

2019 GLOBAL ICS & IIoT RISK REPORT

A data-driven analysis of
vulnerabilities in our industrial
and critical infrastructure

CYBERX

BATTLE-TESTED INDUSTRIAL CYBERSECURITY

Table of Contents

- 1.0 INTRODUCTION** 4
- 2.0 EXECUTIVE SUMMARY** 6
- 3.0 FROM AWARENESS TO ACTION** 9
- 4.0 COMPARING THE 2017 & 2018 DATA** 11
- 5.0 DISTRIBUTION OF INDUSTRIAL PROTOCOLS** 13
- 6.0 RECOMMENDATIONS** 15
 - 6.1 IDENTIFY CROWN JEWEL PROCESSES** 16
 - 6.2 MAP THE DIGITAL TERRAIN** 16
 - 6.3 ILLUMINATE THE MOST LIKELY ATTACK PATHS** 18
 - 6.4 MITIGATE & PROTECT** 19
 - 6.4.1 REDUCE NUMBER OF DIGITAL PATHWAYS TO A MINIMUM** 20
 - 6.4.2 IDENTITY & ADDRESS ICS NETWORK & ENDPOINT VULNERABILITIES** .. 20
 - 6.4.3 IMPLEMENT CONTINUOUS ICS MONITORING** 20
 - 6.5 PRACTICE CYBER HYGIENE** 21
 - 6.6 LEVERAGE ICS THREAT INTELLIGENCE** 21
 - 6.7 CREATE A MANAGEABLE OS UPGRADE SCHEDULE** 21
 - 6.8 REMOVE SILOS BETWEEN OT & IT** 22
- APPENDIX: REPORT METHODOLOGY 24
- ABOUT CYBERX 26

“The risk to OT networks is **real** — and it's dangerous and perhaps even **negligent** for business leaders to ignore it.”

*Michael Assante, ICS/SCADA Lead,
SANS Institute*

1.0

INTRODUCTION



Industrial and critical infrastructure organizations that rely on industrial control systems (ICS) to run their businesses – such as firms in energy and utilities, oil & gas, pharmaceutical and chemical production, food & beverage, and other manufacturing sectors – have known their valuable assets are susceptible to cyberattack since Stuxnet was discovered and publicized in 2010.

The extent to which they are vulnerable, and the attack vectors through which they might be compromised, however, have historically been much harder to know in any measurable sense.

More recently, destructive malware such as WannaCry and NotPetya, as

well as targeted ICS attacks such as TRITON and Industroyer, have shown the potential impact of ICS cyberattacks which include costly production outages and clean-up costs, catastrophic safety and environmental incidents, and threats to the proper functioning of civilized societies such as loss of heat, power, and even human life.

In 2017, CyberX began to shed light on these risks when we published the first-ever Global ICS & IIoT Risk Report. By analyzing real-world network traffic data from 375 production ICS networks worldwide, across multiple industry verticals, CyberX gave the world a data-driven glimpse into the wide range of existing vulnerabilities in ICS environments.

This report supplements the data included in our 2017 report. It analyzes data obtained from over 850 production ICS networks that CyberX assessed from September 2017 to September 2018, using proprietary Network Traffic Analysis (NTA) and deep packet inspection¹. The networks span all sectors across North and South America, EMEA, and Asia-Pacific.

This follow up to our previous report remains one of the only ICS risk analyses based on actual network traffic data – as opposed to interviews or survey-based data – in existence.

The data clearly shows that industrial control systems continue to be soft targets for adversaries. Many sites are exposed to the public internet

and trivial to traverse using simple vulnerabilities like plain-text passwords. Lack of even basic protections like automatically-updated anti-virus enables attackers to quietly perform reconnaissance before sabotaging physical processes such as assembly lines, mixing tanks, and blast furnaces.

