID.
- **Non-OT network**—a network where a firewall did NOT log any OT traffic.

Overview

This whitepaper represents a collaborative effort between Palo Alto Networks and Siemens, combining the expertise of two industry leaders in cybersecurity and operational technology (OT), respectively. Palo Alto Networks, recognized for its cutting-edge cybersecurity solutions, provides insights into network protection, threat detection, and risk mitigation, while Siemens, a global leader in industrial automation and OT, contributes its extensive knowledge of critical infrastructure systems. Together, they offer actionable insights to help organizations secure their cyber-physical systems in an increasingly connected and vulnerable digital landscape.

As the convergence of information technology (IT) and OT systems progresses, the need to secure SCADA (supervisory control and data acquisition) and OT devices becomes critical. These systems, which control essential infrastructure, face unique threats when exposed to the public internet. Unlike traditional IT systems, cyberattacks on OT devices can have real-world, physical consequences. This paper addresses the risks associated with exposing SCADA and OT devices to the internet, where poor network segmentation and misconfigurations expand the attack surface.

To assess these risks, the paper utilizes data from Palo Alto Networks Cortex Xpanse® Internet Landscape Intelligence (ILI), which identified over 1.25 million exposed OT devices in 2023. Enhanced fingerprinting techniques introduced later in the year improved visibility into the global distribution of publicly accessible SCADA devices. The report also analyzes telemetry from OT firewalls, utilizing advanced security solutions like App-ID™, WildFire®, and Threat Prevention.

App-ID plays a critical role in categorizing network traffic by application, independent of port or encryption, enabling granular visibility into OT-specific applications and protocols. It identified over 51,000 firewalls in OT networks, providing valuable insights into vulnerabilities. WildFire's static and dynamic analysis capabilities detect zero-day malware targeting OT systems, offering critical insights into threats such as Trojans and ransomware. Threat Prevention further strengthens defenses by mitigating exploits and attacks, including remote service exploitation and privilege escalation, often seen in OT environments.

Together, App-ID, WildFire, and Threat Prevention offer a comprehensive view of the current threat landscape, providing a roadmap for improving security in SCADA and OT systems exposed to the internet.

Exposed SCADA Devices on the Internet

The information security considerations of SCADA, ICS, and OT devices share much in common with traditional IT systems. Both demand common defensive strategies, including keeping software and firmware up-to-date; deploying network and endpoint security solutions; specifying authentication and access control mechanisms; and applying logging, monitoring, and alerting policies.

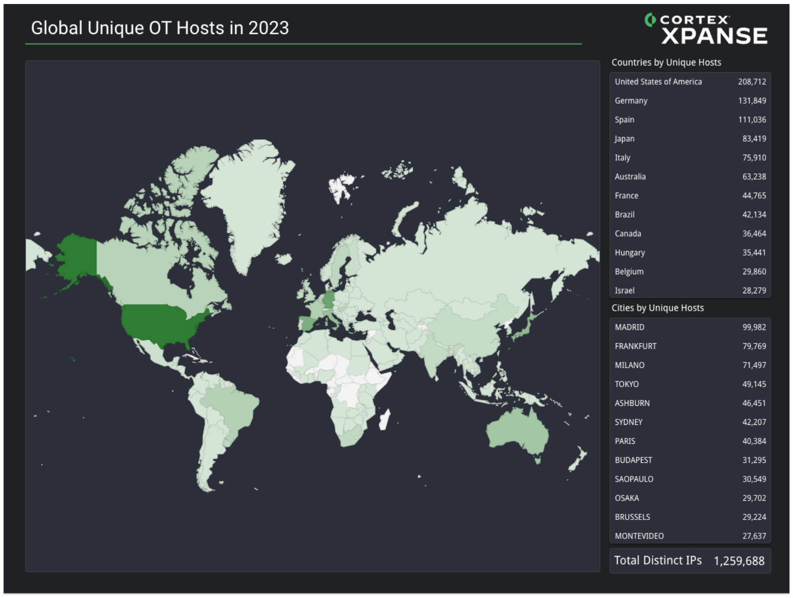
However, the line between the digital and physical spaces in the domain of OT devices comes with additional challenges and consequences. The real-world interactions of OT devices have led to the growing use of the term “cyber-physical systems” due in part to the kinetic or physical operations these devices often affect or perform.

These cyber-physical systems typically should not be exposed to the public internet for remote access (benign, sanctioned, or otherwise). The consequences of poor network configuration or segmentation of cyber-physical systems leads to an attack surface that any threat actor can attempt to exploit, which can result in unexpected real-world impact.

Geographical Analysis

One crucial insight preceding the analysis of threat trends is the global attack surface of SCADA and OT devices. Specifically, we measured the unique hosts and application servers that are accessible on the public internet.

The methodology for global distribution statistics of relevant hosts begins with Palo Alto Networks Cortex Xpanse, which scans the entirety of IPv4 space and targeted portions of IPv6 space every day. Targeting manifests instruct collections infrastructure to scan a wide array of ports and application protocols with many techniques and probes. These scan results are then processed by “fingerprinting” to label specific observations, such as networking devices, applications, operating systems, topological details, and more. Devices are further categorized to attribute more details to an application server, including the manufacturer, product, software version, and protocol.



Countries by Unique Hosts

United States of America	208,712
Germany	131,849
Spain	111,036
Japan	83,419
Italy	75,910
Australia	63,238
France	44,765
Brazil	42,134
Canada	36,464
Hungary	35,441
Belgium	29,860
Israel	28,279

Cities by Unique Hosts

MADRID	99,982
FRANKFURT	79,769
MILANO	71,497
TOKYO	49,145
ASHBURN	46,451
SYDNEY	42,207
PARIS	40,384
BUDAPEST	31,295
SAOPAULO	30,549
OSAKA	29,702
BRUSSELS	29,224
MONTEVIDEO	27,637

Total Distinct IPs 1,259,688

Figure 1: Xpanse ILI view of SCADA and building control system hosts

For this publication, we utilized Cortex Xpanse Internet Landscape Intelligence (ILI) to extract insights for OT devices observed in 2023. Specifically we targeted hosts labeled with the SCADA and building control system fingerprints. Both of these device types were heavily enriched with new fingerprints in March and April of 2023, which led to greater visibility for devices during those months and onward, and comparatively fewer observations in the first calendar quarter of 2023. We collectively call scan observations against these device fingerprints as OT (see figure 1).

In 2023, Xpanse captured approximately 46.2 million OT device observations on over 1.25 million unique IP addresses and over 4.53 million unique device fingerprints, each representing a positive identification of an OT device application server improperly exposed to the public internet. This distinction can be useful for devices colocated on a host or behind a firewall or other NAT network.

The device observations count represents the aggregate daily occurrences of fingerprinted application servers running over the year. The unique IP addresses have been observed hosting an OT service at least once on one or more ports. Lastly, unique device fingerprints describe the count of distinct OT application servers over all of those IP addresses, indicating there is reuse or colocation of application servers on some hosts.

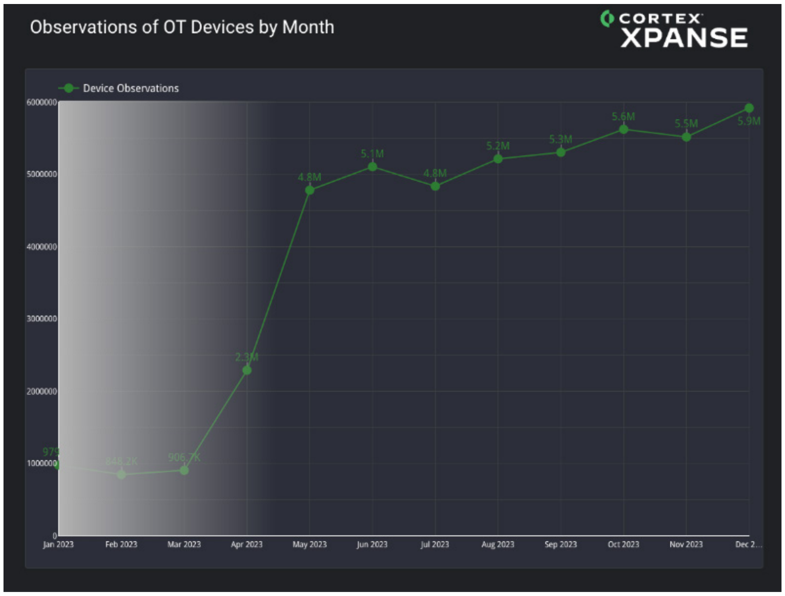


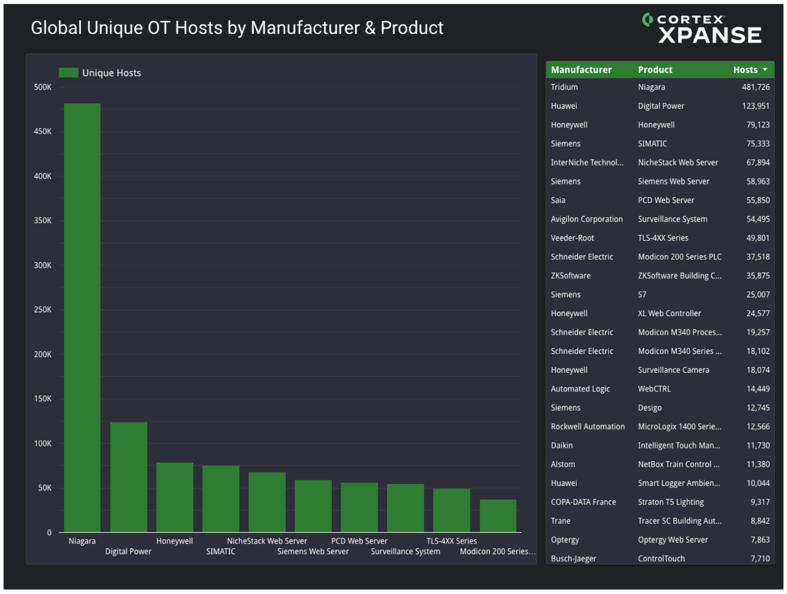
Figure 2: Monthly device observations in 2023 including new fingerprints added in April 2023

Exposed SCADA Devices Trend

Xpanse SCADA and building control system fingerprinting improved during 2023, introducing a dramatic increase in tagged observations. This skew is noticeable from April 2023 onward in the figure 2 graph where new fingerprints increased monthly labeling significantly. We exclude the first quarter of 2023 in the trend analysis in figure 2 as the count of observations in those months cannot include the newer device fingerprints introduced in April 2023. After considering the new SCADA and BCS fingerprints, we observed a modest increase of these devices on the internet over time for the remainder of 2023.

