paloalto NETWORKS

Intelligence-Driven Active Defense Report 2026

Securing Operational Technology Environments

IN PARTNERSHIP WITH

SIEMENS

INL Idaho National Laboratory

Table of Contents

Voices from the Partnership

Adam Robbie, Head of OT Threat Research, Palo Alto Networks

"Leading this partnership as the primary author has been a rewarding journey in collaborative research. At Palo Alto Networks, we recognize that the complexity of the OT threat landscape cannot be solved in isolation. This whitepaper brings together the brightest minds from our partner organizations to provide a comprehensive view of the risks and solutions facing us today. I would like to thank each of the lead authors for their dedication and partnership in producing this meaningful guide to OT threat research."

Priyanjan Sharma, Senior Key Expert, Technology Orchestration for Security Services, Siemens

"Grounded in collaboration, serving as a lead author in this effort has been a meaningful experience in advancing OT security research. At Siemens, we understand that effective OT security demands an understanding of both adversary behavior and the operational realities of industrial systems, where availability, safety, and integrity are paramount. This whitepaper reflects the value of organizations coming together to move beyond theory toward practical, defensible outcomes. By working alongside our partners, we aim to help the broader community better understand today's OT threats and adopt security strategies that are grounded in real-world industrial constraints."

Scott Bowman, Technical Lead, Cyber-Physical Systems, Idaho National Laboratory

"Contributing to this whitepaper as Technical Lead for Cyber-Physical Systems at Idaho National Laboratory and lead analyst for the DOE CESER–sponsored CyOTE Program has been a meaningful opportunity to translate national laboratory research into practical value for industry. As the product owner and creator of the Attack Chain Estimator, my role focused on bridging rigorous, publicly funded OT research with the operational realities faced by asset owners and operators. The analytical details shared in this work aim to help OT system operators and cybersecurity professionals discover adversary behavior in the precursor stages of cyber intrusion, enabling active defense at or near the edge of OT environments before disruptive or unsafe outcomes occur."

Meet the Authors

Palo Alto Networks Team

Adam Robbie
Yiheng An
Matthew Tennis
Cecilia Hu
Fang Liu
Zhanhao Chen
Rick Wyble

Siemens Team

Priyanjan Sharma
Tilo Pinkert
Gaurav Srivastava
Martin Otto
Enrico Lovat

INL Team

Scott Bowman
James Cerkovnik
Sam Farnan
Alycia Honas

Executive Summary

Bring the fight to the edge. In an OT environment, defense is about time, and the edge is where you still have it.

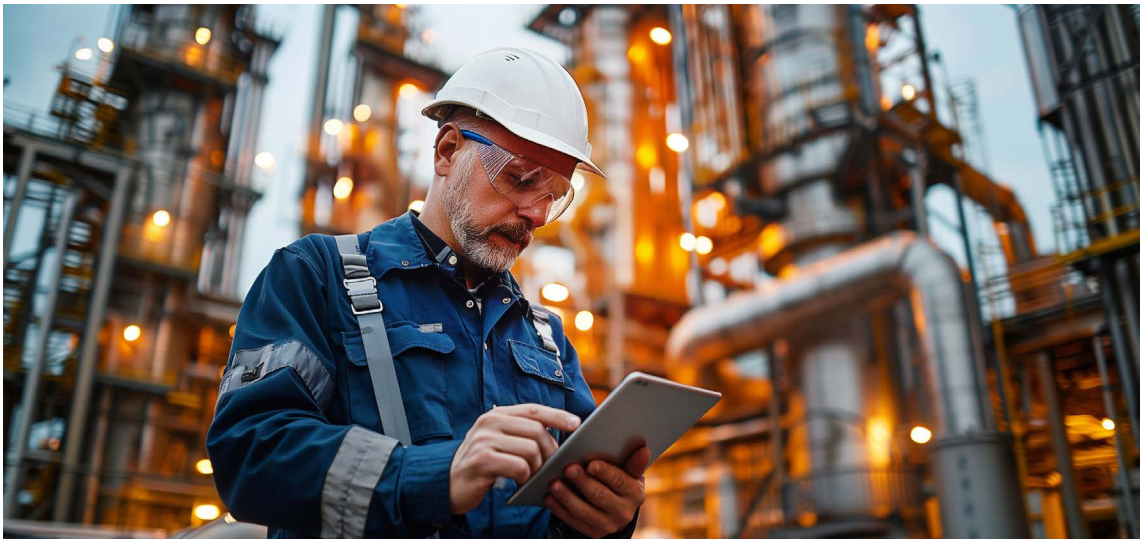
Joint research by Palo Alto Networks, Siemens, and the Idaho National Laboratory (INL) analyzed global telemetry from over 61,000 firewalls deployed in OT environments, alongside 20 years of historical incident data. The analysis shows that industrial threats emerge and persist well before adversaries reach OT environments, creating a measurable window for detection and disruption.

Based on the Idaho National Laboratory Cybersecurity for the Operational Technology Environment (CyOTE™) reports, our research indicates that 82.8% of adversary activity occurs during an extended precursor phase, long before operational impact is realized, with an average dwell time of 185 days. This number of days demonstrates that meaningful time exists between early adversary activity and OT impact—time that can be used to reduce risk if defenders focus their efforts effectively.

At the same time, the traditional assumption of an air-gapped industrial environment is no longer valid. Our research identified a 332% increase in unique internet-exposed OT devices and services, with nearly 20 million OT-related devices now observable on the public internet. Previous studies further show that over 70% of OT attacks originate in IT environments, traversing network boundaries before reaching industrial assets.

Taken together, these findings show that early adversary activity becomes visible upstream of OT impact and remains observable long enough for intervention:

- **Use edge-focused threat intelligence to understand where adversary activity becomes relevant to OT risk.** Threat intelligence provides visibility into exposed services, early-stage techniques, and access paths that surface before adversaries interact with operational systems, helping organizations determine where detection and monitoring should be prioritized.
- **Apply predictive analysis to anticipate where adversary activity is likely to progress.** Observed behavior follows statistically repeatable paths, with hundreds of observable precursor actions per incident, enabling organizations to forecast likely next steps and focus attention where intervention will be most effective.
- **Enable an edge-driven OT-SOC function to operationalize active defense.** By combining threat intelligence and predictive insight at network edges—where enterprise compromise transitions into industrial risk—OT-SOCs can intervene during the precursor phase and disrupt attacks before safety, availability, or operational continuity are impacted.



Introduction

In a recent collaboration, Palo Alto Networks OT Threat Research Lab, Siemens Cybersecurity Research Lab, and Idaho National Laboratory met to examine threats and defense strategies across industrial environments. Each entity brings unique expertise in operational technology (OT) security, for example:

- **Palo Alto Networks** firewall and product telemetry provide large-scale insights into observed attack surfaces and security-relevant activity.
- **Idaho National Laboratory's** predictive analysis methodologies and historical threat landscape research through CyOTE analysis identify long-term adversary behaviors and trends.
- **Siemens** contributes their knowledge and skills in OT-SOC managed services and best practices.

Detection within the OT environment represents a later stage in the attack lifecycle, after adversary access has been established. The know-how between our three entities forms a framework that moves beyond traditional IT-centric security to address the unique risks associated with OT.

Detection within the OT environment represents a later stage in the attack lifecycle, after adversary access has been established.

In this paper, we share our findings on how shifting detection and analysis to the network edge provides earlier visibility, enabling prediction, prevention, and active defense before operational impact occurs. We examine the OT devices and services that are directly accessible from the internet and the security-relevant activity associated with OT applications and industrial protocols that network enforcement points observe.

Our study analyzed both current and historical datasets, including telemetry from 2024 for more than 61,000 OT firewalls. The current data includes threat prevention signatures, exploited Common Vulnerabilities and Exposures (CVEs), Palo Alto Networks WildFire® analysis of malware samples, as well as malicious URL and DNS activity.[1] The historical data is from CyOTE incident research, spanning two decades.

A key finding across these datasets is that a significant portion of adversary behavior historically occurs during early, highly observable phases of activity, well before impact to industrial processes. Network-based telemetry provides critical insight into exposed services and precursor threat behaviors. But, alone, it does not establish adversary intent, asset-specific opportunity, or operational impact. This concern underscores the need to "bring the fight to the edge"—specifically to network enforcement points such as firewalls—where these early activities are most likely to be observed.