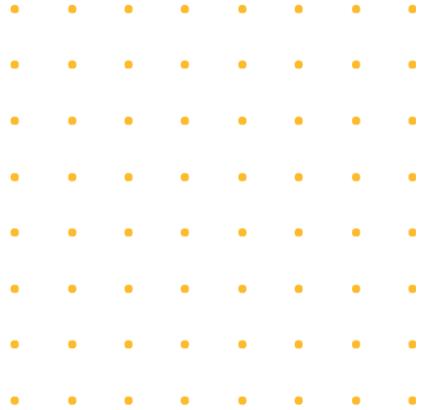
As Sun-Tzu advises, those who know neither their adversaries nor themselves are doomed to lose battles. In order to protect ourselves, our critical systems, and our economies, we need a realistic, data-driven view of the current risk.



¹The analysis was performed on an anonymized and aggregated set of metadata with all identifying information removed. Rigorous attention was paid to preserving the confidentiality of sensitive customer information.

2.0

EXECUTIVE SUMMARY



Here are the top data points from our 2019 Global ICS & IIoT Risk Analysis:

- **The air-gap – still a myth: 40% of industrial sites have at least one direct connection to the public internet**, making them more easily accessible to adversaries and malware. As an industry, we should continue to acknowledge that these findings explode the myth that Operational Technology (OT) networks don't need to be monitored or patched because they're isolated from the internet via "air-gaps" and/or they run proprietary devices and protocols. With digitization as a key business driver, OT networks will increasingly be connected to corporate IT networks – providing additional pathways for attackers.
- **Broken Windows: 53% of sites have obsolete Windows systems such as Windows XP.** Since Microsoft no longer develops security patches for legacy systems, they can easily be compromised by new forms of ransomware and destructive malware. While it may not always be possible to patch or upgrade systems to more modern versions – due to ICS-specific factors such as narrow maintenance windows, legacy applications, and older hardware – best practices suggest implementing compensating

controls such as continuous monitoring to quickly spot cyberattackers in the early phases of a breach, before they've done any damage.

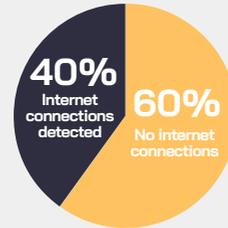
Other compensating controls include better segmentation between IT and OT networks, and granular segmentation between different layers of OT networks. In New York City, the "Broken Windows" theory of policing is credited with turning the tide against crime in the early 1990s². One can hope that updating Windows boxes might help turn the tide against cyberattacks.

- **Hiding in plain sight: 69% of sites have plain-text passwords traversing their ICS networks**, which can easily be sniffed by attackers performing cyber-reconnaissance and then used to compromise critical industrial devices. These are typically associated with legacy devices that don't support modern, secure protocols such as SNMP v3 or SFTP.
- **Anti-anti-virus: 57% of sites aren't running anti-virus protections that update signatures automatically**, increasing the risk of malware infections. While owners of critical infrastructure and industrial control

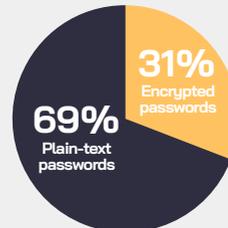
² https://en.wikipedia.org/wiki/Broken_windows_theory

Top Data Points at a Glance

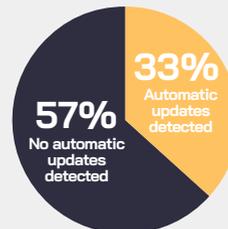
Mythical Air-Gap



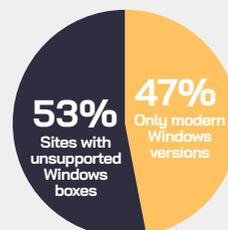
Hiding in Plain Sight



Anti-Anti-Virus



Broken Windows



systems were once uniformly opposed to anti-virus, many no longer consider anti-virus as disruptive to OT processes, and more and more OT vendors are certifying AV vendors as well. As an alternative to anti-virus, many vendors are implementing additional controls such as application whitelisting.

- **Indecent exposure: 16% of sites have at least one Wireless Access Point.** Misconfigured Wireless Access Points (WAPs) increase the attack surface because they can be accessed by unauthorized clients such as employee or contractor laptops and mobile devices. WAPs can also be compromised via the KRACK WPA2 vulnerability.