Global Device Observations by Manufacturer and Product

The diagrams in figures 3–4 illustrate two metrics of observed OT devices by manufacturer and product. Figure 3 displays the unique hosts that are associated with each device by manufacturer.



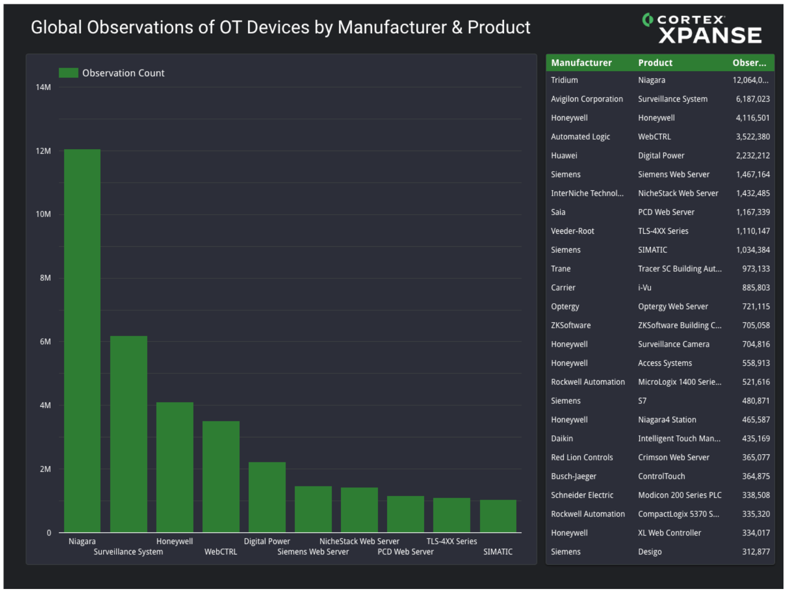
Manufacturer	Product	Hosts ▾
Tridium	Niagara	481,726
Huawei	Digital Power	123,951
Honeywell	Honeywell	79,123
Siemens	SIMATIC	75,333
InterNiche Technol...	NicheStack Web Server	67,894
Siemens	Siemens Web Server	58,963
Saia	PCD Web Server	55,850
Avigilon Corporation	Surveillance System	54,495
Veeder-Root	TLS-4XX Series	49,801
Schneider Electric	Modicon 200 Series PLC	37,518
ZKSoftware	ZKSoftware Building C...	35,875
Siemens	S7	25,007
Honeywell	XL Web Controller	24,577
Schneider Electric	Modicon M340 Proces...	19,257
Schneider Electric	Modicon M340 Series ...	18,102
Honeywell	Surveillance Camera	18,074
Automated Logic	WebCTRL	14,449
Siemens	Desigo	12,745
Rockwell Automation	MicroLogix 1400 Serie...	12,566
Daikin	Intelligent Touch Man...	11,730
Alstom	NetBox Train Control ...	11,380
Huawei	Smart Logger Ambien...	10,044
COPA-DATA France	Straton T5 Lighting	9,317
Trane	Tracer SC Building Aut...	8,842
Optergy	Optergy Web Server	7,863
Busch-Jaeger	ControlTouch	7,710

Figure 3: Unique hosts associated with each OT device by manufacturer

Figure 4 shows the daily observations of those same devices. This view shows the prevalence over time of devices as they respond to scans with “fingerprintable” responses.

The distinction between these two views is subtle but important. Unique host counts show how many distinct application servers were ever deployed to the public-facing internet over 2023, even if they occurred only once for a single day in that year. Alternatively, daily observation counts show a more operational and historical view of these devices. The counts here measure the frequency of which of these devices were exposed to the internet over time.

Some devices may have been deployed on more unique IP addresses, such as Huawei Digital Power appliances in figure 3, but overall were observed less over time, as seen in figure 4. From a surface level view, this implies that the digital power devices were only exposed to the internet for a comparatively short period of time, but on a wider scale than other popular devices.



Manufacturer	Product	Obser...
Tridium	Niagara	12,064,0...
Avigilon Corporation	Surveillance System	6,187,023
Honeywell	Honeywell	4,116,501
Automated Logic	WebCTRL	3,522,380
Huawei	Digital Power	2,232,212
Siemens	Siemens Web Server	1,467,164
InterNiche Technol...	NicheStack Web Server	1,432,485
Saia	PCD Web Server	1,167,339
Veeder-Root	TLS-4XX Series	1,110,147
Siemens	SIMATIC	1,034,384
Trane	Tracer SC Building Aut...	973,133
Carrier	i-Vu	885,803
Optergy	Optergy Web Server	721,115
ZKSoftware	ZKSoftware Building C...	705,058
Honeywell	Surveillance Camera	704,816
Honeywell	Access Systems	558,913
Rockwell Automation	MicroLogix 1400 Serie...	521,616
Siemens	S7	480,871
Honeywell	Niagara4 Station	465,587
Daikin	Intelligent Touch Man...	435,169
Red Lion Controls	Crimson Web Server	365,077
Busch-Jaeger	ControlTouch	364,875
Schneider Electric	Modicon 200 Series PLC	338,508
Rockwell Automation	CompactLogix 5370 S...	335,320
Honeywell	XL Web Controller	334,017
Siemens	Desigo	312,877

Figure 4: Daily OT device observations

Please note that some manufacturers develop application frameworks that are used by other organizations, the primary example in the above diagram being the Tridium Niagara Framework. This particular application server is frequently used by organizations to manage SCADA infrastructure even if the application itself is not a SCADA device.

Threats Inside OT Networks

We identified about 51,000 firewalls in OT networks by using App-ID over 2023. Palo Alto Networks App-ID is a traffic classification system available in the firewalls that determines what an application is irrespective of port, protocol, encryption (SSH or SSL), or any other evasive tactic used by the application. It applies multiple classification mechanisms—application signatures, application protocol decoding, and heuristics—to your network traffic stream to accurately identify applications. App-ID has different categories, one of which is the OT category that we used to identify the traffic. The OT category in App-ID contains an extensive list of known OT applications and protocols.

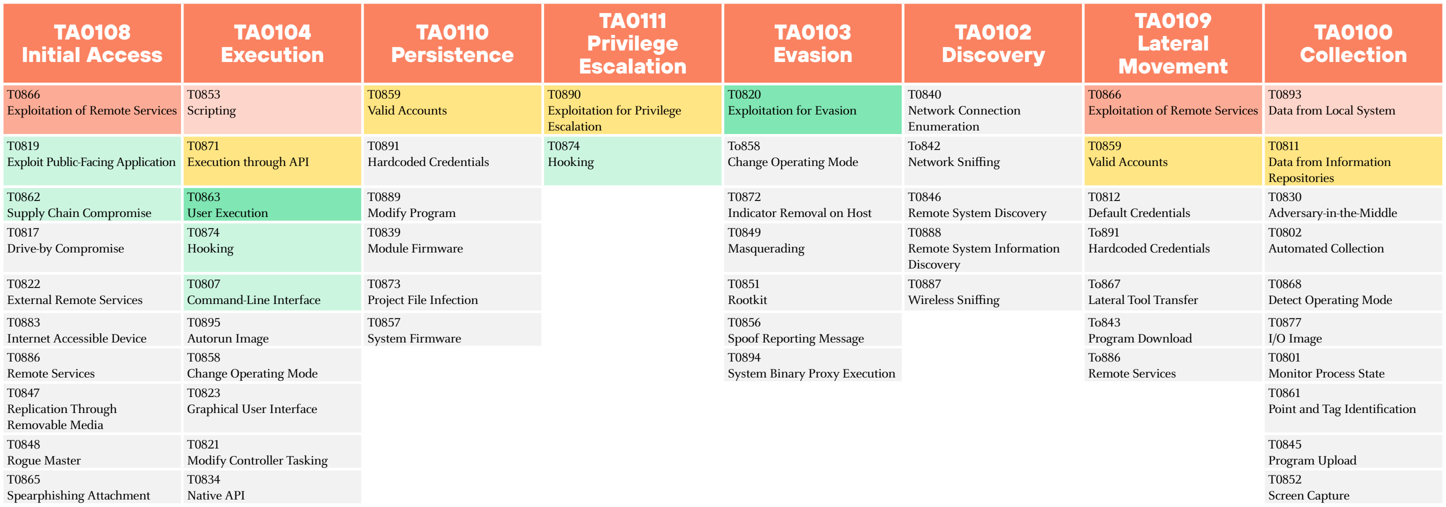
Most of these firewalls enabled threat detection tools like Threat Prevention and WildFire. Threat Prevention is IPS that includes comprehensive exploit, malware, and command-and-control protection and frequently publishes updates that equip the firewall with timely threat intelligence. Advanced WildFire detects and prevents zero-day malware using a combination of static and dynamic analysis and that of its Intelligent Run-time Memory Analysis engine to detect highly evasive threats and create protections to block malware.