In contrast to passive defense models that emphasize visibility and detection without direct interaction, an active defense strategy—implemented within the defender's authority and guided by OT safety constraints—prioritizes an earlier, controlled response to observable precursor activity. Supported by the OT-SOC framework, this approach enables organizations to reduce uncertainty and act sooner to mitigate the risk of a threat actor impacting OT systems.

1. For the latest threat research and updates, see Threat Research Access from Unit 42®.

OT Threat Landscape

Analyzing the OT threat landscape is most effective when viewed from a dual perspective: visibility into the public internet and insight into activity occurring within protected networks. As industrial environments become increasingly interconnected, the distinction between IT and OT continues to blur, expanding the potential attack surface for adversaries. By analyzing both external exposure and internal telemetry, organizations can gain a more holistic understanding of the threat landscape, leading to more effective defense strategies.

In this section, we examine the OT threat landscape across multiple levels, looking at the OT-related attack surface as Palo Alto Networks Cortex Xpanse® observed on the internet. We then shift our focus to threats observed within OT networks, which refers to environments where a firewall has detected OT-related traffic. Our analysis focused on Palo Alto Networks Advanced Threat Prevention telemetries, using signature-based detection to characterize exploit attempts and known attack patterns within the network.

By analyzing both external exposure and internal telemetry, organizations can gain a more holistic understanding of the threat landscape, leading to more effective defense strategies.

OT Devices Exposed to the Internet

Cortex Xpanse analyzed data from OT devices and services to provide our team insights on their quantity, geographic distribution, application protocols, and other relevant metadata. OT devices refer to devices, services, industrial network devices, and systems.[2]

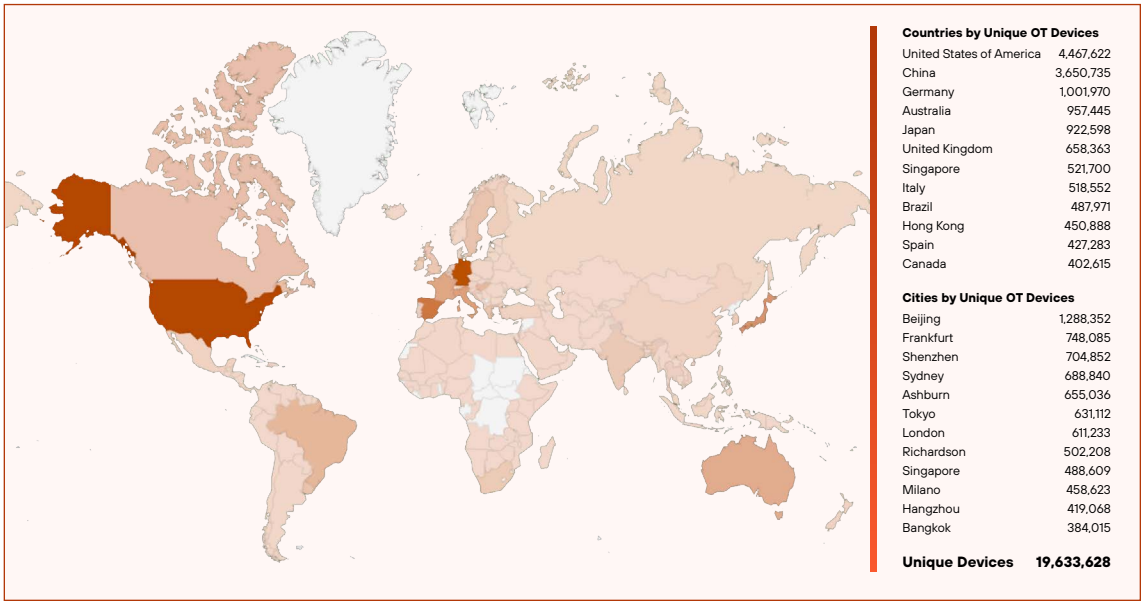
Cortex Xpanse scans the entirety of public IPv4 space and portions of IPv6 space multiple times per day, collecting observations of internet-exposed hosts, to identify exposed devices, ports, and applications. These observations are transformed, enumerated, and fingerprinted, yielding a chronological map of the internet's observable hosts, devices, and application servers. Collecting, transforming, and analyzing petabytes of data require significant engineering effort, but ultimately anyone with a connection to the internet can see the same observations presented here. These findings show the OT attack surface is readily available to threat actors.

For this analysis, we do not distinguish between devices and services that are purposefully configured to be exposed to the internet and those that are otherwise unintentionally exposed.

2. To ensure accuracy, our analysis shifts from counting hosts to aggregating unique services (defined by IP, port, protocol, and fingerprint), providing a more precise measure of distinct application devices for location and infrastructure attribution.

Findings

In 2024, Cortex Xpanse made over 110 million observations of OT devices exposed to the internet, a 138% increase over 2023.[3] From those observations, 19.6 million unique OT devices and services were fingerprinted—a 332% increase over 2023.[4] These devices were hosted on 1.77 million IPv4 addresses, a 41.6% increase over 2023.[5] Figure 1 illustrates the approximate geographic locations of these devices.

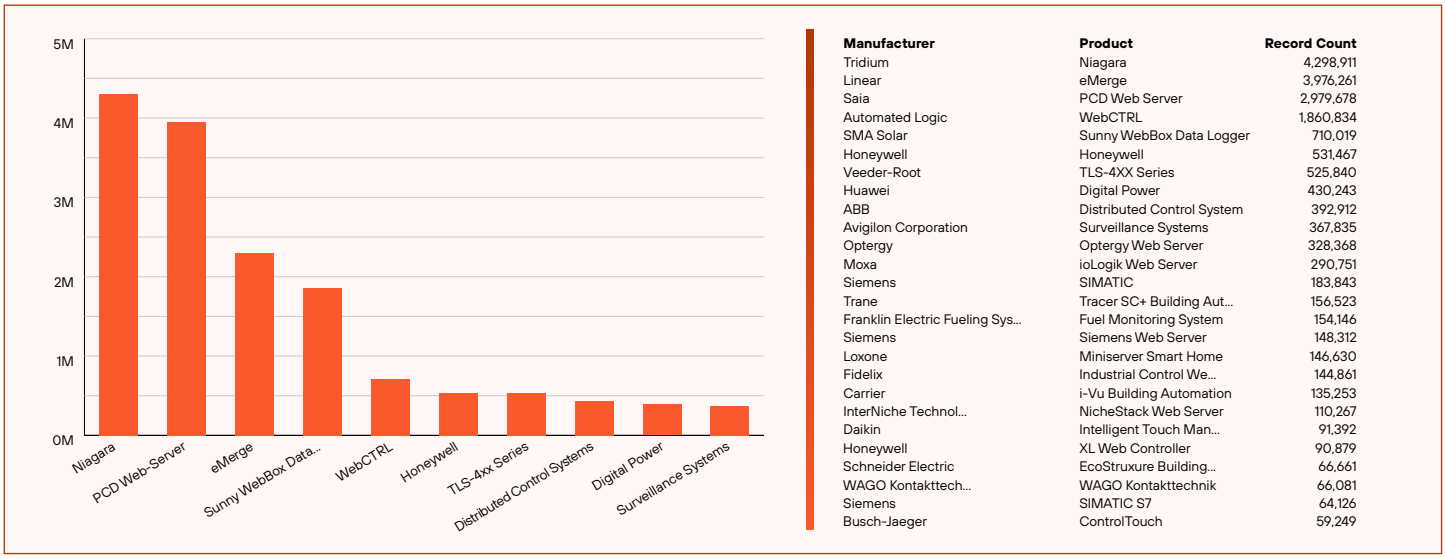


Countries by Unique OT Devices	
United States of America	4,467,622
China	3,650,735
Germany	1,001,970
Australia	957,445
Japan	922,598
United Kingdom	658,363
Singapore	521,700
Italy	518,552
Brazil	487,971
Hong Kong	450,888
Spain	427,283
Canada	402,615

Cities by Unique OT Devices	
Beijing	1,288,352
Frankfurt	748,085
Shenzhen	704,852
Sydney	688,840
Ashburn	655,036
Tokyo	631,112
London	611,233
Richardson	502,208
Singapore	488,609
Milano	458,623
Hangzhou	419,068
Bangkok	384,015
Unique Devices	**19,633,628**

Figure 1. Geographic distribution of 19.6 million unique OT devices in 2024

Figure 2 shows the unique devices by manufacturer and product. Just as in 2023, Tridium Niagara, which is associated with Building Management Systems (BMS) and commonly interfaces with HVAC and other systems, is the most populous OT application fingerprint we observed on the internet.