In addition, access points such as routers, VPN gateways, or switches could also serve as a point of entry for attackers. Access points such as routers and VPN gateways are also exposed to sophisticated malware such as VPNFilter, enabling attackers to capture MODBUS traffic, perform network mapping, destroy router firmware, and launch attacks on OT endpoints from compromised routers. This means that routers should be regularly inventoried and patched to prevent these attacks.

- **Excessive accessibility: 84% of industrial sites have at least one remotely accessible device.** Remote management and access protocols like RDP, VNC, and SSH make it easier for administrators to remotely configure devices – but they also make it easier to attackers with stolen credentials to learn exactly how equipment is configured and eventually manipulate it.

Section 3 of this report describes some of the “Big Picture” ideas that have led to an evolution of thinking in the ICS security industry, along with an acknowledgement of the unique challenges facing OT managers and board members as they strive to improve their OT risk postures.

Section 4 describes some of the changes we found in 2018 as compared to 2017, including a notable and impressive shift away from legacy Windows systems.

Section 5 provides a brief description of the wide range of specialized industrial protocols we found.

Section 6 provides a number of practical steps that organizations can take today to mitigate OT risk. This includes recommendations for how to prioritize vulnerabilities and implement compensating controls, as well as organizational initiatives for breaking down barriers between IT and OT.

3.0



FROM AWARENESS TO ACTION

As early as 2001, a small group of committed individuals began raising awareness of cyber risk to industrial control systems in our critical infrastructure.

The discovery of Stuxnet malware in 2010 and the publicity surrounding the half-dozen known exploits since then – such as TRITON, Industroyer, NotPetya and WannaCry – have helped raise awareness about the risk for management teams as well as for IT and OT personnel. Today, an entire industry dedicated to protecting ICS and IIoT is taking shape. Innovative technology suppliers such as CyberX have raised capital and are collectively monitoring

and defending a growing number of ICS and IIoT networks.

While a minority of organizations have now implemented ICS monitoring solutions, most remain completely unprotected. Many IT and OT personnel have availed themselves of conferences, podcasts, and industry news in order to raise their understanding of the risks and how to address them.

TRITON showed just how sophisticated and dangerous attacks on industrial control systems have become – a simultaneous dismantling of safety controls, combined with malicious instructions

to overheat or overpressurize a boiler, showed how determined attackers can cause catastrophic environmental damage and loss of human life.

As we continue to both assess past attack methods and the current state of our networks and vulnerabilities, a path towards remediation and protection becomes clearer. Not everything can be protected at once, and the deeply complicated and critical nature of OT networks mean that by definition systems cannot be easily taken offline in order to install upgrades, patches, or anti-virus. Ruthless prioritization is required.

Section 6.0 describes a number of practical steps – steps that take into

consideration both convenience and efficacy – that organizations can take to mitigate OT risk. These steps include both basic “hygiene” that can thwart opportunistic attacks, as well as more resource-intensive steps that can reduce vulnerabilities to targeted attacks. It also includes technology initiatives such as using compensating controls and multi-layered defenses, including continuous monitoring with behavioral anomaly detection and threat modeling, to mitigate vulnerabilities that might take years to fully remediate. SANS describes this proactive approach as “Active Cyber Defense,” which is the process of using security operations to continuously identify and counter threats.

4.0

COMPARING THE 2017 & 2018 DATA

Analyzing the data for the second time in two years gives us an opportunity to compare data and look for trends³.

Perhaps the most important conclusion we reached after looking at the delta between last year's report and this year's report is that the delta itself is small, and the industry may not have changed much over the course of the past year. With one exception (the number of sites

using outdated Windows systems, which improved year over year), the rest of our data changed in relatively small increments.

As noted earlier, awareness about the need for stronger ICS defenses is growing, but there's still a lot of work to be done. It bears remembering that we are attempting to close a ~25 year gap between OT and IT security practices.

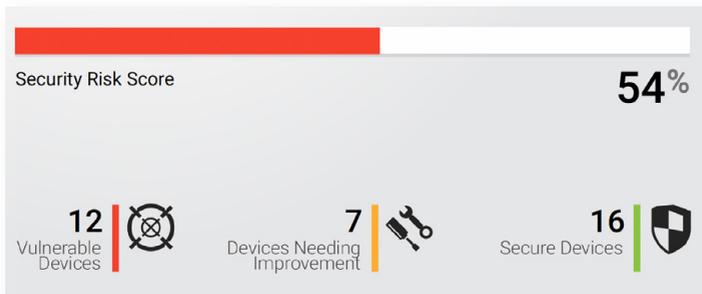
³ The customer networks we assessed are not random samples and thus whatever data we collect should be taken as indicative of possible trends as opposed to universal representations of risk within particular industries.