After we identified the firewalls, we collected threat telemetries from them. The threat telemetries came from multiple sources, including Threat Prevention and WildFire. In the following sections, we will dive in the analysis of these threat telemetries to offer more insights on threats in OT systems.

Exploits Observed in OT Networks

This section provides an analysis of the top 100 exploit signatures gathered from firewalls within OT networks. The data has been mapped to the MITRE ATT&CK® Matrix for ICS and shows that most exploit attempts occur using five ATT&CK tactics: **Initial Access** [TA0108], **Execution** [TA0104], **Privilege Escalation** [TA0111], **Lateral Movement** [TA0109], and **Collection** [TA0100]. The key observations and potential implications for OT cybersecurity are detailed below.

🟥 Very high frequency 🟧 High frequency 🟨 Medium frequency 🟩 Low frequency ▨ Very low frequency



TA0108 Initial Access	TA0104 Execution	TA0110 Persistence	TA0111 Privilege Escalation	TA0103 Evasion	TA0102 Discovery	TA0109 Lateral Movement	TA0100 Collection
🟥 T0866 Exploitation of Remote Services	🟧 T0853 Scripting	🟨 T0859 Valid Accounts	🟨 T0890 Exploitation for Privilege Escalation	🟩 T0820 Exploitation for Evasion	T0840 Network Connection Enumeration	🟥 T0866 Exploitation of Remote Services	🟧 T0893 Data from Local System
▨ T0819 Exploit Public-Facing Application	🟨 T0871 Execution through API	T0891 Hardcoded Credentials	▨ T0874 Hooking	To858 Change Operating Mode	To842 Network Sniffing	🟨 T0859 Valid Accounts	🟨 T0811 Data from Information Repositories
▨ T0862 Supply Chain Compromise	🟩 T0863 User Execution	T0889 Modify Program		T0872 Indicator Removal on Host	T0846 Remote System Discovery	T0812 Default Credentials	T0830 Adversary-in-the-Middle
T0817 Drive-by Compromise	▨ T0874 Hooking	T0839 Module Firmware		T0849 Masquerading	T0888 Remote System Information Discovery	To891 Hardcoded Credentials	T0802 Automated Collection
T0822 External Remote Services	▨ T0807 Command-Line Interface	T0873 Project File Infection		T0851 Rootkit	T0887 Wireless Sniffing	To867 Lateral Tool Transfer	T0868 Detect Operating Mode
T0883 Internet Accessible Device	T0895 Autorun Image	T0857 System Firmware		T0856 Spoof Reporting Message		To843 Program Download	T0877 I/O Image
T0886 Remote Services	T0858 Change Operating Mode			T0894 System Binary Proxy Execution		To886 Remote Services	T0801 Monitor Process State
T0847 Replication Through Removable Media	T0823 Graphical User Interface						T0861 Point and Tag Identification
T0848 Rogue Master	T0821 Modify Controller Tasking						T0845 Program Upload
T0865 Spearphishing Attachment	T0834 Native API						T0852 Screen Capture

Figure 5: MITRE ATT&CK® Matrix for ICS

The **Initial Access** tactic encompasses methods that attackers employ to breach a network for the first time. It was observed that the **Exploitation of Remote Services** [T0866] technique, accounting for 20.0% of incidents, is the predominant method used by malicious actors to gain initial entry. Attackers exploit software vulnerabilities caused by programming errors in applications, services, or even within either the operating system's software or kernel to manipulate remote services. After finding a way in through a vulnerable remote system, attackers facilitate **Lateral Movement** within the OT environment seeking access to high-impact assets like a data historian, workstation, VPN server, or HMI.

Two known prominent cyberattack incidents have utilized this technique. In 2017, this technique was used to deploy the **Bad Rabbit** [S0606] ransomware to attack Ukraine and Russia. Although initially infecting IT networks, Bad Rabbit was spread to OT networks through the MS17-010 exploit that targeted SMBv1. The other significant cyberattack that used this technique is the well-known **Stuxnet** [S0603] campaign.

The **Execution** tactic allows adversaries to run malicious code on a victim's system, leading to potential data breaches, system compromises, and further exploitation. The **Scripting** [T0853] technique was the most used within this tactic, accounting for 13.5% of the top 100 exploit incidents. With this technique, attackers utilize scripting languages to execute arbitrary code by either predesigned scripts or inputting code directly. Once an attacker is inside an environment, they can weaponize code in real time to be deployed on a target device to execute tasks on servers, data gateways, HMIs, and workstations.

Examples of this technique in use include the **Triton Safety Instrumented System Attack** [C0030], first discovered in 2017 and executed by the Russian-based threat group **TEMP.Veles** [G0088]. The group used the PowerShell tool WMImplant to facilitate lateral movement.[1] More recently, the **Sandworm Team** [G0034] used the **Scripting** technique as part of their **2022 Ukraine Electric Power Attack** [C0034]. They used a Visual Basic command against a MicroSCADA supervisory control system.[2]

Just as **Scripting** utilizes programming or services errors, **Privilege Escalation** can also be accomplished through software vulnerabilities. Performing **Privilege Escalation** is often essential for bad actors to access protected resources and functionalities within a target system or network that are otherwise restricted. Representing 12.3% of the top 100 exploit incidents, the main technique observed to achieve this is **Exploitation for Privilege Escalation** [T0890]. If successful, an attacker with root permissions could wreak havoc in an OT environment by modifying or disrupting operation sequences for safety systems or control logic on programmable logic controllers (PLCs), or gain access to sensitive information such as production schedules, formulas, or design specifications on the data historian.

The **INCONTROLLER** [S1045] malware can achieve **Privilege Escalation** by exploiting a vulnerable driver on Omron and Schneider Electric PLCs, and the OPC UA, Modbus, and CODESYS protocols. While there are no known reports of **INCONTROLLER** being used in the wild as of publication, the risk is still prevalent on unpatched systems.

[1] FireEye Intelligence, "TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers," Google Cloud Blog, October 23, 2018.

[2] Ken Proska et al., "Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology," Google Cloud Blog, November 9, 2023.

Cyberattacks are complex operations; therefore, some ATT&CK techniques fall within multiple tactics. So is the case with the **Exploitation of Remote Services** used for **Lateral Movement** as well as **Initial Access**. **Lateral Movement** is a malicious actor moving throughout the OT network as they pivot from one device to another. Attackers use techniques in the **Discovery** [TA0102] and Collection tactics to determine which devices to target. With the correct privileges, an adversary can move freely within the OT network to valuable assets like engineering workstations, routers, HMIs, application and control servers, and safety controllers.

The **Bad Rabbit** ransomware uses **Exploitation of Remote Services** to self-propagate through a network by exploiting the SMBv1 protocol. The protocol was designed to allow devices to communicate with each other and share data. If exploited for malicious purposes, an attacker or malware can move throughout a network to any device that is open to this protocol. Additionally, **Volt Typhoon** [G1017] is known to utilize **Exploitation of Remote Services** to accomplish **Lateral Movement** by employing RDP in a suspected attempt to pivot to OT devices.[3]

As mentioned above, the **Collection** tactic is used to gather information about the OT environment, from operation states and IP addresses to network topology and more. To collect this data, exploits that perform the **Data from Local System** [T0893] technique were the second-highest number observed, at 18.9% of the top 100. Bad actors use this technique to target local OT system resources like HMIs, data historians, jump hosts, and workstations to collect data from databases or systems and configuration files.

In one **Volt Typhoon** compromise, OT asset diagrams and documentation regarding relays, SCADA systems, and switchgear were collected from a local file server. The data was then exfiltrated via SMB back to the adversaries.[4]

[3] "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," Canadian Centre for Cyber Security, February 7, 2024.

[4] Ibid.

Exploited CVE Age in OT Networks

While analyzing the top 100 exploits, we examined the ages of the CVEs that correlated with the exploit signatures identified within OT networks.

The data represented in figure 6 indicates that CVEs aged between six and 10 years account for the highest percentage of signature triggers at 61.9%. It makes sense to conclude that threat actors continue to use older exploits because they get good results from them. This suggests that older exploits have a considerably higher success rate in OT environments.

