

# 2020 GLOBAL IoT/ICS RISK REPORT

---

A data-driven analysis  
of vulnerabilities in  
our Internet of Things  
(IoT) and industrial  
control systems  
(ICS) infrastructure

**CYBERX**  
BATTLE-TESTED CYBERSECURITY

CyberX.io

# Table of Contents

- 1.0 EXECUTIVE SUMMARY**..... 4
- 2.0 CURRENT STATE OF IoT/ICS SECURITY** ..... 7
  - 2.1 Broken Windows: Outdated Operating Systems** ..... 7
  - 2.2 Hiding in Plain Sight: Unencrypted Passwords** ..... 9
  - 2.3 Excessive Access: Remotely Accessible Devices** ..... 9
  - 2.4 Clear and Present Danger: Indicators of Threats** ..... 10
  - 2.5 Not Minding the Gap: Direct Internet Connections** ..... 10
  - 2.6 Stale Signatures: No Automatic AV Updates** ..... 11
  - 2.7 Median Security Scores by Industry** ..... 12
- 3.0 COMPARING 2020 TO 2019 DATA** ..... 13
- 4.0 DIVERSE IoT & INDUSTRIAL PROTOCOLS** ..... 15
- 5.0 FROM AWARENESS TO ACTION (RECOMMENDATIONS)** ..... 17
  - 5.1 Identify Crown Jewel Processes** ..... 18
  - 5.2 Map the Digital Terrain** ..... 19
  - 5.3 Illuminate the Most Likely Attack Paths** ..... 22
  - 5.4 Mitigate & Protect** ..... 25
    - 5.4.1 Reduce Number of Digital Pathways to a Minimum** ..... 25
    - 5.4.2 Secure Incoming Pathways** ..... 25
    - 5.4.3 Implement Continuous IoT/ICS Network Security Monitoring** ..... 25
  - 5.5 Practice Cyber Hygiene** ..... 26
    - 5.5.1 Address Weak Credentials and Unauthorized Devices** ..... 26
    - 5.5.2 Identify & Address Network and Endpoint Vulnerabilities** ..... 27
    - 5.5.3 Create a Manageable OS Upgrade Schedule** ..... 27
  - 5.6 Leverage IoT/ICS Threat Intelligence** ..... 28
  - 5.7 Enable Cooperation Between OT & IT Teams** ..... 29
- APPENDIX** ..... 31
  - Report Methodology** ..... 31
  - About Section 52, CyberX's Threat Intelligence Team** ..... 33
  - About CyberX** ..... 34

"The industrial sector is going through a 4th revolution, one that will allow industrial machines to communicate across the supply chain autonomously, creating an environment that is **more efficient, more productive, and less wasteful.**

But for the Industrial Internet of Things (IIoT) to fulfill its promise, a complete technological overhaul of the ecosystem is needed. We need advanced, security-rich solutions across connectivity, analytics, robotics, AI, and more.

**Security is essential for the success of the IIoT revolution and fundamental for any enterprise connecting its plants and production lines."**

— Qualcomm<sup>1</sup>

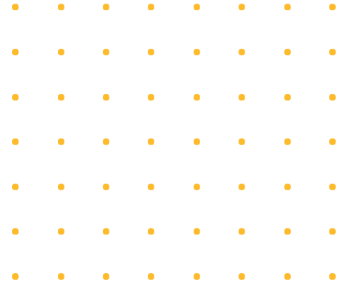
---

<sup>1</sup> Qualcomm, April 2019

---

# 1.0

---



## EXECUTIVE SUMMARY

Organizations that rely on Internet of Things (IoT) devices and industrial control systems (ICS) to run their businesses have known that their day-to-day operations, safety, and sensitive intellectual property are susceptible to compromise since Stuxnet was discovered and publicized in 2010.

This year's report analyzes data collected from 1,821 production networks using passive, agentless monitoring with patented deep packet inspection (DPI) and Network Traffic Analysis (NTA) algorithms<sup>2</sup>.

Spanning diverse IoT/ICS systems – including robotics, refrigeration, chemical and pharmaceutical production, power generation, oil production, transportation, mining, and building management systems (HVAC, CCTV, etc.) – the report is based on network data collected globally during the 12-month period spanning October 2018 to October 2019.

Unlike other reports that rely on opinion-based surveys to assess the current state of IoT/ICS security, this report is unique in presenting a data-driven analysis based on actual traffic collected from real-world networks.