Regarding the one exception we did find: 76% of sites included legacy Windows systems in 2017, while the figure decreased to “just” 53% in 2018. In other words, in the sites we assessed in 2018, greater attention was paid to upgrading Windows boxes to more modern versions. We believe that continued publicity about WannaCry and NotPetya resulted in top-down attention to the issue by boards and C-level personnel — who witnessed for the first time how their quarterly financials could be significantly impacted by vulnerabilities in production environments.

In 2017, we evaluated the median for the overall risk score across all customer sites at 61%, with 80% being our minimum recommended score. The distribution across verticals was fairly even, with 66% for manufacturing, 63% for Oil & Gas, 62% for Energy & Utilities, and 56% for Pharmaceuticals & Chemicals.

In 2018 the median overall risk score improved to 70% overall. Oil & Gas and Energy & Utilities showed their relative maturity with scores of 81% and 79%, respectively. The Manufacturing and Pharmaceutical & Chemical sectors showed their relative immaturity with scores of 67% and 68% respectively.

The number of manufacturing companies in the analysis went up in 2018 relative to 2017. Manufacturers are generally less mature from a security viewpoint compared to electric utilities which are regulated. The median overall risk score for manufacturing companies is lower than those in other verticals, and the heavier weighting of manufacturing may account for some lack of improvement in individual statistics.



Overall risk score calculated using CyberX's continuous vulnerability assessment

5.0

DISTRIBUTION OF INDUSTRIAL PROTOCOLS

Industrial networks contain a complex mix of specialized non-IT protocols, including proprietary protocols developed for specific families of industrial automation devices. This heterogeneous mix complicates security for OT environments.

In addition, many OT protocols were originally designed when robust security features such as authentication were not even a requirement – because it was assumed that simply having connectivity to a device was sufficient authentication.

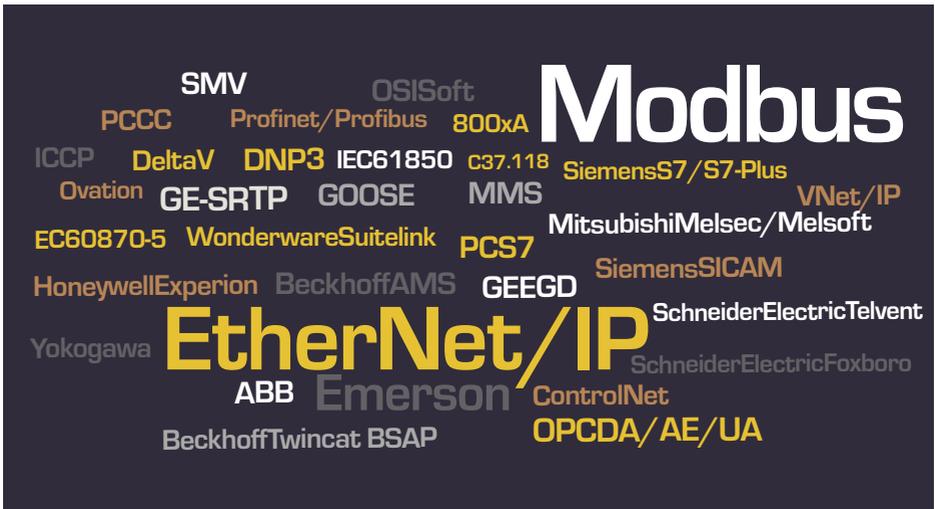
The most commonly-used protocol in our sample was Modbus, a serial communications protocol originally published by Modicon (now Schneider Electric) in 1979. Modicon invented PLCs, which are widely-used today to control physical processes such as motors and valves.

To further complicate OT security, industrial organizations have historically lacked any visibility into OT network activity and assets because traditional

monitoring tools designed for corporate IT networks are “blind” to OT-specific protocols like Modbus TCP.