Manufacturer	Product	Record Count
Tridium	Niagara	4,298,911
Linear	eMerge	3,976,261
Saia	PCD Web Server	2,979,678
Automated Logic	WebCTRL	1,860,834
SMA Solar	Sunny WebBox Data Logger	710,019
Honeywell	Honeywell	531,467
Veeder-Root	TLS-4XX Series	525,840
Huawei	Digital Power	430,243
ABB	Distributed Control System	392,912
Avigilon Corporation	Surveillance Systems	367,835
Optergy	Optergy Web Server	328,368
Moxa	ioLogik Web Server	290,751
Siemens	SIMATIC	183,843
Trane	Tracer SC+ Building Aut...	156,523
Franklin Electric Fueling Sys...	Fuel Monitoring System	154,146
Siemens	Siemens Web Server	148,312
Loxone	Miniserver Smart Home	146,630
Fidelix	Industrial Control We...	144,861
Carrier	i-Vu Building Automation	135,253
InterNiche Technol...	NicheStack Web Server	110,267
Daikin	Intelligent Touch Man...	91,392
Honeywell	XL Web Controller	90,879
Schneider Electric	EcoStruxure Building...	66,661
WAGO Kontakttech...	WAGO Kontakttechnik	66,081
Siemens	SIMATIC S7	64,126
Busch-Jaeger	ControlTouch	59,249

Figure 2. Most observed OT devices exposed to the internet in 2024

3. *OT Security Insights 2024*, Palo Alto Networks and Siemens, January 23, 2025.
4. Ibid.
5. Ibid.

Figure 3 charts the number of unique OT devices on a monthly basis. Some devices might be short-lived or sporadically deployed, while others are consistent and long-lived. It shows a general upward trend of observed devices through 2023 (not shown) and 2024 (shown).

Figure 4 shows the distribution of ports that were positively identified as part of the OT application or device network socket. TCP port 4911 is associated with the Niagara FOX secure or FoxS protocol, as opposed to the unencrypted Fox protocol on port 1911, and TCP port 5011 is associated with Niagara's platform connections over TLS.[6] TCP port 3011 is the default administration port for Niagara hosts.[7] The UDP port 47808 is the default port for BACnet.

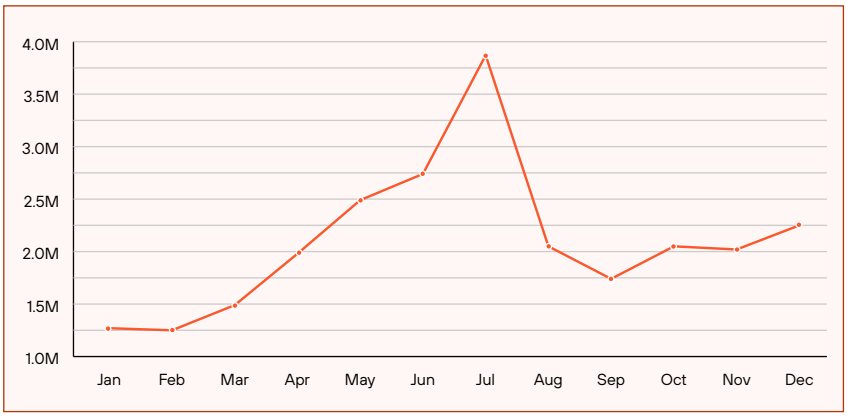


Figure 3. Monthly unique OT devices in 2024

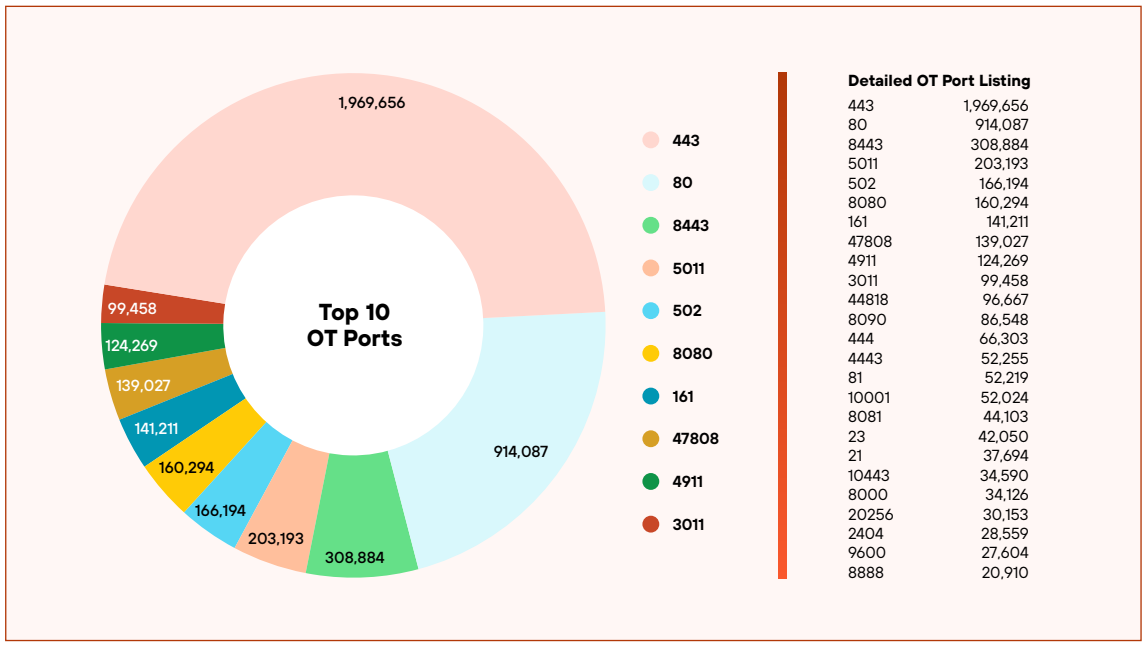


Figure 4. Most popular OT device ports in 2024

All three TCP ports are related to building automation and control. If we add the number of their exposed services, the total for these three ports would be roughly 428,000 services, making them third overall and first overall for OT-specific ports. This estimate aligns with Niagara being the most frequently observed vendor of exposed devices.

Although this use case is not the focus of this paper, it raises the question of whether new installations and HVAC system servicing are responsible for a significant portion of the internet-exposed OT devices and services observed. New installations and servicing typically occur most frequently in the summer months of the Northern Hemisphere, aligning with the notable spike shown in figure 3.

6. *Niagara 4 Hardening Guide*, Tridium, January 17, 2025.
7. *Niagara Networking & Connectivity Guide*, Tridium, May 22, 2002.

Foundations of the OT Cyber Analysis

Our analysis is grounded on a curated dataset of 27 publicly disclosed cyber incidents that impacted OT environments during the years 2000–2022 (figure 5). By using open-source intelligence (OSINT), we assembled a diverse corpus that spans multiple industrial sectors and geographic regions.