---

<sup>2</sup>The 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.

Including the data presented in our previous reports, CyberX has now analyzed over 3,000 networks worldwide. This data-driven analysis of IoT/ICS security remains the only one of its kind in the industry.

**The data clearly illustrates that IoT/ICS networks continue to be soft targets for adversaries.**

These adversaries range from nation-states aiming to disrupt our critical infrastructure<sup>3</sup>; cybercriminals shutting down factories with ransomware<sup>4</sup>; nation-states looking to steal trade secrets about proprietary formulas and manufacturing processes from IoT/ICS systems (such as engineering workstations and historians)<sup>5</sup>; and nation-states and terrorists planning to cause major safety or environmental incidents<sup>6</sup>. In particular:

- **More than 3 out of 5 sites (62%) have outdated Windows systems** such as Windows 2000 and XP that no longer receive security patches from Microsoft – with the figure **rising to 71% of sites when Windows 7 is no longer supported in January 2020.**

- **Nearly two-thirds (64%) have unencrypted passwords** traversing their networks – with more than half (54%) incorporating devices that are remotely accessible via standard remote management protocols such as Remote Desktop Protocol (RDP), SSH and VNC – making it simple for adversaries to pivot undetected from a single compromised system to other critical assets.

For example, during the TRITON attack on the safety systems in a petrochemical facility operated by Saudi Aramco and Sumitomo Chemical, the adversary leveraged RDP to pivot from the IT network to the OT network in order to deploy their targeted malware.

- **Indicators of threats were observed in more than 1 out of 5 sites (22%).** Suspicious activity such as port scanning, malicious DNS queries, abnormal headers, and excessive number of connections between devices are flagged as indicators of threats. These indicators also include detection of malware such as WannaCry and Conficker, which we regularly find in client sites.

<sup>3</sup> <https://www.securityweek.com/gao-says-electric-grid-cybersecurity-risks-only-partially-assessed>

<sup>4</sup> <https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/>

<sup>5</sup> <https://www.cnbc.com/2019/09/23/chinese-theft-of-trade-secrets-is-on-the-rise-us-doj-warns.html>

<sup>6</sup> <https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html>

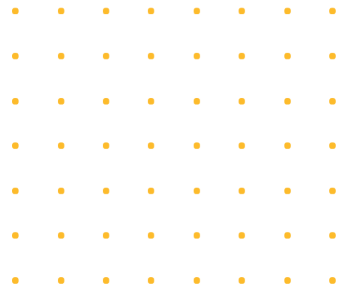
### What can be done?

This report summarizes a practical 7-step process modeled on recommendations developed by NIST as well as the Idaho National Labs (INL), both leading global authorities on critical infrastructure and ICS security. The INL process emphasizes “ruthless prioritization” of protection for your most critical systems and elimination of all unnecessary “digital pathways” to those systems.

Additionally, the INL approach recommends deploying compensating controls such as continuous network security monitoring to rapidly detect and mitigate adversaries in the initial stages of a compromise – before they shut down or blow up your facility. In the TRITON attack on the safety controllers in a petrochemical facility, for example, the adversaries were inside the network for several years before being discovered due to a bug in their code that inadvertently shut down the plant for a week.

NIST also recommends continuous network security monitoring with behavioral anomaly detection (BAD) as a key security component in sustaining business operations. In its report, NIST describes how detecting anomalous conditions can improve the reliability of ICS in addition to providing specific cybersecurity benefits<sup>7</sup>.

As the US Food and Drug Administration remarked in October 2019, without awareness of our own vulnerabilities, we cannot take steps to mitigate risk. This report, along with our previous two reports on the state of security for IoT/ICS networks and unmanaged devices, attempts to bring just such awareness to business leaders and security professionals across the globe.