In our automated risk assessments, we also encountered a number of standard IT protocols (HTTP, SMB, RDP, etc.). The SMB protocol is in wide usage across IT and OT, and managers should note that vulnerabilities in the decades-old SMB protocol were a key factor in the costly WannaCry and NotPetya attacks of 2017.

As expected, our risk assessments found a diverse mix of OT protocols. The following word cloud shows a sampling of the types of OT protocols that we encountered over the course of the past year.



Note: The CyberX platform is protocol- and vendor-agnostic and supports many other protocols not shown here.

6.0

RECOMMENDATIONS

“It’s a golden age to be an attacker against critical infrastructure. If you are in critical infrastructure you should plan to be targeted. And if you are targeted, you will be compromised. It’s that simple.”

Andy Bochman, Senior Grid Strategist for National & Homeland Security at the Idaho National Laboratory (INL)

Listening to ICS security experts and learning about both the extent of our vulnerabilities, as well as the skill and persistence of attackers, can be discouraging. This should not, however, be an excuse to pursue an ostrich-like defense by sticking one’s head in the sand.

Ruthless prioritization is key. Many problems exist, but not all of them need be solved at once. CyberX and other

knowledgeable vendors can provide both technology and expert professional services to help prioritize mitigation of vulnerabilities affecting the organization’s most important assets and processes.

Following are eight steps towards protecting your most essential assets and processes, based in part on the INL methodology⁴.

⁴ Andy Bochman: “The End of Cybersecurity”, *Harvard Business Review*. May 2018.

6.1 Identify Crown Jewel Processes

You can't protect everything all of the time, but you can protect the most important things most of the time. Through conversations with business owners and OT managers, identify the things you most need to protect.

What are "Crown Jewel" processes? Functions whose failure would threaten your company's very survival, for example by leading to:

- Catastrophic safety incidents
- Revenue loss (e.g., from critical manufacturing lines)
- Lawsuits and compliance violations (e.g., from safety and environmental incidents)
- Brand reputation impact (from public disclosure of breach)
- Theft of intellectual property such as data about proprietary manufacturing processes

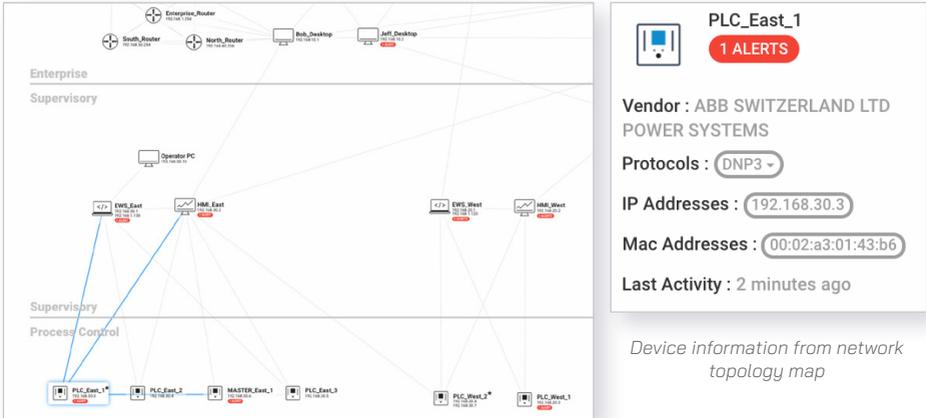
Once you've identified your "crown jewel" processes, you can use technologies such as automated ICS threat modeling,

as described in section of 5 of this report, to eliminate the most likely ways that attackers might compromise them.