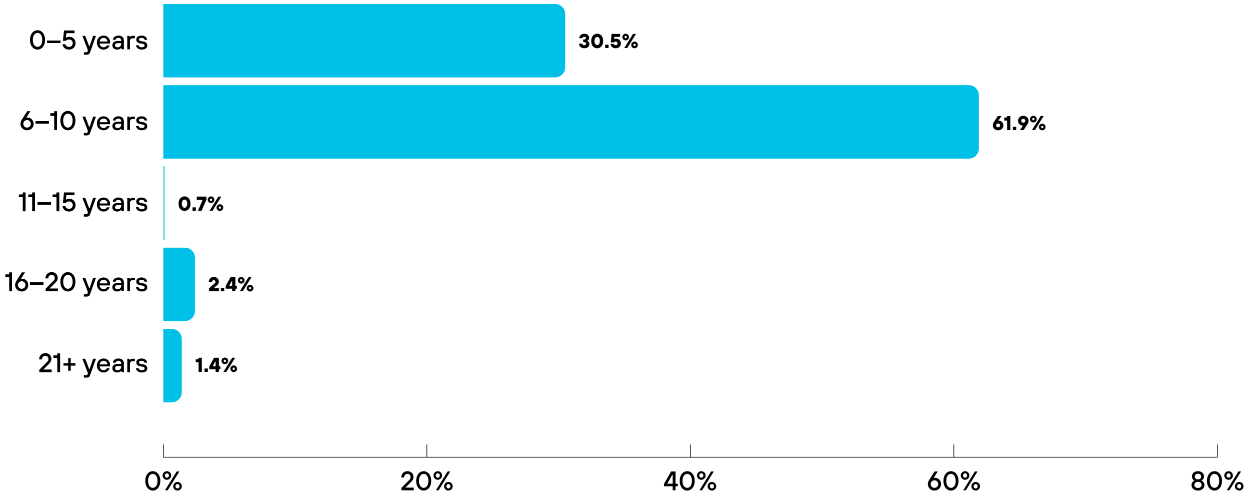


Figure 6: OT network CVE age

We know the use of older exploits in OT networks is largely driven by the combination of these systems being slow to update, operating with legacy technology, and having complex operational requirements that limit rapid changes, plus the economic considerations of replacing aging infrastructure. For that set of reasons, we are seeing CVEs more than 20 years old. While 1.4% of the total might not seem like a large number, consider that it equates to about 42,000,000 exploit instances being recognized within OT networks around the globe and came from only seven CVEs: CVE-1999-262, CVE-2000-0208, CVE-2000-0884, CVE-2000-0886, CVE-2001-0537, CVE-2002-0563, CVE-2002-1042.

Exploit Trend over Time

The data presented illustrates the monthly percentage difference between OT attack averages and the overall attack averages across a calendar year in 2023. Notably, OT attacks exhibited significant fluctuations compared to the overall attack averages. In June and July, OT attacks were approximately 30% and 36% higher, respectively, than the average of all attack types, indicating a substantial increase in targeted activity within OT systems during these months. Conversely, in May and August, OT attack averages were approximately 7% and 19% lower, respectively, than the overall attack averages, suggesting a relative decrease in OT-specific attacks during these periods. December also stands out, when, despite a moderate level of OT attacks, the overall attack average surged by about 138%, reflecting a broader increase in cyberthreats that extended beyond OT environments. These percentage differences highlight the dynamic and varying nature of cyberthreats targeting OT systems, emphasizing the need for continuous monitoring and adaptive security measures.

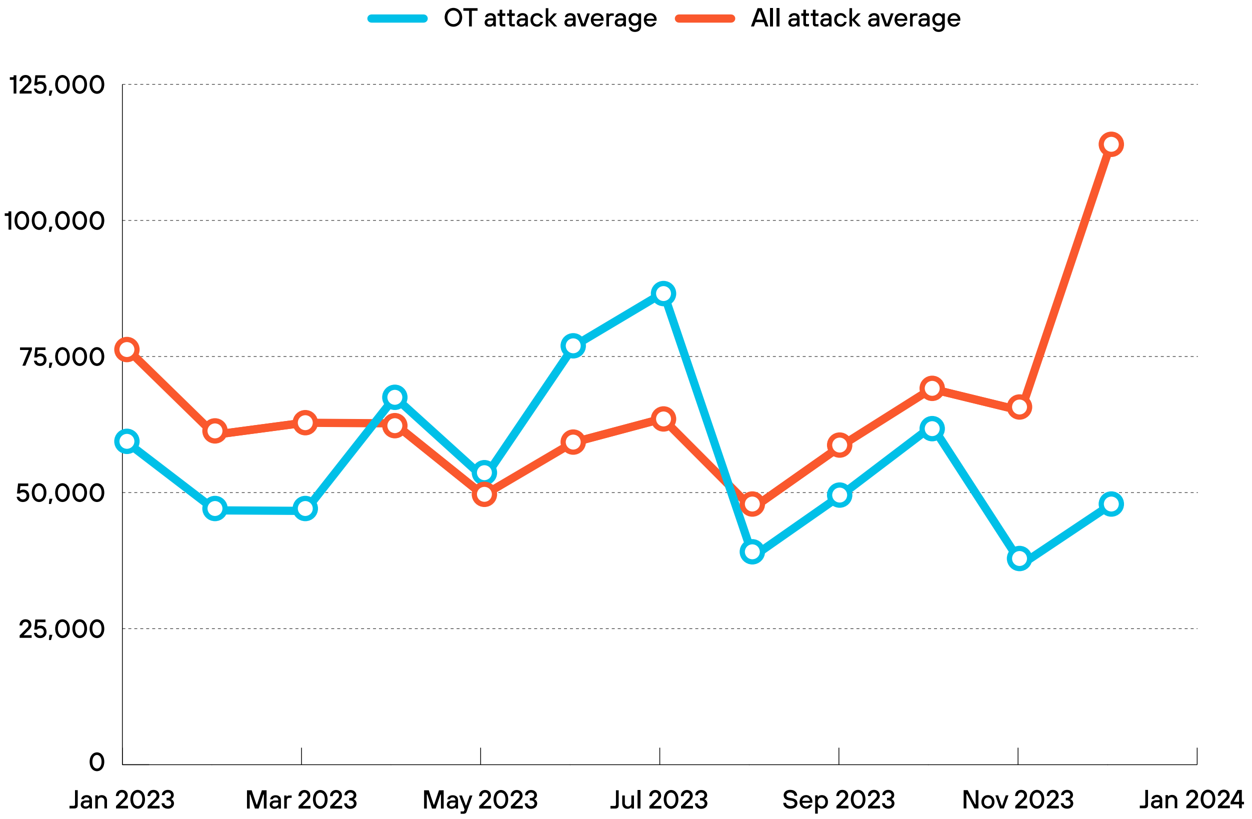


Figure 7: OT attack averages compared to overall attack averages in 2023

Exploits Observed Against the OT/ICS Industries: A Focused Analysis

In the increasingly vulnerable landscape of operational technology and industrial control systems (ICS), understanding the nature and distribution of cyberthreats is critical. This report provides an in-depth analysis of exploit attempts observed against these industries, focusing on inbound and internal network traffic. The analysis highlights the most impacted industries in each traffic category, along with the most common exploits observed, offering valuable insights into the cybersecurity challenges facing OT and ICS environments.

Internal Traffic: Vulnerabilities Within the Network

Internal Traffic Overview

Internal traffic involves data packets that originate and terminate within the same network, typically between private IP addresses within corporate and OT environments. Exploits observed in this traffic type often indicate that internal systems have been compromised, with attackers attempting to achieve persistence, collect data, or execute further attacks.

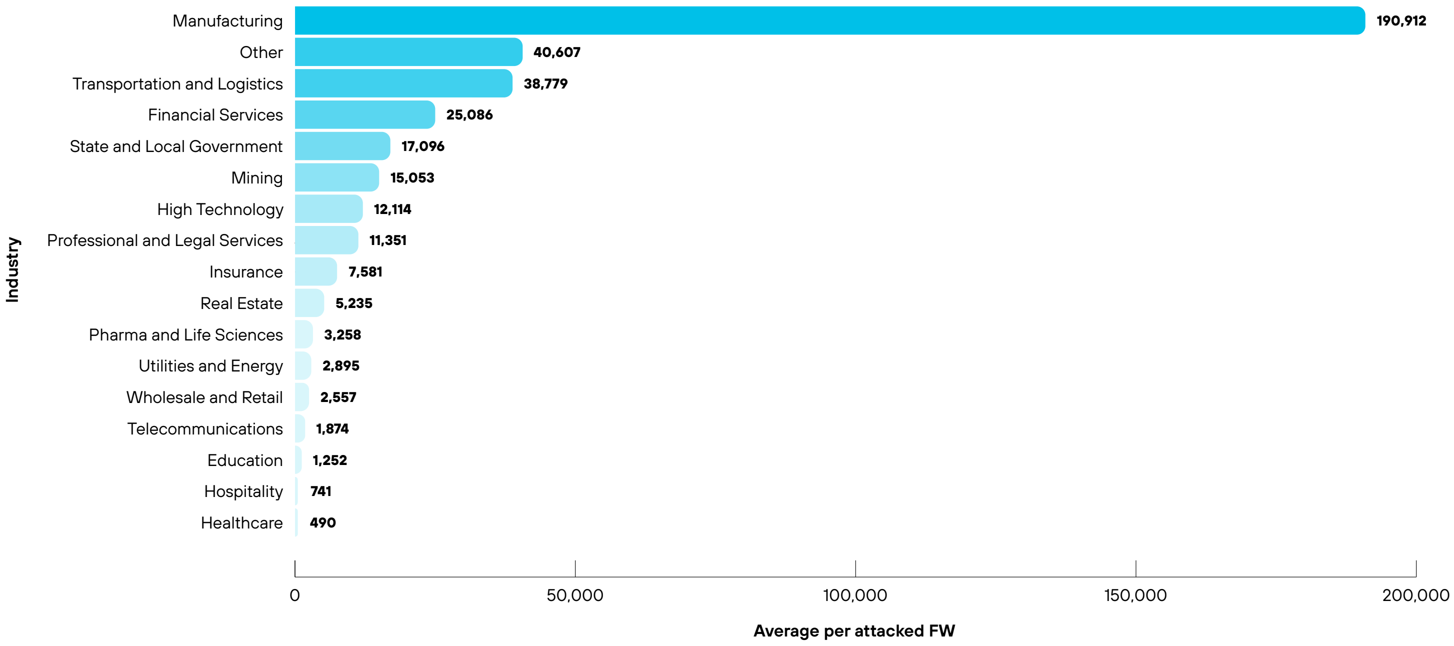


Figure 8: Average per attacked FW vs. industry

Most Impacted Industries

- **Manufacturing (82.7% of total internal exploit attempts)**:
  - **Prominent tactics**: Persistence [TA0110], Collection [TA0100]
  - **Preferred techniques**: Valid Accounts [T0859], Data from Local System [T0893], Data from Information Repositories [T0811]
  - **Common exploits**: HTTP /etc/passwd Access Attempt, HTTP directory traversal, HTTP SQL injection
  - **Threats**: The manufacturing sector's reliance on interconnected processes, machines, and systems increases the risk of internal exploits. Legacy systems and the convergence of IT and OT networks further exacerbate these vulnerabilities, making them prime targets for internal attacks.