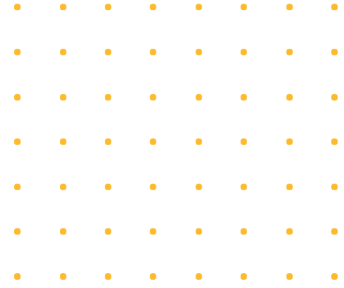


<sup>7</sup> <https://cyberx-labs.com/resources/nist-recommendations-for-iot-ics-security/>

---

# 2.0

---



## CURRENT STATE OF IoT/ICS SECURITY

Our analysis of 1,821 IoT/ICS networks, in the 12-month period ending October 2019, yielded the following findings:

### **2.1 Broken Windows: Outdated Operating Systems**

**62% of sites have outdated and unsupported Microsoft Windows boxes such as Windows XP and Windows 2000, which means they no longer receive security patches from Microsoft. The figure jumps to 71% if we include Windows 7, which reaches end-of-support status in January 2020.**

Older and unpatched Windows systems are particularly vulnerable because attackers don't need to exploit a zero-day vulnerability to successfully compromise them – they simply need to exploit known vulnerabilities that are publicly-documented in open source databases.

In 2019 there were several critical Windows vulnerabilities discovered including BlueKeep and DejaBlue, which enable attackers to gain complete control of systems by exploiting flaws in the RDP protocol<sup>9</sup>. WannaCry and NotPetya, which exploited vulnerabilities in the widely-used SMB protocol, caused

---

<sup>9</sup> <https://arstechnica.com/information-technology/2019/05/microsoft-says-its-confident-an-exploit-exists-for-wormable-bluekeep-flaw/>

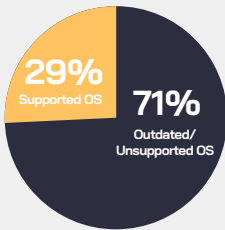
billions of dollars in financial losses from plant downtime and clean-up costs<sup>9</sup>, with NotPetya described by the US government as “the most destructive and costly cyberattack in history.”

Outdated Windows boxes are highly correlated with unpatched Windows boxes, because it is complex and disruptive – and sometimes impossible – to upgrade or patch systems in IoT/ICS environments

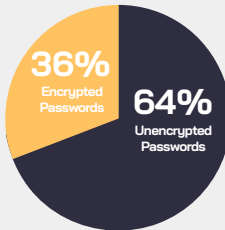
Even in the rare instances when Microsoft does introduce an emergency patch for an unsupported OS version, that doesn’t mean that organizations can easily apply the patch to their IoT/ICS systems. Because so many sites have unsupported and unpatched Windows boxes, CyberX frequently finds instances of WannaCry or even decades-old worms such as Conficker in production networks.

### Top Data Points at a Glance

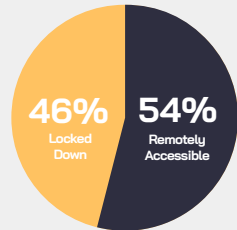
#### Broken Windows



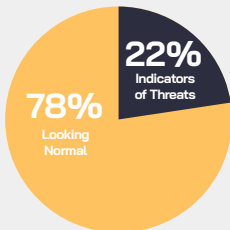
#### Hiding in Plain Sight



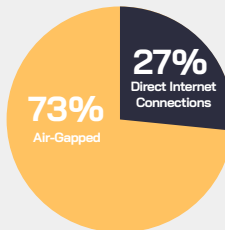
#### Excessive Access



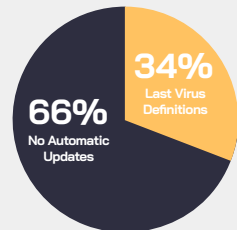
#### Clear and Present Danger



#### Not Minding the Gap



#### Stale Signatures



<sup>9</sup> <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>



## 2.2 Hiding in Plain Sight: Unencrypted Passwords.

**64% of sites have unencrypted (cleartext) passwords traversing their networks.**

The reason cleartext is dangerous is because it makes gaining access to restricted systems easy – since these passwords are transmitted “in the clear” and can easily be sniffed. Legacy devices that don’t support modern protocols such as SNMP v3 or SFTP are usually the culprits for leaving passwords in cleartext.

And unlike IT environments where policies dictate that passwords must be changed every 30, 60, or 90 days, passwords in IoT/ICS environments are rarely, if ever, changed. The combination of cleartext passwords and passwords that are rarely changed makes IoT/ICS networks ripe for targeted attacks. Once sniffed, passwords can be used to compromise additional networks or devices – or quietly perform “cyber reconnaissance” before launching an attack.

## 2.3 Excessive Access: Remotely Accessible Devices

**54% of sites have devices that can be remotely accessed using standard protocols such as RDP, SSH, and VNC.**

One of the primary attack vectors for ransomware is RDP, whereby attackers gain access by stealing remote access credentials through phishing attacks, social engineering, brute force attacks – or by simply sniffing plaintext passwords as mentioned above. Remote access enables attackers to move laterally from IT to OT networks and silently expand their presence throughout networks. In fact, US Cyber Command used similar techniques to take down ISIS sites in Operation Glowing Symphony, as reported in September 2019<sup>10</sup>.