6.2 Map the Digital Terrain

A key element of "knowing yourself" is knowing what hardware, software, and communications protocols are in use in your site. This includes gathering detailed information about:

- All of your ICS assets (model, type, OS, firmware revision, etc.) – and how they're connected
- How information moves through your ICS network, including to the corporate IT network
- Who touches your equipment – and how they connect to it – including both employees and 3rd-party contractors



Example of automated asset discovery and network topology mapping

PLC #9
10.2.1.9

Schneider Electric

Security Level 24%

Opened Ports

- TCP PORT 22 (SSH)
- TCP port 80 (HTTP)
- TCP PORT 502 (MODBUS)
- UDP Port 123 (Network Time Protocol)
- TCP PORT 20 (FTP)
- TCP port 20000 (DNP3)

Remote Access

- TCP port 22 (SSH) Connections from 10.2.1.17

Most Severe CVE

CVE ID	Score	Description
CVE-2015-7937	10.0	Stack-based buffer overflow in the GoAhead Web Server on Schneider Electric Modicon M340 PLC BMXNOx and BMXPx devices allows remote attackers to execute arbitrary code via a long password in HTTP Basic Authentication data.
CVE-2013-2763	5.0	Schneider Electric M340 PLC modules allow remote attackers to cause a denial of service (resource consumption) via unspecified vector

Example of detailed asset information including vulnerabilities (CVEs) and open ports

6.3 Illuminate the Most Likely Attack Paths

Schedule and perform regular table-top exercises. Use automated threat modeling to identify vulnerabilities and calculate the most likely attack paths on critical assets. Hire pen testers to identify other holes in your perimeter such as those that can be exploited via social engineering.

CyberX's automated ICS threat modeling technology incorporates proprietary analytics to continuously predict the most likely paths of attacks on ICS networks.

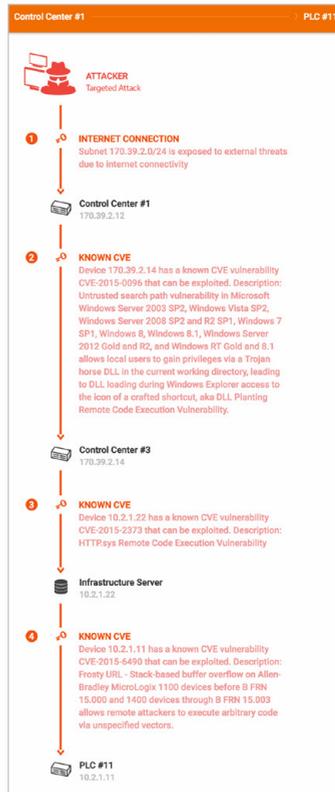
Understanding these paths and implementing mitigations for them, combined with continuous monitoring of their choke points, are primary aspects of mounting an Active Cyber Defense.

CyberX's automated ICS threat modeling uses an organization's vulnerability data, as described in this report, as input for its analysis.

The visual representation of attack vectors enables security teams to prioritize essential mitigations and simulate what-if scenarios to reduce their attack surface, such as "If I isolate or patch this insecure device, does it

eliminate the risk to my most critical assets?"

In this example, internet access via a particular subnet is used to gain initial access. The attacker then exploits a chain of known vulnerabilities to move laterally within the OT network, eventually compromising PLC #11.



Automated ICS threat modeling illuminates the most likely attack paths on your crown jewel assets



Simulating attack vectors for a critical ICS asset

6.4 Mitigate & Protect

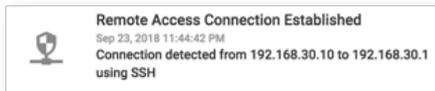
Once you have mapped and monitored the digital terrain you should have an idea of the number of ways attackers can access your ICS network. Triage these digital pathways ruthlessly – are each of them absolutely necessary? Eliminating pathways altogether may introduce some

inefficiencies into business processes but doing so is also the most effective way to keep attackers out.

We recommend implementing the following mitigations and protections:

6.4.1 Reduce number of digital pathways to a minimum

- Unauthorized internet connections
- Wireless Access Points
- Direct connections between IT and OT (that don't pass through a DMZ), such as unauthorized subnet connections and dual-homed devices
- Remote Access (VPNs): Is 2-factor authentication enforced? Are you monitoring for unauthorized remote access?