OT-Specific Exploits

To this point, the exploits analyzed have lacked OT specificity. That is because the vast majority of the exploits detected in OT networks continue to be IT centric. In fact, only 1.0% of all the exploits detected in 2023 were specific to only OT. Expanding the dataset to include exploits that share OT and IT signatures, the percentage of detections increases to 35.0%.

The top three ATT&CK tactics for the observed OT-specific exploits are **Execution** [TA0104], **Inhibit Response Function** [TA0107], and **Collection** [TA0100]. The top techniques for each respective tactic are **Command-Line Interface** [T0807], **Denial of Service** [T0814], and **Adversary-in-the-Middle** [T0830]. The exploits falling under these tactics account for 94.4% of all the OT-specific exploit detections.

The fourth-most prominent technique is **Exploitation of Remote Services** [T0866], accounting for 3.5% of detections. As described above, this technique falls under two tactics: **Initial Access** [TA0108] and **Lateral Movement** [TA0109]. The drop-off in detection percentage appears significant in that it could signal bad actors have already established a foothold deep in the OT network and do not need to create access, and only move minimally between devices. Because of the large percentage from the top three techniques, the data could indicate that adversaries have attained local access, are interacting with devices on their CLI, are hard at work disrupting device functionality, and are possibly modifying network traffic to cover their tracks.

OT-specific exploits

IT-/OT-specific exploits

Total attacks in OT environment

Malware Analysis

In this section, we have divided the analysis into two sections. First, we focused on all the malware detected in 2023 for all firewalls in the OT networks. Next, we focused the analysis on only malware moved over OT ports.

Analyzing All Malware from OT Networks

Geographical Analysis

In 2023, malware detection rates varied significantly across countries, highlighting disparities in cybersecurity infrastructure and threat exposure. The Netherlands and the United States reported the highest averages, with 1,536 and 1,046 detections, respectively. This likely reflects their advanced digital infrastructures and robust monitoring systems, capable of detecting a wide range of malware. In contrast, countries such as Bulgaria, China, and Russia showed moderate detection rates, which may indicate either different cybersecurity challenges or variations in detection capabilities. The lower detection rates observed in countries like Brazil and India could suggest gaps in their cybersecurity frameworks, underreporting, or less aggressive targeting by cyberthreats.

Interestingly, several countries, including Malta and the Åland Islands, reported minimal malware detections, potentially due to smaller digital footprints or effective preventive measures, though this might also indicate underreporting. The overall disparity in malware detection underscores the need for international collaboration in cybersecurity. Developing nations, in particular, could benefit from shared intelligence and resources from countries with more advanced cybersecurity systems. Standardizing threat detection and reporting on a global scale is essential to ensure all countries can adequately defend against the growing sophistication of cyberthreats.

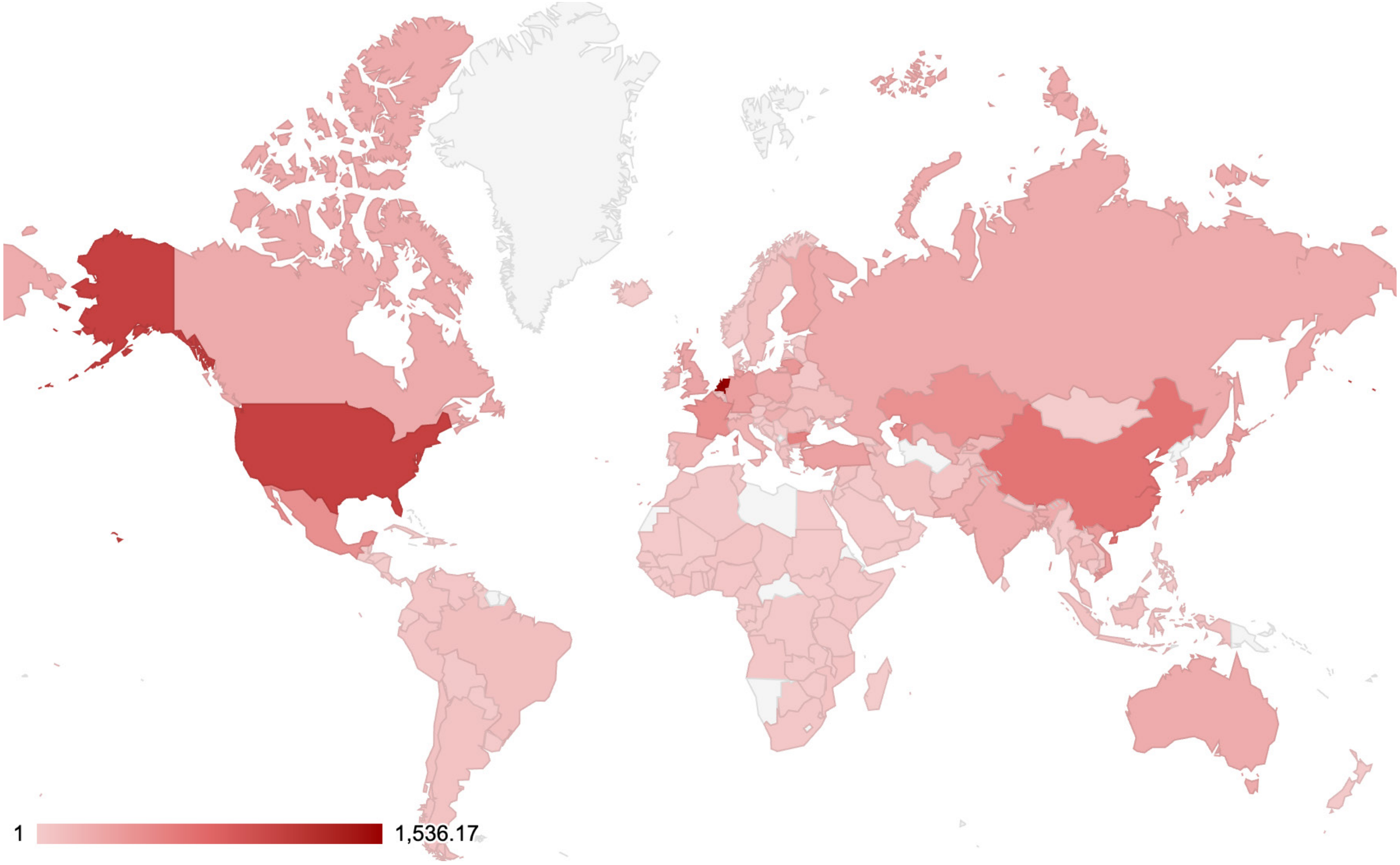


Figure 9: Global malware detection rates

Industrial Analysis

The analysis of average malware detections across ICS industries in 2023 highlights significant cybersecurity risks in certain sectors. The federal government sector led with 22.8% of the total malware detections, underscoring its vulnerability to cyberthreats, likely due to the critical nature of its operations and data. The hospitality industry followed closely, representing 12.5% of detections, reflecting the high exposure of this sector to cyberattacks, given its reliance on customer-facing technologies.

Manufacturing, a key component of ICS, accounted for 2.9% of the total malware detections. While this percentage is lower compared to the government and hospitality sectors, it still indicates a substantial risk, especially considering the potential impact of disruptions in manufacturing processes. The data suggests that industries integral to national infrastructure, such as government and manufacturing, are particularly at risk, necessitating enhanced cybersecurity measures to protect these critical systems from evolving threats.