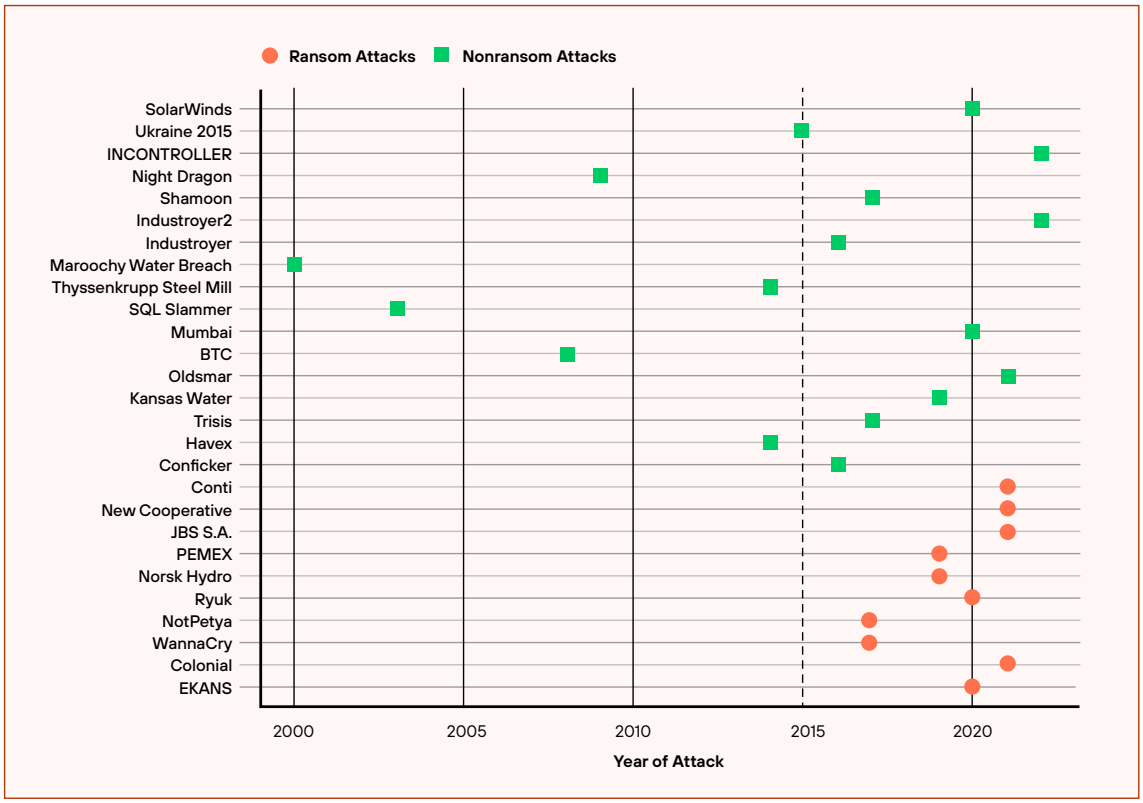


Figure 5. Highly publicized cyberattacks impacting OT, 2000–2022

Approach

All observables were normalized to the MITRE ATT&CK® for ICS framework and systematically reviewed by using the CyOTE analysis. The dataset was not intended as an exhaustive census of OT cyber incidents. Instead, it serves as a foundational baseline for near-real-time analytics and decision support.

For more information on ACE and other CyOTE tools, visit the INL.

By mapping public cyber incident data to MITRE ATT&CK for ICS, we could quantify the prevalence of adversary techniques and sequence of behaviors most frequently employed by attackers. The CyOTE research is meant to generalize the cyberattack process into three phases:

- **Precursor phase:** The part of the attack where the adversary is taking action but the targeted organization has not initiated a response.
- **Triggering event phase:** When a collection of observable events are characterized as anomalous and the targeted organization determines that the observables are associated with adversary behavior, as opposed to systemic failures, and require a cybersecurity response.
- **Post-triggering event phase:** How the adversary continues to behave after the triggering event and how the target organization handles their response.

The value of the CyOTE reports are to leverage these historical analyses within your OT cybersecurity program to coordinate responses against known adversary behaviors before high-consequence events occur. It is the foundation of threat-informed active defense measures, strengthening both strategic risk management and operational readiness.

Findings

Across the 27 incidents, we cataloged 14,039 observables, of which 82.8% occurred in the precursor phase before a high consequence event caused a triggering event for the victim organization. Each incident, on average, involved 430 precursor observable events spanning 13 unique techniques, with 205 of these observables classified as highly perceivable.[8]

These findings underscore a notable and encouraging observation. That is, most attacker behavior is theoretically visible to defenders well before an operational disruption occurs. Dozens of observable events, if generated and streamed to a SIEM, can be used to craft analytics (such as signatures, rules, and correlation searches) to detect and alert on these precursor behaviors.

These findings underscore a notable and encouraging observation. That is, most attacker behavior is theoretically visible to defenders well before an operational disruption occurs.

Precursor Technique Families

The data highlights five dominant precursor technique families:

- Execution via scripting
- Execution via native API
- Command-and-control (C2) using standard application-layer protocols
- Discovery through remote system discovery
- Execution via a CLI

Among these, CLI activity stands out as both highly perceivable and diagnostically rich, while native API and application-layer C2 activity tend to blend into background noise. It's worth noting that, by default in Windows, command-line process audit logging is disabled.[9] Similarly, while PowerShell Script Block Logging has been available since PowerShell version 5.0, it also is not enabled by default. While the activity is perceivable, it relies on both the associated logging being enabled on the endpoints in question and having those logs forwarded to a SIEM for analysis and alerting.

8. "Highly perceivable" means the INL team estimated that OT professionals would be aware and understand the significance of the observed event.
9. "Windows Server command line process auditing," Microsoft, updated: May 12, 2025.

Mapping OT Detection Signatures to MITRE ATT&CK TTPs

We now shift our focus to threat detection events associated with industrial application traffic as observed by network security devices. Classification based on App-ID™ can identify OT applications and industrial protocols that traverse firewalls. By using this classification, we identified that firewalls register OT traffic based on App-ID and then collected the telemetries from these firewalls independent of placement, network topology, or asset role.

From these firewalls, we examined the top 100 exploit signatures detected by the Palo Alto Networks Advanced Threat Prevention service. Because these detections are derived from network-based signatures, their presence alone does not establish adversary intent, successful exploitation, operational impact, or the specific industrial assets involved.

To provide structured threat context without architectural or behavioral assumptions, figure 6 maps the observed activities to the MITRE ATT&CK Matrix for Industrial Control Systems (ICS) and Enterprise. These mappings characterize the observed protocol behavior, rather than asserting confirmed adversary actions. We focus our analysis on the capability dimension of the threat intelligence triangle.[10] This way, you can assess how similar capabilities, when combined with asset exposure in their own environments, might contribute to threat scenarios involving industrial control systems.

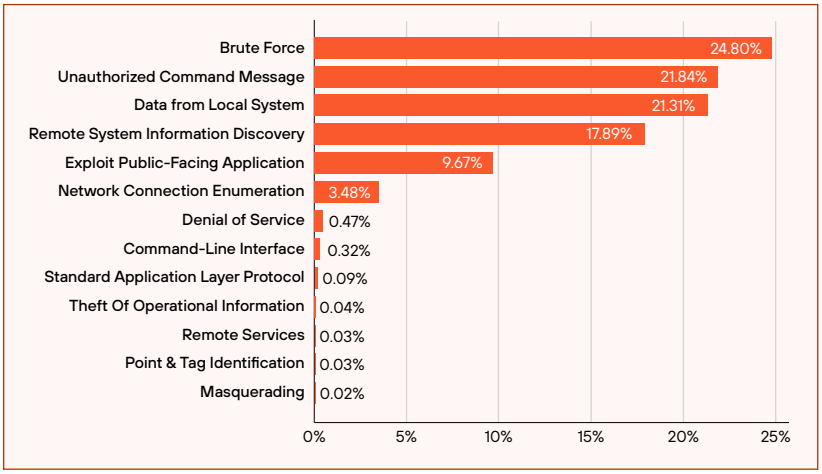


Figure 6. Top TTPs mapped from detected signatures within OT networks

Threat Detection Event and Signature Mapping

The following techniques and corresponding signature mappings are not 1:1. So, you'll see more context and description of the signatures grouped for each tactic, technique, and procedure (TTP).

Brute Force (Enterprise T1110)

This technique's mapping represents the largest volume of observed activity. The technique represents the capability for credential abuse. Also, the associated signatures detect brute-force activity targeting authentication services for SMB, SSH, HTTP login portals, and database systems. This activity illustrates threat actors' desire to acquire valid account credentials as a means of gaining access.