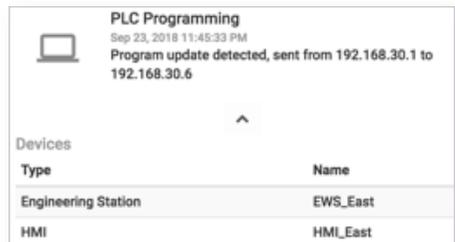


6.4.2 Identify & address ICS network and endpoint vulnerabilities

- Flat networks & lack of segmentation
- Weak passwords
- Unused open ports
- Patch Windows, Linux, and controller firmware when feasible given operational constraints

6.4.3 Implement continuous ICS monitoring

- Continuous monitoring with ICS-specific behavioral anomaly detection is essential for early detection of targeted and zero-day attacks that signature-based solutions miss
- Continuously update with the latest threat intelligence
- Integrate OT monitoring with existing SOC workflows and security stacks (SIEMs, ticketing, orchestration, analytics) for unified IT/OT security monitoring and governance
- Integrate OT monitoring with next-generation firewalls to create granular asset-based policies and rapidly block threats such as malware-infected hosts



6.5 Practice Cyber Hygiene

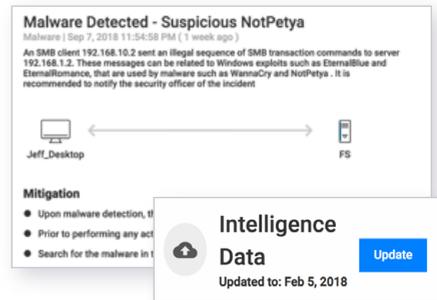
There are certain requirements that should become automatic, the way brushing your teeth is automatic to your dental hygiene habits, so should certain habits be non-negotiable. A few examples include⁵:

1. Default passwords should be changed the moment devices come online.
2. USB devices and laptops that haven't been cleaned or checked must never be inserted into the ICS network (including mobile phones connected for charging purposes).
3. No worker should ever be allowed to surf the internet from within an ICS network.

6.6 Leverage ICS Threat Intelligence

Just as Sun-Tzu advises that we know ourselves, he advises that we also know our enemy. This means staying apprised of the latest threats including ICS-specific malware, campaigns, and adversary groups. Continuously update

your monitoring systems with ICS threat intelligence data. Participate in your sector-specific Information Sharing and Analysis Center (ISAC).



6.7 Create a Manageable OS Upgrade Schedule

ICS systems are clearly more difficult to upgrade than corporate IT systems. Many ICS networks run 24x7 and have limited maintenance windows. Windows systems often host legacy applications that would need to be extensively tested or possibly re-written after an upgrade. FDA-validated systems in the pharmaceutical industry require a new cycle of validation after being upgraded.

While creating a software and hardware upgrade schedule is more difficult for OT than it is for IT, it is not impossible given the appropriate top-down attention and

⁵ For more information on defining cyber hygiene for ICS networks, see Dale Peterson's "Unsolicited Response" podcast with Marty Edwards and Michael Toecker from May 15, 2018, or read the show notes here: <https://dale-peterson.com/2018/05/23/lets-kill-or-correct-the-term-cyber-hygiene-in-ics/>

resources. Legacy Windows systems are extremely vulnerable and should be updated. Imagine what a jury would say during a corporate liability trial when presented with evidence that the plant was still running Windows 2000 or XP?

Whether the OS upgrade occurs during downtime caused by a catastrophic shut-down – or whether it happens during scheduled downtime – is, to some extent, controllable by the organization.

At the least, be aware of legacy Windows systems in your sites and implement compensating controls such as monitoring and segmentation if you can't upgrade them within the foreseeable future.

6.8 Remove Silos between OT & IT

IT and OT teams have a lot to teach each other about their respective disciplines. Management needs to create a top-down culture that fosters a belief that “we’re all in this together, so let’s help each other.”

Get people to understand that if malware or targeted attacks infect the plant, everyone suffers – downtime leads to work stoppages, a decline in stock price, and slower growth which leads to fewer opportunities for career advancement.

One way to start is by integrating OT personnel into your Security Operations Center (SOC), so that you can modify your incident response workflows for the unique characteristics of OT. Another is to assign IT security people to the OT organization for temporary assignments, so they learn firsthand how control systems work, and about the differences between IT and OT.