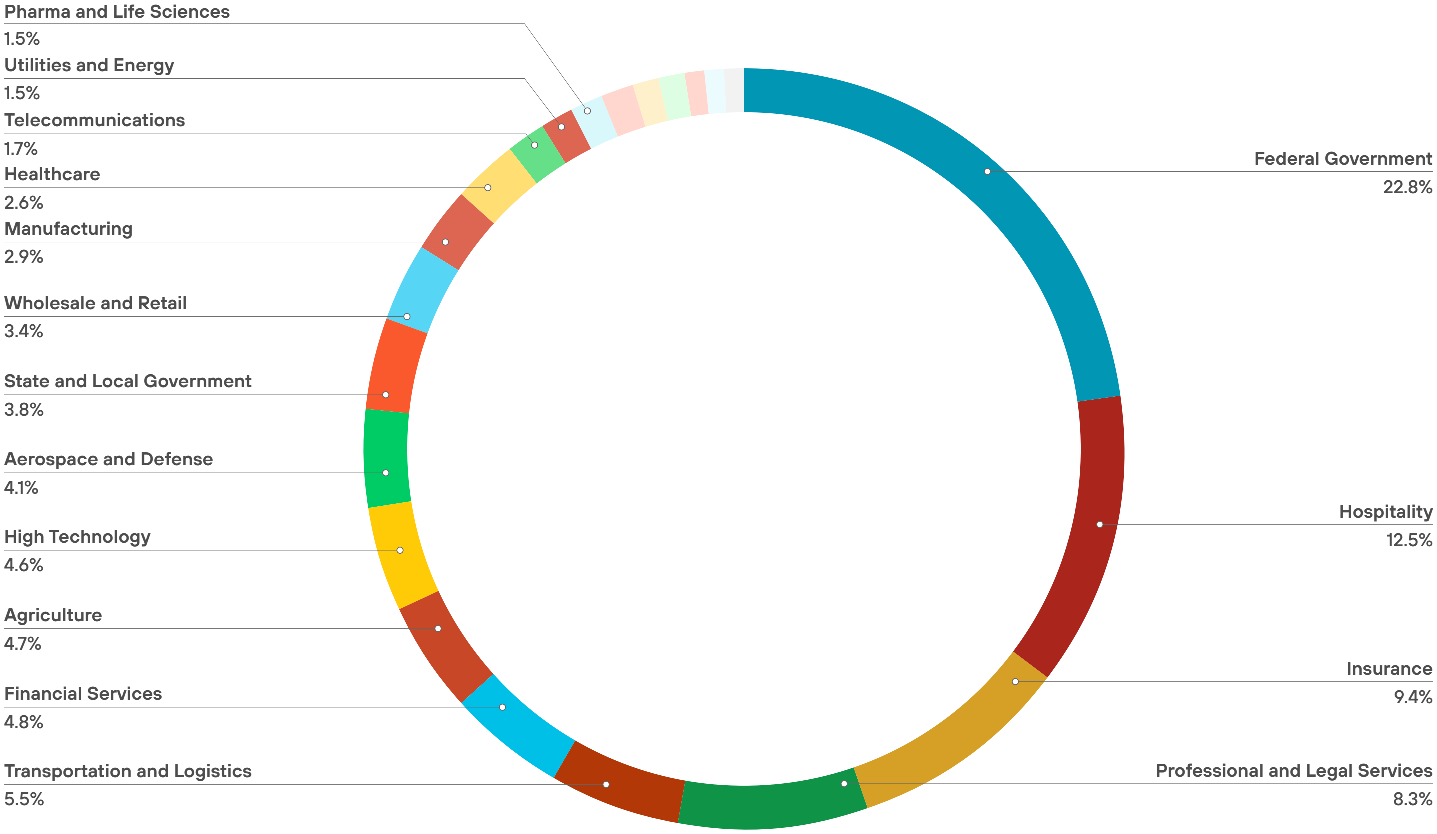


Figure 10: Malware detection across ICS industries

Analyzing Malware by OT Network Port

This analysis examines malware detections in 2023 related to OT network ports and protocols. Two datasets were used: the first contains OT-specific network port numbers and associated protocols, while the second lists malware incidents detected across different industries linked to these OT ports. By merging the two datasets based on port numbers, the study investigates the types of malware targeting OT systems, focusing on their distribution across industries and protocols.

In the analysis of detected malware types in 2023, the largest proportion of threats was categorized as "**unknown**," comprising 78.4% of the total detections. **Trojans** and **ransomware** were next in prevalence, each accounting for 9.1% of the total malware, while **adware** made up 2.5%. Less common threats included exploits (0.11%), viruses (0.05%), potentially unwanted applications (PUAs) (0.02%), riskware (0.02%), potentially unwanted programs (PUPs) (0.02%), phishing (0.01%), and grayware (0.004%). The high percentage of "unknown" malware highlights the growing challenge of identifying novel or previously unseen threats in cybersecurity systems. Trojan accounted for approximately 77% of all malware families, ransomware for 10%, and adware and exploit together contributed around 7% of the total detected malware families.

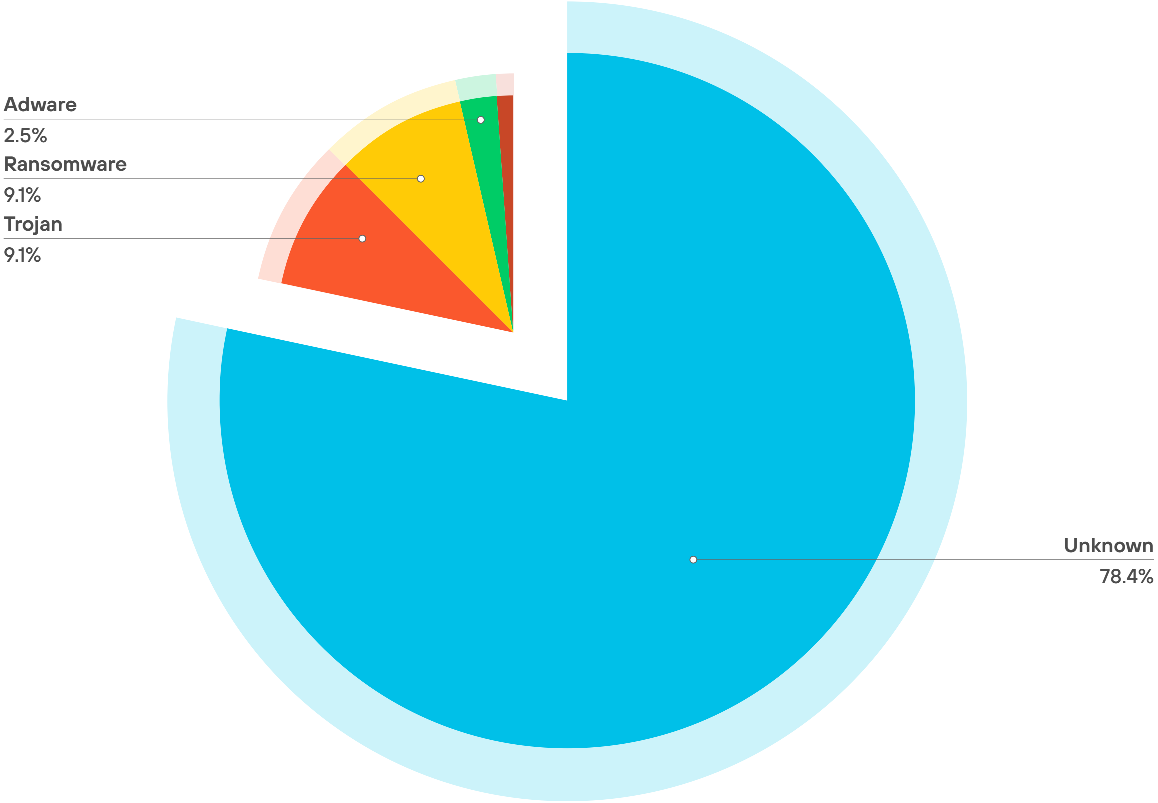
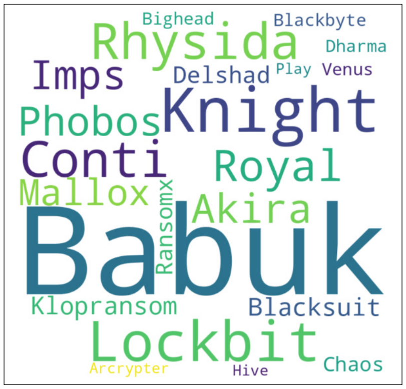


Figure 11: Malware types detected in 2023

Analysis of Ransomware in 2023 (Associated with OT Ports)

The analysis of ransomware in 2023 reveals key insights into the malware families, targeted OT protocols, and affected industries. Ransomware accounts for 10.2% of all malware families detected, making it one of the most significant threats in the dataset.



Most Common Ransomware Families

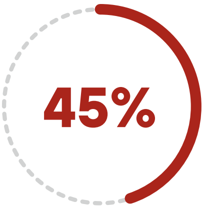
The most frequently detected ransomware families include Babuk and LockBit. Dominating ransomware detections, especially in the wholesale and retail sector, Babuk was the most prominent family. Another notable ransomware family, LockBit primarily affects the manufacturing industry. These ransomware families have been linked to attacks that focus on encrypting critical systems and demanding ransom payments, with Babuk leading by a considerable margin.

Analysis of "Unknown" Malware

The **unknown** malware type consists of files deemed malicious but that have not been identified, which means the malware is either new or a new variant of known malware. This analysis provides a detailed look into the most impacted port numbers, protocols, and industries, highlighting the areas where unknown malware poses the highest risks.

Statistical Analysis of Impacted Port Numbers and Protocols

Among the ports targeted by the unknown malware type, Port **50004 (TCP)** emerges as the most impacted, accounting for approximately **45%** of the total occurrences in the dataset. This port is commonly associated with critical OT systems. **Ports 50110 (TCP)** and **50001 (TCP)** are also notably affected, with **15%** and **10%** of unknown malware detections linked to these ports, respectively. These ports are commonly used for communication in SCADA and ICS environments, indicating that these systems are being targeted by undefined threats. The distribution across these ports highlights that **TCP-based protocols** are particularly vulnerable to attacks by unknown malware, suggesting the need for improved security measures on these essential OT ports.