Unauthorized Command Message (ICS T0857)

Closely following brute force is the Unauthorized Command Message technique,, which represents the capacity to issue instructions to control devices. Specifically, the signatures responsible for alerting on this activity were designed to detect attempts to send unauthorized command messages and write requests using SCADA protocols like DNP3.

10. "Threat Intelligence," Pristine Solutions, February 1, 2024.

Data from Local System (ICS T0846)

The high prevalence of this technique represents attackers' inclination toward data extraction. In particular, the signatures associated with these alerts look for attempts to read configurations and control values from SCADA field devices.

Remote System Information Discovery (ICS T0846) and Network Connection Enumeration (ICS T0844)

These techniques collectively capture the capacity for network mapping and reconnaissance. This capability is associated with signatures that:

- Detect the use of dedicated network scanning tools, such as Nmap-style activity.
- Attempt to query available network services, including RPC Portmapper requests.
- Make remote access attempts to collect system and configuration information.
- Detect specialized tools used to enumerate Windows services and network shares on remote hosts.

Exploit Public-Facing Application (ICS T0819)

This technique is associated with signatures modeling the feasibility of leveraging various vulnerabilities. They include high-impact remote code execution (RCE) flaws, cross-site scripting (XSS), and directory traversal attempts directed at internet-facing industrial and supporting IT systems.

Denial of Service (ICS T0833)

The DoS technique reflects attackers' ability to disrupt system response and availability. Associated signatures detect flood attacks and malformed requests, targeting communication services like SIP, DNS, and HTTP/2.

Lower-Volume Techniques

The remaining techniques are observed at lower volumes:

- **Standard Application Layer Protocol (ICS T0874):** Captures the capability for covert communications. The associated signatures detect C2 traffic related to known cryptomining malware.
- **Command-Line Interface (ICS T0843):** Reflects the execution capability. The associated signatures detect malicious payloads embedded within HTTP traffic and suspicious formatting in request headers.
- **Point & Tag Identification (ICS T0868):** Represents a targeted discovery capability. The associated signatures detect requests to identify device metadata, such as vendor and model information, from Modbus devices.
- **Theft of Operational Information (ICS T0890):** Illustrates the capacity for data exfiltration. It's associated with a signature that detects use of the FTP REST command for evasive file transfer.
- **Remote Services (ICS T0865):** Represents unauthorized connection capabilities. The associated signatures detect connection establishment using the ICCP protocol.
- **Masquerading (ICS T0822):** Reflects the ability to make files blend in with the targeted environment or system. The associated signatures detect evasion techniques that are embedded within the HTTP response traffic.

TTP Mapping, Predictive Analysis with Attack Chain Estimator

Attack Chain Estimator (ACE) is a full-stack application developed by INL that has two primary functions. First, it supports classifying observed events in a text format as MITRE ATT&CK TTPs. Once the observed events are classified as a MITRE ATT&CK for ICS TTP, the user can leverage a Markov model that estimates which TTPs will likely occur based on the historical OT cyber incidents the team analyzed.

The INL team developed this predictive capability using a first-order Markov model from analyzing the sequence of MITRE ATT&CK for ICS TTPs during publicly reported OT cyberattacks. The resulting model is a microservice within ACE that can:

- Identify recurring starting point initial access techniques.
- Identify recurring ending state impact techniques.
- Generate forward attack chains from selected initial access techniques.
- Generate reverse attack chains from selected impact techniques.

The first order Markov model turned the frequency counts of TTPs in an attack sequence into transition probabilities and end-to-end path likelihoods for hunt scoping, tabletop design, and control placement across the OT environment. ACE gives you the proactive capability to expand your intelligence-driven active defense measures and refine your investigation hypotheses. This tool helps bridge the behavior observed at the edge of your OT environment to the defenders in the OT-SOC function.

ACE gives you the proactive capability to expand your intelligence-driven active defense measures and refine your investigation hypotheses.

Revised Transition

The predictive insights generated by ACE must be interpreted with an understanding of how the model was developed and what it represents. ACE's transition probabilities are derived from publicly available reporting on 27 OT-impacting cyber incidents occurring over a two-decade span. These incidents vary widely in sector, geography, and reporting quality. Accordingly, the modeling reflects historically observed attacker behavior across industry, not a tailored prediction of how any specific environment will be targeted. In practice, ACE provides a data-informed starting point that organizations can refine and adapt to their own operational context.

This nuance is especially important given ACE's current maturity. The tool is a proof-of-concept capability developed by Idaho National Laboratory under the US Department of Energy, presently at Technology Readiness Level (TRL) 4 and under consideration for future technology transfer. To explore how historically grounded attack-chain patterns can complement commercial detection technologies, the CyOTE team initiated its first joint analysis with OT industry partners, Palo Alto Networks and Siemens, as part of this research effort.

Table 1 highlights one outcome of that collaboration. Using Palo Alto Networks OT-focused detection signatures mapped to MITRE ATT&CK for ICS, we examined how the most frequently observed techniques align with ACE-derived transition probabilities. The leftmost column lists commonly observed entry or early chain techniques. Next, the three "Attack Chain Step *n*" columns outline the most probable subsequent behaviors based on the historical transition model. Finally, the rightmost column identifies the earliest impact-class technique appearing within each chain.

Table 1. Detection Telemetry and Predictions Analysis				
Detection Telemetries Mapped to MITRE TTPs	**Predictive Analysis (CyOTE ACE)***			
Top Techniques	**Attack Chain Step 1**	**Attack Chain Step 2**	**Attack Chain Step 3**	**Impact Technique**
T1110 Brute Force (Credential Access)	T0859 Valid Accounts (Lateral Movement)	T0886 Remote Services (Lateral Movement)	T0867 Lateral Tool Transfer (Lateral Movement)	T0826 Loss of Availability
T0855 Unauthorized Command Message (Impair Process Control)	T0831 Manipulation of Control (Impact)	T0864 Transient Cyber Asset (Initial Access)	T0822 External Remote Services (Initial Access)	T0831 Manipulation of Control
T0893 Data from Local System (Collection)	T0882 Theft of Operational Information (Impact)	T0813 Denial of Control (Impact)	T0815 Denial of View (Impact)	T0829 Loss of View

* The findings are derived from historical and observational data. Applicability and outcomes may vary across individual environments.

Description of Predictive Attack Chains

Each row in table 1 represents an attack chain. The following descriptions provide a detailed walk-through of each identified attack path. These narratives translate the ACE Markov model transitions into a functional understanding of how an adversary moves from an initial observed event to final operational impact.

Through this combined analysis, historical patterns distilled through ACE and contemporary detection data illustrate where defenders are likely to encounter precursor behaviors and why early, context-rich detection remains critical in industrial environments. The approach also demonstrates the value of collaboration between national laboratories and industry to share their respective tools, insights, and expertise toward maturing OT-specific cybersecurity strategies and analytics.

Path 1: Credential-Based Lateral Movement and Operational Shutdown

The detected **Brute Force (T1110)** technique begins this attack chain to achieve credential access. According to the ACE transition model, an adversary successfully capturing these credentials typically moves to leverage **Valid Accounts (T0859)** for seamless lateral movement. The chain then progresses through **Remote Services (T0886**) and **Lateral Tool Transfer (T0867)** as the attacker pivots deeper into the industrial control network. The modeled end-state for this sequence is a **Loss of Availability (T0826)**, which represents a disruption of the controlled process or the disabling of critical OT assets.

Path 2: Direct Process Manipulation via External and Transient Access

This path illustrates a high-velocity escalation from initial access to process interference. The detection of **External Remote Services (T0822)** or the introduction of **Transient Cyber Asset (T0864)** triggers it. The ACE model estimates that, once this foothold is established, the adversary bypasses traditional IT reconnaissance to directly impair process control through an **Unauthorized Command Message (T0855)**. This facilitates the **Manipulation of Control (T0831)**, where the attacker gains the ability to maliciously alter physical parameters, leading to immediate operational impact or safety-critical failures.

Path 3: Operational Espionage and Blinded Control

This scenario begins with the collection of **Data from Local System (T0893)** to harvest project files and network logic. The predictive model suggests this intelligence gathering facilitates the **Theft of Operational Information (T0882)**, an impact that compromises proprietary manufacturing data. To maintain their position, the adversary is likely to initiate **Denial of View (T0815)** and **Loss of View (T0829)** to blind operators to the system's true status. The chain concludes with **Denial of Control (T0813)**, where the adversary successfully blocks legitimate operator commands, resulting in a facility that is both unmonitored and unmanageable.