---

<sup>10</sup><https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis>

<sup>11</sup>Indicators of Threats is a new data point that we’re introducing this year.

## 2.4 Clear and Present Danger: Indicators of Threats

### **22% of sites exhibited indicators of threats**

CyberX's network traffic analysis flags suspicious activity such as scan traffic, malicious DNS queries, abnormal HTTP headers, excessive number of connections between devices, and known malware, which we regularly detect in client networks.

In some cases this might be due to misconfigured or malfunctioning equipment – but without continuous network security monitoring, it's impossible to become aware of any suspicious activity so that it can be investigated further.

## 2.5 Not Minding the Gap: Direct Internet Connections

**More than a quarter (27%) of sites analyzed have direct connections to the internet, making them potential targets of malware, targeted attacks, and even the most basic adversarial tactics such as phishing.**

Security professionals and bad actors alike understand that it takes only one internet-connected device to provide a gateway into IoT/ICS networks for malware and targeted attacks, enabling the subsequent compromise of many more systems across the enterprise.

Anecdotally, we've found these internet connections are typically established for various reasons including obtaining software updates directly from the internet (rather than from an internal server) or providing access to third-party contractors for maintenance purposes (without using a more secure VPN) – and sometimes simply because a bored operator wants to check sports scores.

This result shows that management teams and board members should be skeptical of operations teams that respond to questions about the security of their IoT/ICS networks with the classic knee-jerk response that there's no need for concern because "our network is air-gapped." The air-gap is rapidly disappearing, and will continue to disappear as more and more IoT devices are directly connected to the cloud for data collection and analysis.

Additionally, ICS networks are almost always also connected to corporate IT networks for remote management and data collection, providing additional pathways for attackers into production networks.

Even when corporate policies prohibit connecting IoT/ICS devices to the internet, most network personnel really don't – and can't – know if their networks are air-gapped or not, unless they've already deployed continuous network security

monitoring to alert them to the presence of these connected devices.

There are simply too many third-party contractors in too many sites coming and going, and too many sensors, cameras, and other IoT devices connected to production networks, to know whether any of them are also connected to the internet.

Without continuous network security monitoring in place, claims of “air-gapping” are naive at best.

## 2.6 Stale Signatures: No Automatic AV Updates

**66% of sites are not automatically updating their Windows systems with the latest antivirus definitions.**

Antivirus is the very first layer of defense against known malware – and the lack of antivirus perhaps is another factor explaining why CyberX still finds older malware such as WannaCry and Conficker in IoT/ICS networks.

These Windows systems include critical systems such as Human Machine Interfaces or HMIs (used to monitor and control OT processes), engineering workstations (used to program controllers), and historians (used to store process information in relational databases).

In the IT world, antivirus is considered the most basic of endpoint protections. In the past, many OT vendors did not allow antivirus to run on their Windows systems, fearing it might affect the sub-millisecond response times required to control physical processes. While automation vendors have now certified certain antivirus vendors, our findings show that uptake is slow.

A possible explanation for this result is that some organizations are increasingly deploying other types of endpoint security such as application whitelisting.

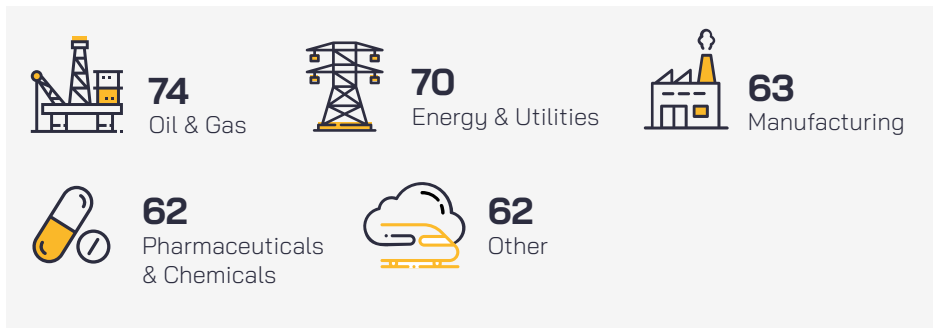
Note that embedded IoT/ICS devices such as sensors, cameras, and Programmable Logic Controller (PLCs) are considered “unmanaged” because they’re incapable of running any antivirus agents due to their limited CPU/memory resources and runtime operating systems. This is another reason why network security monitoring is required to detect attacks, by continuously inspecting the network layer for unusual or unauthorized behavior.