Port 50004 (TCP)

Port 50110 (TCP)

Other ports, such as **56015 (TCP)** and **56010 (TCP)**, show smaller impacts, with **5–8%** of detections attributed to them. These ports are primarily used in retail and logistics systems, which may explain their smaller yet significant exposure to this malware type.

The **unknown** malware type disproportionately affects **state and local government** OT systems, with **Port 50004 (TCP)** being the most frequently targeted, making up nearly **45%** of the total detections. **Ports 50110** and **50001 (TCP)** also show substantial impacts, emphasizing the vulnerability of SCADA and ICS systems to these undefined threats. While the **wholesale and retail** sectors are less affected, they still face risks on ports like **56015** and **56010 (TCP)**. This analysis underscores the need for more stringent security measures on vulnerable TCP-based protocols, particularly in the government and retail sectors, to protect against unknown and evolving malware threats.

Port 50001 (TCP)

Solutions and Recommendations

The scale and sophistication of threats targeting OT environments, such as exploitation of legacy vulnerabilities and unknown malware, highlight the growing risks to critical operations. With millions of exposed OT devices (46.2 million observations of OT devices publicly exposed to the internet in 2023, as per Xpanse report) and attackers leveraging outdated protocols, organizations may feel overwhelmed about where to begin their security journey. Understanding the threat landscape and effectively implementing security controls might be challenging for organizations.

We recognize these challenges and provide a **Siemens Foundation of Industrial Security Concept**, a comprehensive approach to addressing OT security concerns. This framework is built around three critical pillars: **plant security**, **network security**, and **system integrity**, all aligned with the globally recognized **IEC 62443 standard** for industrial automation security. These pillars consider all key factors, including physical access protection and organizational measures such as guidelines and processes as well as technical measures to protect networks and systems against unauthorized access, espionage, and manipulation. Implementing security measures at multiple layers and the combined effect of different protective measures provide a high degree of security, reducing the risk of successful attacks and ultimately improving plant availability and productivity.

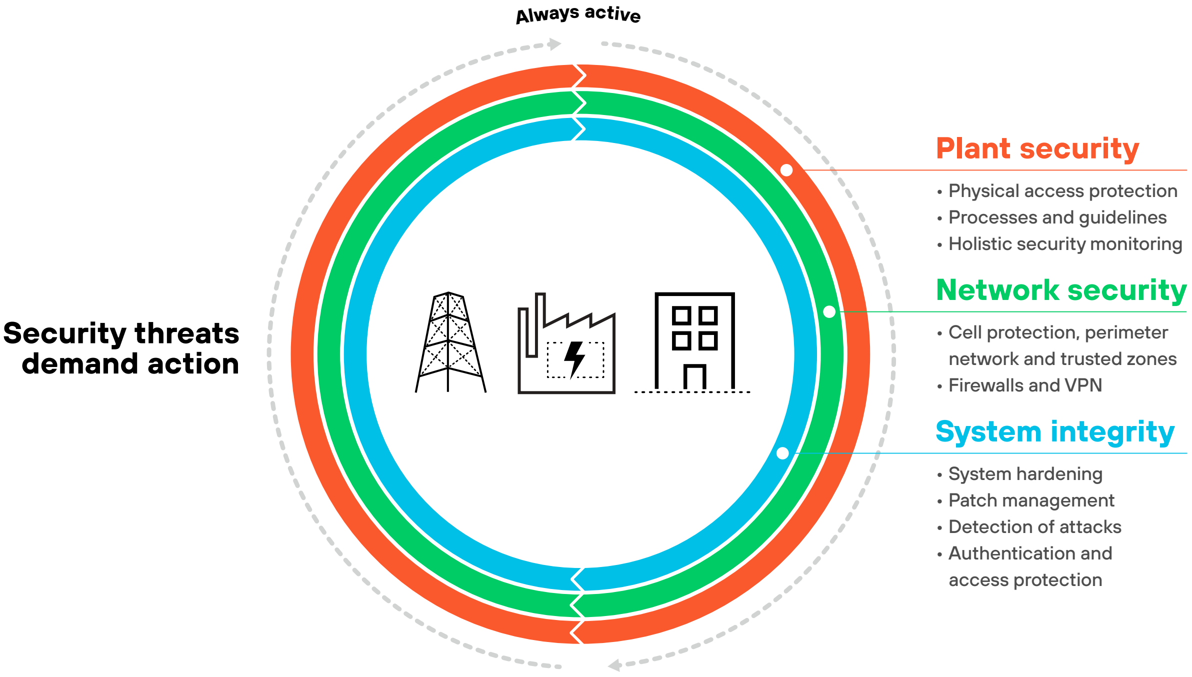

Always active
Security threats demand action
Plant security
• Physical access protection
• Processes and guidelines
• Holistic security monitoring
Network security
• Cell protection, perimeter network and trusted zones
• Firewalls and VPN
System integrity
• System hardening
• Patch management
• Detection of attacks
• Authentication and access protection

Figure 12: Siemens industrial security concept foundation

In this whitepaper, we **focus on network security**, a cornerstone of protecting OT environments. Read *Cybersecurity for Industry* for further information about the full Siemens Foundation of Industrial Security Concept.

Focus Highlight with Network Security

Securing industrial networks is paramount to safeguarding OT environments. To achieve robust protection, OT networks must be **logically and physically separated** from external networks, including corporate IT systems and the internet. Direct connections to industrial systems pose a significant risk, as they can be exploited by threat actors. Effective management of these connections is critical to minimizing vulnerabilities.

Securing Interfaces to Other Networks

Interfaces to other networks are protected by using **firewalls** and implementing a **demilitarized zone (DMZ)**. A DMZ, protected by firewalls, serves as a controlled interface for secure communication between OT networks and external systems, including the IT or enterprise environment. It can host essential services such as remote access, data exchange, and update servers, ensuring critical OT systems are not directly exposed to the internet. A DMZ is typically designed so that it also does not permit to access the automation network, which means that the automation network remains protected even is an attacker gains control of a system inside the DMZ.

Network Segmentation with Automation Cells

To further enhance network security, OT environments should be segmented to create **separated automation cells** protected by technical security mechanisms. The devices within a segmented cell are protected against unauthorized access from outside without the need for any compromise in terms of real-time capability, performance or other functions. If an attacker compromises a system within one cell, they are contained, reducing the overall impact. It is important to:

- Control access attempts to and from the cell on a need-to-connect basis.
- Stipulate which network nodes are permitted to communicate with each other and, where appropriate, which protocols are allowed to use.

This means that unauthorized access attempts can be blocked, first and foremost, and also makes it possible to reduce the network load, as only those communications that are explicitly desired and permitted are able to proceed.

Figure 13 represents a multilayered architecture for an industrial control system (ICS) that integrates IT and OT. Firewalls and segmented networks ensure secure communication and prevent unauthorized access between these layers. At the lowest levels, Layers 2 down to 0 **(L2-0)**, the architecture integrates physical equipment like Programmable Logic Controllers (PLCs) and Human-Machine Interfaces (HMIs), which interact directly with the industrial processes. **Level 3 (L3)** is the OT zone, comprising operational functional areas (e.g., Functional Areas 1-4) for critical OT operations like production control, supported by shared **Common Services**. **Level 4** represents enterprise IT systems, such as corporate networks, separated from operational networks by an IT/OT demilitarized zone (L3.5), which includes **Infrastructure DMZ** and **Access DMZ** for secure cross-domain communications. The **Infrastructure DMZ** enables secure data exchange and shared services between IT and OT networks, ensuring segmentation. The **Access DMZ** provides controlled remote access to the OT network via VPNs or jump servers, safeguarding critical operations. At the top, **Level 5 (L5)** connects to the **cloud/internet**, providing SaaS/IaaS services, and is separated from enterprise IT (**L4**) through security firewalls.