Bridge to the OT-SOC Framework

The insights uncovered through the CyOTE analysis and the Palo Alto Networks detection mapping raise an important question: How can organizations structure their defensive operations so they can act on these early indicators of adversary behavior? Historical data shows that most observable malicious activity occurs during the precursor phase—long before an attacker attempts to manipulate or disrupt a physical process. However, turning early visibility into protective action requires organizational capabilities, processes, and technologies that are tailored to industrial environments.

The collaboration between Siemens and Palo Alto Networks presents an OT-SOC framework developed specifically to address this challenge. This framework builds on identified patterns to provide a practical, operations-centered approach to disrupting adversary behaviors across the OT attack chain. By aligning a defensive architecture with precursor activity, the research bridges the gap between threat insights and actionable defense.

OT-SOC Framework

Industrial operations are increasingly targeted by sophisticated cyber-physical threats as described earlier in this paper. Incidents, such as ransomware campaigns (e.g., LockBit), have shown that operational downtime, safety risks, and financial losses can occur simultaneously across multiple organizations. Traditional IT-centric defenses are not enough.

OT requires a specialized, safety-conscious approach. The OT-SOC framework provides this capability. An OT-SOC is both a cybersecurity initiative and a business resilience enabler. By embedding safety and operational reliability into its core, the SOC protects human lives, ensures production continuity, and safeguards the reputation and trust of the enterprise.

By embedding safety and operational reliability into its core, the SOC protects human lives, ensures production continuity, and safeguards the reputation and trust of the enterprise.

Key Highlights

- **Vision and guiding principles:** Safety-first, business-aligned, compliance-driven, layered (defense in depth), continuously improving, and tightly integrated with IT and enterprise SOCs.
- **Governance and operating model:** Clear accountability between oversight (plant management and business leaders) and responsibility (CISO, VP Engineering, and IT). Flexible operating models (hybrid, on-premises, or MSSP) supported by defined OT-SOC roles and policies.
- **Reference architecture:** Built on layered segmentation, with secure data flows, visibility across all layers, OT-specific analytics, and orchestration. Emphasis on precision monitoring to balance operational safety and effective threat detection.
- **Integration with the enterprise SOC:** Cross-domain playbooks, enriched alert handovers, and joint red and blue team exercises to address blended IT and OT attacks.
- **Roadmap:** A pragmatic, phased approach:
  - **0–3 months:** Begin limited data collection supported by OT-dedicated SIEM, refinement, and aggregation.
  - **3–6 months:** Baseline and pilot SOC in a limited plant area.
  - **6–18 months:** Integrate OT and IT playbooks, as well as tabletop exercises.
  - **18–36 months:** Mature into automation, AI analytics, and cross-site threat hunts.
- **KPIs:** Mean time to detect and respond, a percentage of assets monitored, SLA containment, compliance remediation, and reduction in repeat incidents.
- **Training and awareness:** OT-focused workforce training, joint CERT drills, sector-wide exercises, and industry engagement.
- **Continuous improvement:** Postincident reviews, purple team testing, and enrichment with evolving threat intelligence.

An OT-SOC framework is a cybersecurity initiative as well as a business resilience enabler. By embedding safety and operational reliability into its core, the SOC protects human lives, ensures production continuity, and safeguards the reputation and trust of the enterprise.

Coherent and Resilient Operational Security Delivery

The OT-SOC framework shown in figure 7 demonstrates how coherent and resilient operational security is achieved by integrating guiding principles, cross-network visibility, context-rich analytics, and measurable outcomes into a unified model.

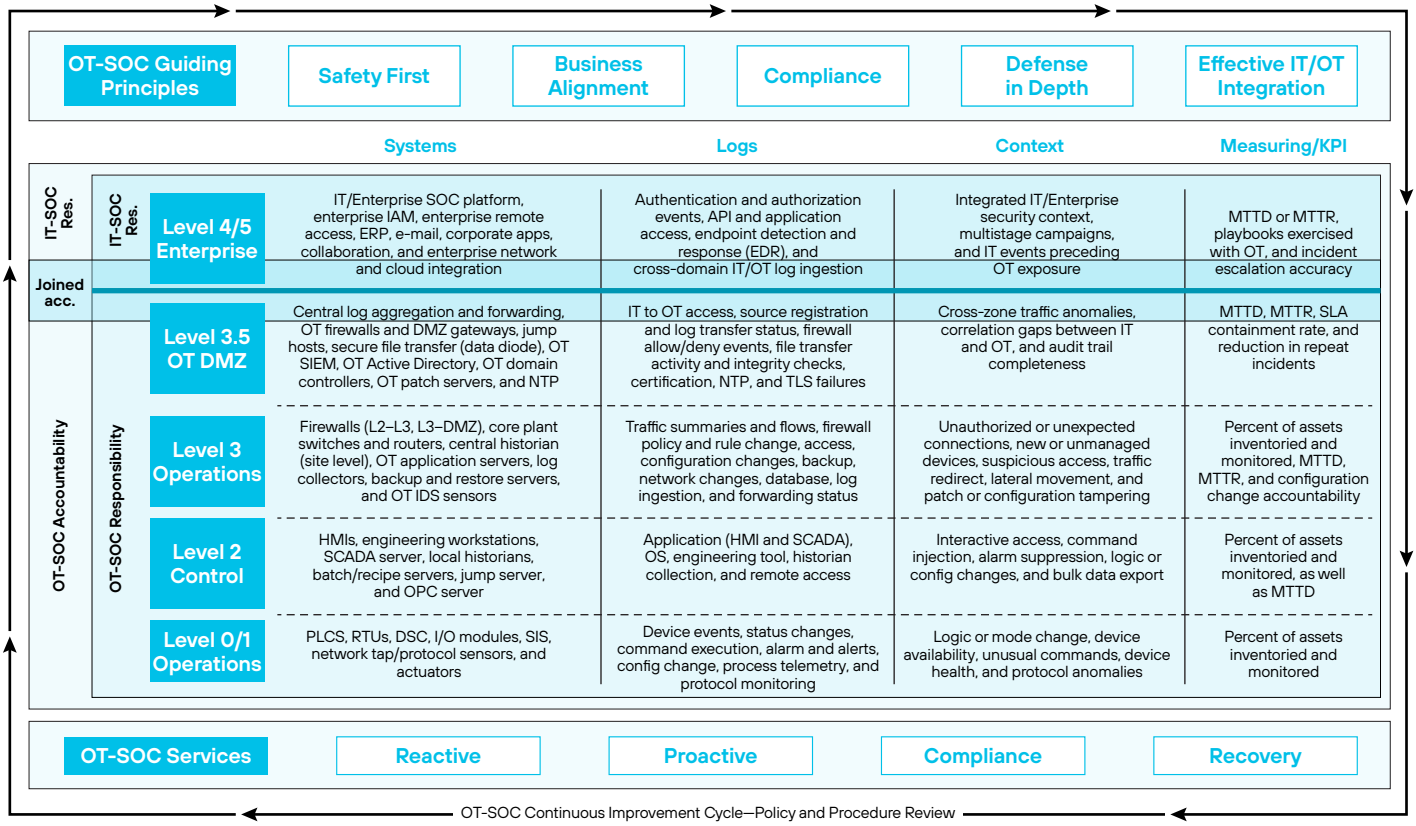


Figure 7. OT–SOC framework

At the foundational Levels 0 and 1 through Level 3, the framework defines OT-SOC responsibilities for capturing and interpreting essential telemetry—including protocol activity, logic changes, alarms, and configuration events—generated by process, control, and operations systems. As the architecture extends upward to Level 3.5 (OT DMZ) and Level 4/5 (Enterprise), accountability broadens to incorporate centralized logging, SIEM and SOAR capabilities, identity and access platforms, remote access services, and business applications.