## 2.7 Median Security Scores by Industry

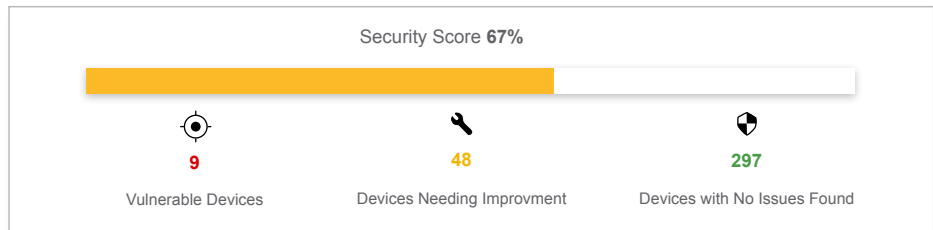
Overall, the median security score across all sites we observed was 69. We recommend a minimum score of 80 to our clients.

The scores across industries remained mostly consistent with our findings last year, with regulated industries such as energy utilities maintaining a slightly higher score than other industries.

Here is the breakdown of median security scores by industry:

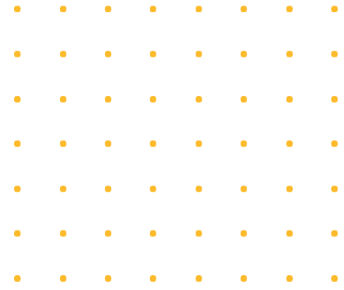


Security scores by industry. Note that organizations in regulated and semi-regulated industries such as oil & gas and energy utilities scored higher than manufacturing, chemical, and pharmaceutical industries. "Other" includes transportation, mining, and other industries.



Sample "Security Score" readout from the CyberX Vulnerability Assessment report, obtained via passive, agentless monitoring.

# 3.0



## COMPARING 2020 TO 2019 DATA

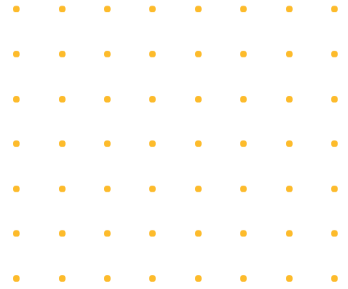
	2019	2020
Broken Windows: Outdated Operating Systems	53%	71%
Hiding in Plain Sight: Unencrypted Passwords	69%	64%
Excessive Access: Remotely Accessible Devices	84%	54%
Minding the Gap: Direct Internet Connections	40%	27%
Stale Signatures: No Automatic AV Updates	43%	66%

*Percentage of sites showing vulnerabilities related to attack surface.*

While some of the metrics appear to have improved this year, this is due to having a much higher percentage of energy utility and oil & gas sites in this year's data sample. These are typically much more locked down than in other industries such as manufacturing.

The most important data point in this year's analysis is the one showing that outdated and unsupported Windows boxes grew precipitously since our previous report, jumping from an already high 53% to a staggering 71% of sites.

This data point is arguably the “worst” news that came from this year’s analysis. Although some of the jump can be attributed to the fact that Windows 7 is now considered an unsupported OS as of January 2020, we still found that 62% of sites are running “really old” operating systems such as Windows XP and 2000.



This data point highlights the need for compensating controls such as continuous network security monitoring with behavioral anomaly detection (BAD), to quickly recognize and mitigate unauthorized or suspicious behavior, as discussed in recent NIST white papers<sup>12</sup> and SANS webinars<sup>13</sup>.

---

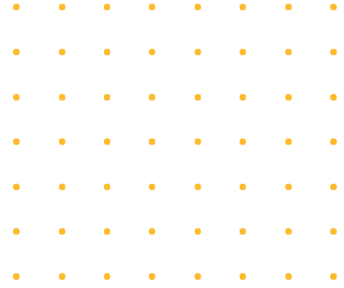
<sup>12</sup> <https://cyberx-labs.com/resources/nist-recommendations-for-iot-ics-security/>

<sup>13</sup> <https://cyberx-labs.com/event/sans-webinar-to-promote-a-principal-control-engineers-perspective-on-defending-energy-utilities-from-iot-ics-attacks/>

---

# 4.0

---



## DIVERSE IoT & INDUSTRIAL PROTOCOLS

IoT/ICS networks contain a complex mix of specialized non-IT protocols, including proprietary protocols developed for specific families of 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.