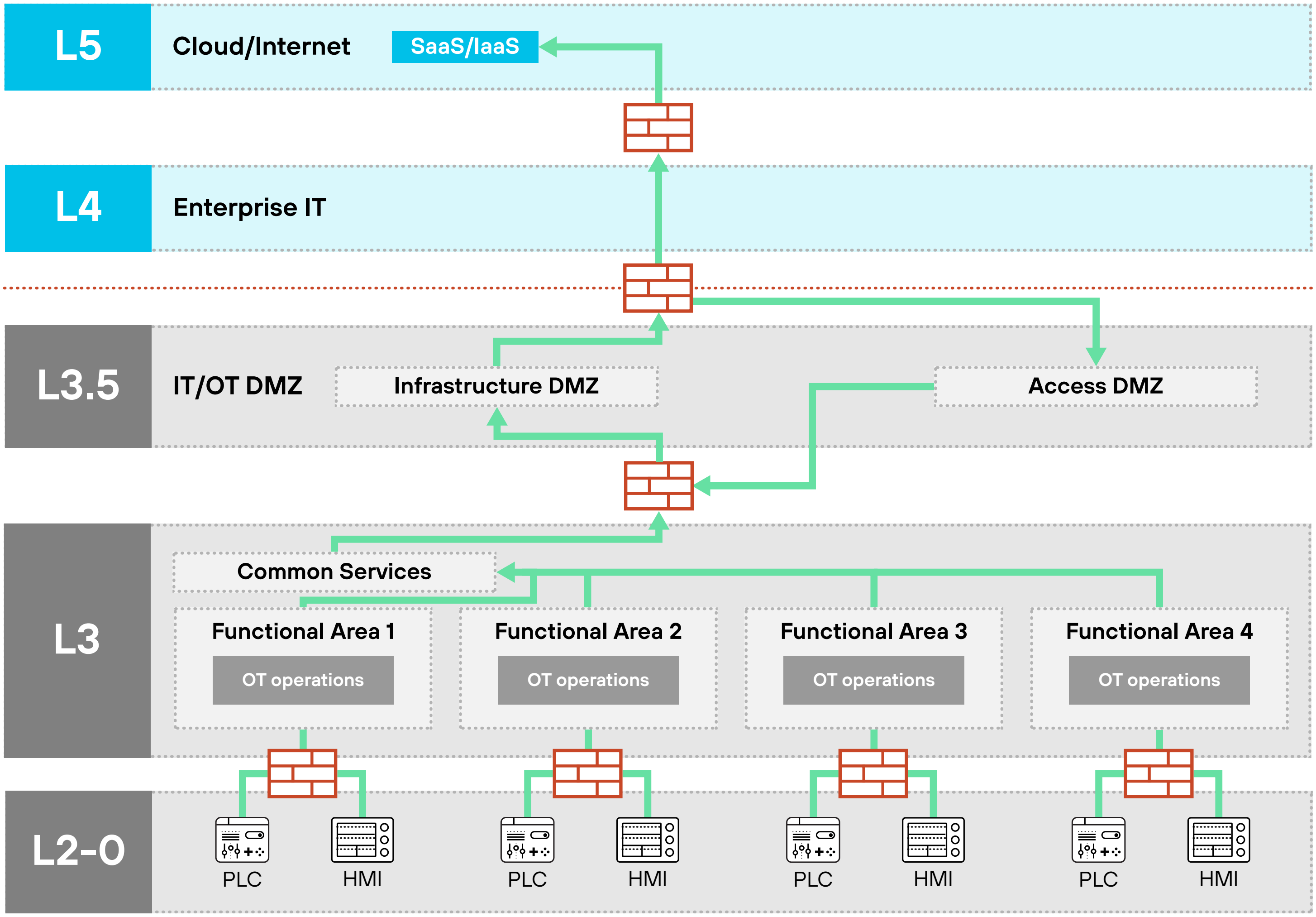


Figure 13: Industrial network reference architecture

Securing Remote Access

As OT operations advance, remote access to industrial networks becomes necessary for configuration, maintenance, and updates. Secure remote access measures include:

- Using **VPN tunnels** with robust authentication and authorization controls.
- Strategically deploying a **separate domain controller (DC)** from corporate IT Active Directory to prevent two-way trust vulnerabilities.
- Utilizing **jump hosts** to provision tools and enforce strict authorization for remote tasks.

Reflecting on Your OT Security Posture

As the OT threat landscape evolves, securing industrial networks is no longer optional—it is a necessity. The findings in this whitepaper and the recommended solutions highlight the urgent need for organizations to adopt a proactive and layered approach to cybersecurity. By leveraging frameworks like the **Siemens Foundation of Industrial Security Concept**, organizations can build resilient defenses tailored to their unique operational challenges.

To guide your organization's journey toward stronger OT security, consider these critical questions:

- **Network Separation and Segmentation**
  - Have you effectively separated your OT networks from external networks, including corporate IT and the internet?
  - Is your industrial network segmented into automation cells to contain potential breaches and minimize their impact?
- **Remote Access Security**
  - Do you have secure remote access controls in place, such as VPNs and jump hosts, to protect against unauthorized access?
  - Is your OT domain controller independent of your corporate Active Directory, ensuring no two-way trust vulnerabilities?
- **External Footprint and Exposure**
  - Have you conducted a comprehensive assessment of your OT devices' external footprint to identify public-facing or internet-accessible systems?
  - Are legacy systems that don't require external access disconnected, and are necessary internet-facing systems secured with firewalls and DMZs?
- **Patching and Monitoring**
  - Are you operationalizing a robust patch management program to address vulnerabilities in both legacy and modern systems?
  - Do you have continuous monitoring systems to detect and respond to emerging threats in real time?
- **Cultural and Strategic Readiness**
  - Do you perform regular security assessments for your OT environment?
  - Are your employees equipped with the training and awareness to recognize and respond to potential security threats?
  - Is your organization leveraging the latest threat intelligence and best practices to continuously refine your security posture?

By addressing these questions, you can evaluate your current OT security measures and identify areas that require immediate attention. A proactive, adaptive approach will not only mitigate risks but also safeguard your operations against the challenges of an ever-changing cybersecurity landscape. The journey to resilient OT security starts with the questions you ask today.

Data Methodology

This whitepaper combines data from Palo Alto Networks **Cortex Xpanse Internet Landscape Intelligence (ILI)** and telemetry from OT firewalls to analyze exposed SCADA and OT devices on the internet. The study's core methodology relies on **daily scans of IPv4 and IPv6 spaces**, using enhanced fingerprinting techniques to identify over **1.25 million unique IP addresses** and **4.53 million unique OT devices over those IP addresses and various ports globally**. This fingerprinting process improved significantly in **March–April 2023**, leading to a noticeable increase in detected devices, which skews early 2023 data and necessitates its exclusion from trend analysis.

Data was also gathered from **51,000 firewalls in OT networks using App-ID**, Palo Alto Networks' traffic classification tool, providing granular insights into OT applications. Threat detection tools such as **WildFire** and **Threat Prevention** were utilized to analyze malware, zero-day threats, and exploits in OT networks.

The geographical analysis highlights disparities between regions, where countries with advanced cybersecurity infrastructure, such as the U.S. and the Netherlands, reported higher detection rates due to **better visibility**, while regions like Brazil and India showed fewer detections, likely due to **weaker cybersecurity frameworks**. Industry-specific analysis revealed that the **manufacturing**, **energy**, and **retail** sectors were most affected by OT-targeted threats, though the data may be biased toward industries with better detection systems.

Analysis Biases

The analysis is influenced by several biases:

1. **Fingerprinting improvements**: The significant improvements in fingerprinting in Q2 2023 skew data trends, leading to inflated device counts after March 2023.
2. **Reliance on Palo Alto Networks tools**: The use of proprietary Palo Alto Networks tools, including App-ID and WildFire, introduces bias toward threats best detected by these technologies, potentially missing other threat vectors.
3. **Geographical and industry disparities**: Regions and industries with advanced cybersecurity practices report more threats, creating bias toward these areas, while less-developed regions or sectors may underreport incidents due to weaker detection capabilities.

Despite these biases, the data provides valuable insights into the growing risks and vulnerabilities facing **exposed OT systems**, underscoring the importance of **continuous threat monitoring and adaptive security strategies**.

About Palo Alto Networks

Palo Alto Networks is the global cybersecurity leader, committed to making each day safer than the one before with industry-leading, AI-powered solutions in network security, cloud security and security operations. Powered by Precision AI, our technologies deliver precise threat detection and swift response, minimizing false positives and enhancing security effectiveness. Our platformization approach integrates diverse security solutions into a unified, scalable platform, streamlining management and providing operational efficiencies with comprehensive protection. From defending network perimeters to safeguarding cloud environments and ensuring rapid incident response, Palo Alto Networks empowers businesses to achieve Zero Trust security and confidently embrace digital transformation in an ever-evolving threat landscape. This unwavering commitment to security and innovation makes us the cybersecurity partner of choice.

For more information, visit www.paloaltonetworks.com.

About Siemens

Siemens is a technology company focused on industry, infrastructure, transport, and healthcare. From more resource-efficient factories, resilient supply chains, and smarter buildings and grids, to sustainable transportation as well as advanced healthcare, we create technology with purpose adding real value for customers.

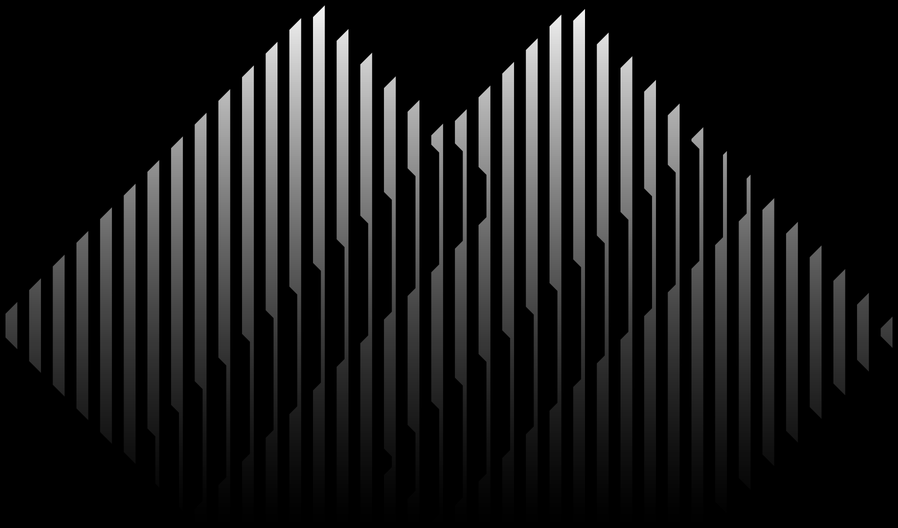
Siemens USA has been a national asset moving America forward for more than 160 years, investing $40 billion in the United States over the past two decades. The company's technology supports the critical infrastructure and vital industries forming the backbone of America's economy.

Palo Alto Networks Team

Adam Robbie
Yiheng An
Matthew Tennis
Rick Wyble
Chao Lei

Siemens Team

Priyanjan Sharma
Enrico Lovat
Johannes Setz



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com