APPENDIX

REPORT METHODOLOGY



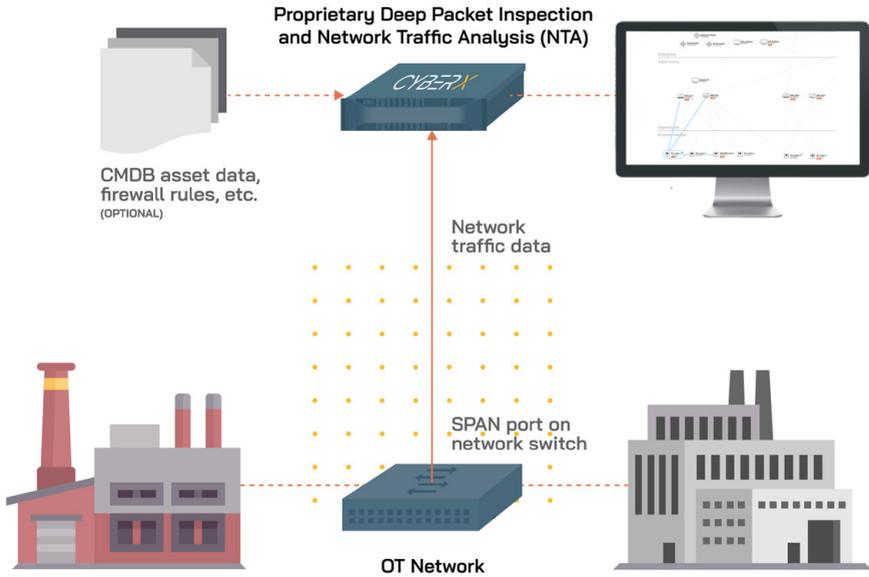
The network traffic data used in this analysis was collected through passive (agentless) monitoring of OT networks. Unlike traditional vulnerability assessment tools used in IT environments, this approach has zero impact on ICS networks and systems.

Passive monitoring entails connecting a CyberX collector appliance (physical or virtual) to the OT network via the SPAN port of a network switch, which provides a mirror of all network traffic, as illustrated in the diagram on the next page⁶.

The risk and vulnerability data are compiled using proprietary Deep Packet Inspection (DPI) and Network Traffic Analysis (NTA) algorithms. DPI examines the data part and the header of all packets traversing the network, while NTA is used to deduce information from patterns in the communication.

The CyberX platform is 100% OT vendor agnostic, and our algorithms are designed to support all industrial automation protocols (Modbus, Siemens S7, GE SRTP, etc.) and devices (Rockwell Automation, Schneider Electric, GE, Siemens, etc.).

⁶ CyberX also offers the optional ability to selectively probe (actively scan) devices, but the automated vulnerability assessments conducted for this study were completed using passive scanning exclusively.



CyberX collected traffic data from more than 850 production ICS networks and then used proprietary Network Traffic Analysis (NTA) algorithms to analyze the traffic for vulnerabilities. The analysis was performed on anonymized and aggregated metadata, with all customer-identifying information removed.

We make no claims that the findings of this report are representative of all organizations at all times, but we found the results to be fairly consistent across our sample set and believe the findings are indicative of the security posture of the industries we monitored on the whole.

ABOUT CYBERX

We know what it takes.

CyberX delivers the only industrial cybersecurity platform built by blue-team military cyber-experts with nation-state expertise defending critical infrastructure. That difference is the foundation for the most widely-deployed platform for continuously reducing ICS risk and preventing costly production outages, safety failures, and environmental incidents.

Notable CyberX customers include 2 of the top 5 US energy providers; a top 5 US chemical company; a top 5 global pharmaceutical company; and national electric and gas utilities across Europe and Asia-Pacific. Strategic partners include industry leaders such as Palo Alto Networks, IBM Security, Optiv Security, DXC Technologies, and Deutsche-Telekom/T-Systems.

Customers choose CyberX because it's the simplest, most mature, and most interoperable solution for auto-discovering their assets, identifying critical vulnerabilities and attack vectors, and continuously monitoring their ICS networks for malware and targeted attacks. What's more, CyberX provides the most seamless integration with existing SOC workflows for unified IT/OT security governance.

For more information visit CyberX-Labs.com or follow @CyberX_Labs.

CYBERX
BATTLE-TESTED INDUSTRIAL CYBERSECURITY