At these upper layers, the framework also formalizes the shared responsibility between the OT-SOC and the IT-SOC function by establishing a structured, bidirectional handover process for high-fidelity alerts, ensuring that events are aggregated, enriched, and correlated consistently across both domains. This process includes joint ownership of cross-domain playbooks and regular training exercises so that both SOC functions can coordinate seamlessly during blended IT and OT incidents. The layered structure enables secure event federation and multidomain correlation, which are essential for recognizing blended IT/OT threats.

Figure 7 shows how each Purdue layer contributes distinct systems, log types, and contextual insights, creating a continuous visibility and detection fabric spanning from equipment on the plant floor to enterprise-level systems. The guiding principles—Safety First, Business Alignment, Compliance, Defense in Depth, and Effective IT/OT Integration—anchor the SOC team's decisions and en-

sure operational integrity. Meanwhile, OT-SOC service categories—Reactive, Proactive, Compliance, and Recovery—operate within a continuous improvement cycle supported by KPIs such as MTTD, MTTR, SLA adherence, and asset monitoring coverage.

By applying the OT-SOC framework, an organization can improve their performance in:

- **Early detection,** such as brute force, command manipulation, and masquerading.
- **Safe containment,** for example, of project uploads, transient devices, and exfiltration attempts.
- **Rapid recovery,** such as from denial-of-view and loss-of-control scenarios with offline backups and redundant systems.
- **Continuous resilience,** for example, through cross-SOC collaboration and evolving playbooks.

Collectively, this framework orchestrates people, processes, and technologies across all organizational layers to deliver a resilient, risk-aligned, and operationally coherent industrial cybersecurity capability.

Roadmap

Building an OT-SOC function is a phased and strategic journey that grows in capability, sophistication, and resilience over time. Organizations rarely start with full visibility or mature processes. Instead, they evolve through deliberate steps that balance operational safety, resource constraints, and business priorities. A phased roadmap ensures that early progress builds confidence, later phases deliver enterprise-scale value, and each stage reinforces the next one through continuous improvement:

Building an OT-SOC is a phased and strategic journey that grows in capability, sophistication, and resilience over time.

- **0–6 months:** Establish foundational readiness by conducting a baseline security assessment, inventorying OT assets, and validating segmentation across Purdue levels (or begin establishing segmentation). Focus early efforts on achieving quick wins—ideally through a controlled pilot in a noncritical part of the plant—allowing teams to prove value, test workflows, and refine their approach without putting operations at risk.
- **6–18 months:** Expand capabilities by deploying OT SIEM and intrusion detection systems (IDS) across critical zones, enabling real-time monitoring and more reliable anomaly detection. During this phase, organizations develop and validate incident response playbooks through tabletop exercises and strengthen collaboration with the enterprise and IT-SOC functions to ensure effective cross-domain escalation and information sharing.
- **18–36 months:** Advance toward full operational maturity with SOAR-driven automation, AI-enabled analytics, and cross-site threat hunting campaigns. This stage transforms the OT-SOC from a monitoring function into a resilient, enterprise-scale capability that can detect sophisticated threats, correlate events across plants, and accelerate response through orchestrated workflows.

This phased roadmap delivers early measurable improvements while laying the foundation for long-term maturity, ensuring that the OT-SOC function grows sustainably and remains aligned with operational and business requirements.

Putting It All Together

The strategy for optimizing OT log collection was derived by using a two-phased, threat-informed approach.

In "Mapping OT Detection Signatures to MITRE ATT&CK TTPs," we analyzed the most frequent intrusion attempts observed within the OT environment, derived from top Advanced Threat Prevention signatures that fired either inside the network or at the perimeter firewall. For each of these high-frequency initial detections, the ACE tool predicted the subsequent four most probable adversary steps. The result was multiple full-sequence attack chains, for example: Brute Force → Valid Accounts → Remote Services → Loss of Availability.

Then, in "TTP Mapping, Predictive Analysis with Attack Chain Estimator," we mapped the detection requirements of every TTP within those generated chains back to their necessary log sources, such as VPN Concentrator, HMI App Logs, and Historian. By cross-referencing all attack chains, we could isolate the top common log sources that offer visibility into the broadest range of predicted adversary activities. This methodology ensures that resources are allocated efficiently, prioritizing the collection, parsing, and alerting for logs from systems like Historian, HMI and SCADA servers, and jump host/bastion host. It maximizes the SOC's detection coverage against the most probable end-to-end attack sequences, without requiring exhaustive collection across all assets.

Table 2. Detection Telemetry, Predictions Analysis, and Log Aggregation

Detection Telemetries Mapped to MITRE TTPs	Predictive Analysis (CyOTE ACE)*				OT Data and Logs Needed for Detection in OT-SOCs
Top Techniques	Attack Chain Step 1	Attack Chain Step 2	Attack Chain Step 3	Impact Technique	Log Sources
T1110 Brute Force (Credential Access)	T0859 Valid Accounts (Lateral Movement)	T0886 Remote Services (Lateral Movement)	T0867 Lateral Tool Transfer (Lateral Movement)	T0826 Loss of Availability	• VPN Concentrator • Firewall/Perimeter • Jump Host/Bastion • HMI/SCADA App Logs
T0855 Unauthorized Command Message (Impair Process Control)	T0831 Manipulation of Control (Impact)	T0864 Transient Cyber Asset** (Initial Access)	T0822 External Remote Services (Initial Access)	T0831 Manipulation of Control	• HMI/SCADA App Logs • PLC/RTU • Historian • ICS IDS Appliance • Engineering Workstations • Switches and Routers • Firewall and Perimeter
T0893 Data from Local System (Collection)	T0882 Theft of Operational Information (Impact)	T0813 Denial of Control (Impact)	T0815 Denial of View (Impact)	T0829 Loss of View	• Historian • HMI/SCADA Servers

* The findings are derived from historical and observational data. Applicability and outcomes may vary across individual environments.

** Because this is late in the attack chain, once the attackers historically were able to manipulate control, they would leverage transient cyber assets and then use External Remote Services to cause other effects.

Conclusion: From Visibility to Resilient Active Defense

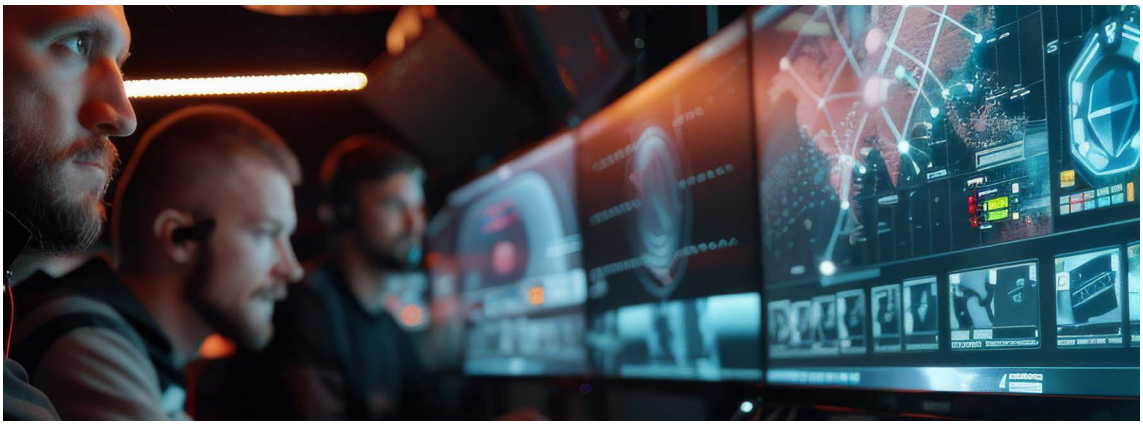
The collaboration between Palo Alto Networks, Siemens, and INL provides an in-depth look at the current state of industrial cybersecurity—moving beyond theoretical risk to a data-driven model for active defense.

Our analysis reveals a stark reality: The OT attack surface is expanding rapidly, with a 332% increase in unique fingerprinted OT devices and services observed in 2024. While the sheer volume of exposure is concerning, the historical data provided by CyOTE offers a strategic advantage. Over 80% of adversary behavior occurs during the "precursor phase"—highly observable actions that take place long before an attacker achieves operational impact.