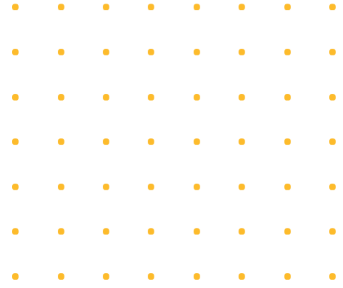




---

# 5.0

---



## FROM AWARENESS TO ACTION (RECOMMENDATIONS)

**"If you're a critical infrastructure provider, you will be targeted. And if you are targeted, you will be compromised."**

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

You can't prevent a determined and sophisticated adversary from compromising your network – so the best strategy is to eliminate as many vulnerabilities as possible while implementing mechanisms to quickly spot intruders before they can cause real damage to your operations.

Since then, the preponderance of educational outreach around best practices – combined with vivid examples of organizations whose plants were shut down by malware and targeted attacks – seem to have had a positive effect on the collective mindset of those in charge of securing our IoT/ICS networks. The fact

that demand continues to grow rapidly for IoT/ICS-aware security solutions is also a good sign, as are some of the data points covered earlier in this report.

Where many of us were blind, we now can see. As IoT/ICS-specific security solutions are installed by more and more organizations, IoT/ICS vulnerabilities that were once invisible are now in plain sight and can be mitigated in a risk-prioritized manner.

It is now well-understood that common “IT” approaches to security hardening – such as monthly patching and regular OS upgrades – don’t usually work for production networks, due to their 24x7 operations and reluctance to make any changes that might “break production.”

Faced with an endless list of “must-dos” we must face the reality that ruthless prioritization is key. This is the key principle behind the following recommendations which are based on the strategy defined by Andy Bochman of Idaho National Labs<sup>14</sup>.

## 5.1 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, 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

---

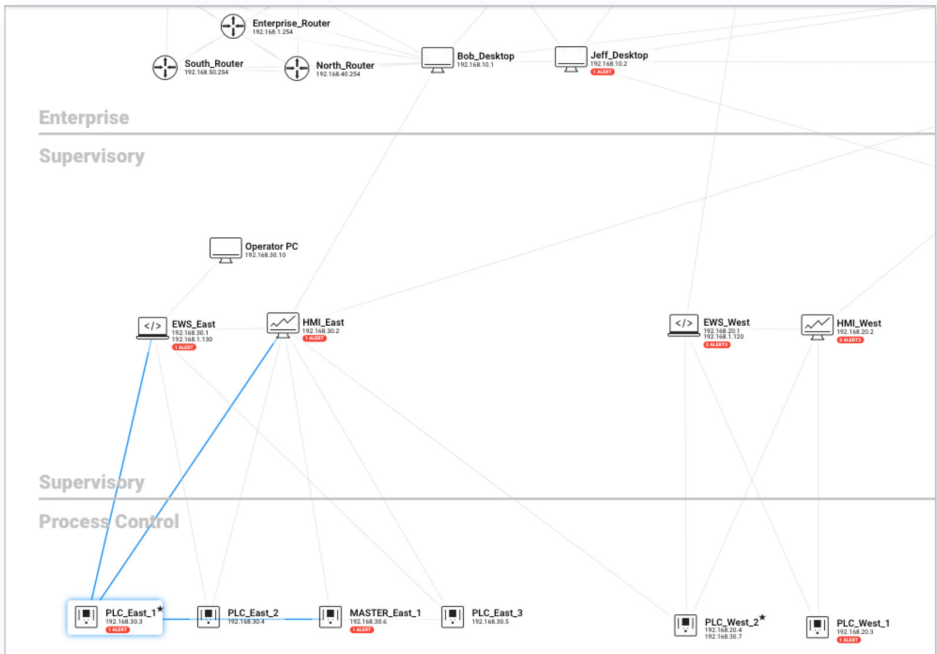
<sup>14</sup> Andy Bochman covers many of his recommendations for securing critical infrastructure in his SANS webcast here: <https://www.sans.org/webcasts/109200>. You can also read his article in the Harvard Business Review here (behind paywall): <https://hbr.org/cover-story/2018/05/internet-insecurity>.