By integrating Palo Alto Networks real-time telemetry with the INL Attack Chain Estimator and the jointly developed OT-SOC framework, this paper establishes a blueprint for modern industrial defense:

- **Shift to an active defense:** Passive monitoring is no longer sufficient. Organizations must "bring the fight to the edge," using network enforcement points to disrupt adversary capabilities during the early, observable stages of an attack.
- **Use threat-informed logging:** Rather than attempting exhaustive log collection, defenders should use Markov-modeled attack chains to prioritize logs from high-value sources like Historians, HMIs, and jump hosts.
- **Establish a resilient OT-SOC capability:** This jointly developed framework ensures that operational continuity and human safety govern incident response, transforming security from a cost center into a business resilience enabler.
- **Collaborate as a force multiplier:** The synergy between national laboratories and industry leaders, like Palo Alto Networks and Siemens, provides the context-rich intelligence necessary to outpace sophisticated threats.

As industrial environments continue to modernize and converge with IT infrastructure, the window of opportunity to detect precursors will only be as valuable as the defender's ability to act on them. Through the phased roadmap and integrated framework presented in this paper, organizations can evolve from reactive posturing to a proactive and resilient stance that safeguards the world's most critical infrastructure.



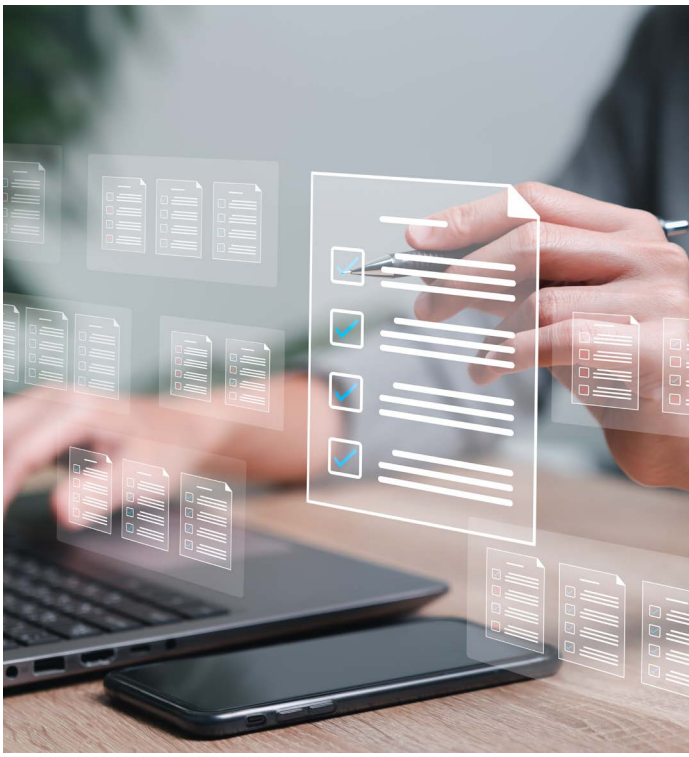
Data Methodology

Exposed Device to the Internet

- **Scope:** This study analyzed OT using 2024 global scan data, encompassing SCADA, IoT, and building control systems.
- **Internet-exposed services:** The data represented point-in-time observations of devices responding on specific ports.
- **Overcoming IP limitations:** Identifying unique devices by IP address was unreliable due to dynamic IP assignment, NAT, and hidden infrastructure, such as CDNs and VPNs.
- **Unit of analysis:** To ensure accuracy, the analysis shifted from counting hosts to aggregating unique services (defined by IP, port, protocol, and fingerprint). This provided a more precise measure of distinct application devices for location and infrastructure attribution.

Signature-Based Telemetries

- **Internal network insights:** We analyzed data from 61,000 OT firewalls by using Palo Alto Networks App-ID and Advanced Threat Prevention tools to characterize application traffic and alerts.



Analytical Constraints

- **Geographic bias:** Higher detection rates in the US and Netherlands likely reflected superior visibility and cybersecurity infrastructure rather than higher risk. Conversely, lower rates in regions, like Brazil and India, might stem from weaker monitoring frameworks.
- **Industry bias:** Results might skew toward industries with more mature threat detection systems.

Analysis Biases

- **Reliance on Palo Alto Networks tools:** The use of proprietary Palo Alto Networks tools, including App-ID and Advanced Threat Prevention, introduced bias toward threats best detected by these technologies, potentially missing other threat vectors.
- **Geographical and industry disparities:** Regions and industries with advanced cybersecurity practices reported more threats, creating a bias toward these areas, while less-developed regions or sectors might underreport incidents due to weaker detection capabilities.

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

About Idaho National Laboratory

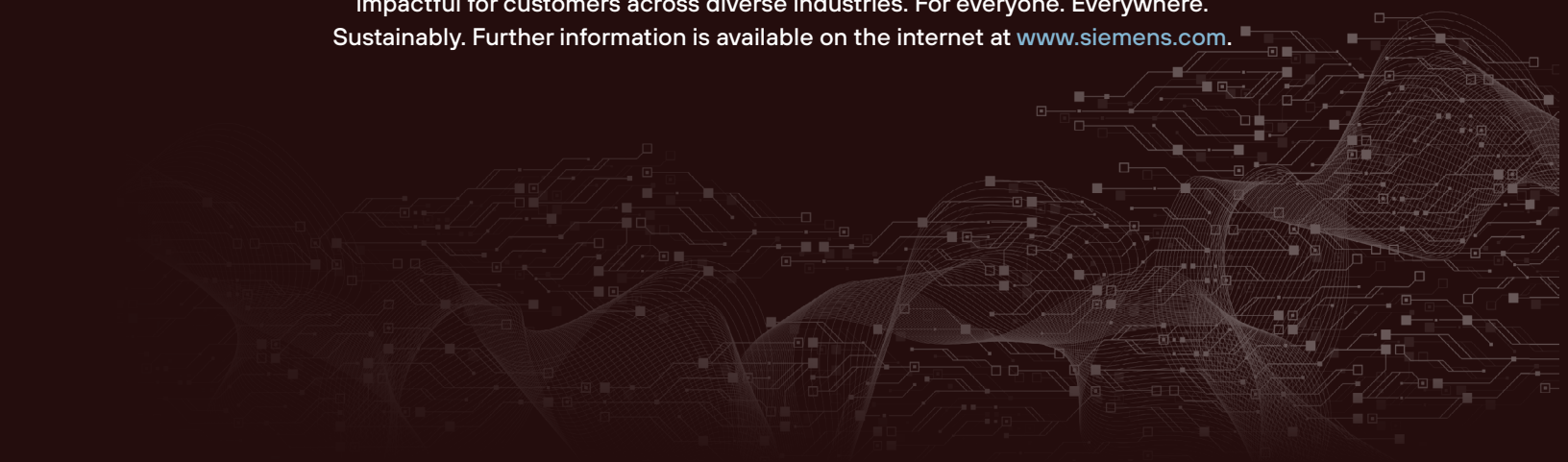
Idaho National Laboratory (INL) is the nation's leading center for nuclear energy research and development. Operated for the US Department of Energy by Battelle Energy Alliance, INL plays a critical role in advancing energy security, scientific innovation, and environmental sustainability. The laboratory's mission spans across nuclear energy, clean energy integration, critical infrastructure protection, and national security, driving technological advancements to solve some of the world's most complex challenges. Located in Idaho Falls, Idaho, INL collaborates with government, academia, and industry to deliver impactful solutions and shape a secure and sustainable energy future. For more information, visit www.inl.gov.

About Palo Alto Networks

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.

About Siemens

Siemens Corporation is a US subsidiary of Siemens AG, a leading technology company focused on industry, infrastructure, transport, and healthcare. The company's purpose is to create technology to transform the everyday, for everyone. By combining the real and the digital worlds, Siemens empowers customers to accelerate their digital and sustainability transformations, making factories more efficient, cities more livable, and transportation more sustainable. A leader in industrial AI, Siemens leverages its deep domain know-how to apply AI—including generative AI—to real-world applications, making AI accessible and impactful for customers across diverse industries. For everyone. Everywhere. Sustainably. Further information is available on the internet at www.siemens.com.



paloalto NETWORKS SIEMENS INL Idaho National Laboratory

INL/RPT-26-90246 Rev:000