Once you’ve identified your “crown jewel” processes, you can use modern technologies such as automated threat modeling to eliminate the most likely ways that attackers might compromise them.

## 5.2 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 IoT/ICS assets (model, type, OS, firmware revision, etc.) – and how they’re connected
- How information moves through your IoT/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\_Unit\_24**

SECURED

Type : PLC

Vendor : ROCKWELL AUTOMATION

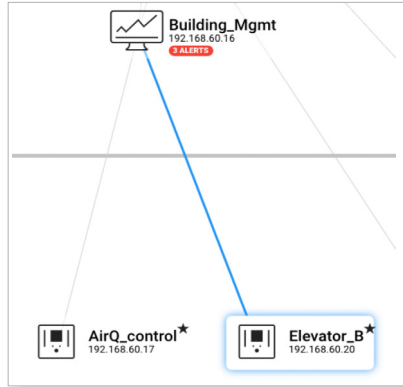
Protocols : CIP EtherNet/IP I/O

EtherNet/IP

IP Addresses : 192.168.1.131

Mac Addresses : 00:1d:9c:dc:9e:c9

Last Activity : 4 days ago



Detailed device information obtained by right-clicking on network topology map.

Automated asset discovery and network topology mapping for Building Management System (BMS).

**PLC\_East\_3**  
192.168.30.5

SIEMENS AG

Security Level 

 53%

**Ports In Use**

- TCP PORT 102 (ISO Transport)

**Most Severe CVE**

CVE ID	Score	Description
CVE-2016-9158	7.8	A vulnerability in SIEMENS SIMATIC S7-300 PN CPUs before V3.X.14 and SIMATIC S7-400 PN CPUs (V6 and V7) could allow a remote attacker to cause a Denial of Service condition by sending specially crafted packets to port 80/TCP.
CVE-2016-9159	4.3	A vulnerability in SIEMENS SIMATIC S7-300 PN CPUs (all versions including V3.2.12) and SIMATIC S7-400 PN CPUs (all versions including V7) could allow a remote attacker to obtain credentials from the PLC if protection-level 2 is configured on the affected devices.

Known vulnerabilities (CVEs) for a Siemens PLC (embedded device). The Industroyer/CrashOverride grid attack exploited a similar Denial-of-Service (DoS) vulnerability in Siemens relays.

**CCTV Conference #2**  
10.140.33.9

Sricam SP005

Security Score 

 40%

**Ports In Use**

- TCP PORT 23 (Telnet)

**Most Severe CVE**

CVE ID	Score	Description
CVE-2019-6973	7.5	Sricam IP CCTV cameras are vulnerable to denial of service via multiple incomplete HTTP requests because the web server (based on gSOAP 2.8.x) is configured for an iterative queueing approach (aka non-threaded operation) with a timeout of several seconds.

Known vulnerabilities for CCTV camera (embedded device).

**Operator's\_Station**

192.168.7.7

Windows 7

Security Score 40%

**★ Marked As Important**

**Ports In Use**

- TCP PORT 100

**Most Severe CVE**

CVE ID	Score	Description
CVE-2014-1776	10.0	Use-after-free vulnerability in Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors related to the CMarkup::IsConnectedToPrimaryMarkup function, as exploited in the wild in April 2014. NOTE: this issue originally emphasized VGX.DLL, but Microsoft clarified that "VGX.DLL does not contain the vulnerable code leveraged in this exploit. Disabling VGX.DLL is an exploit-specific workaround that provides an immediate, effective workaround to help block known attacks."
CVE-2014-1763	10.0	Use-after-free vulnerability in Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code and bypass a sandbox protection mechanism via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2014.
CVE-2014-1764	10.0	Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code and bypass a sandbox protection mechanism by leveraging "object confusion" in a broker process, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2014.
CVE-2010-2550	10.0	The SMB Server in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate fields in an SMB request, which allows remote attackers to execute arbitrary code via a crafted SMB packet, aka "SMB Pool Overflow Vulnerability."
CVE-2011-1868	10.0	The Distributed File System (DFS) implementation in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly validate fields in DFS responses, which allows remote DFS servers to execute arbitrary code via a crafted response, aka "DFS Memory Corruption Vulnerability."

**192.168.90.106**

192.168.90.106

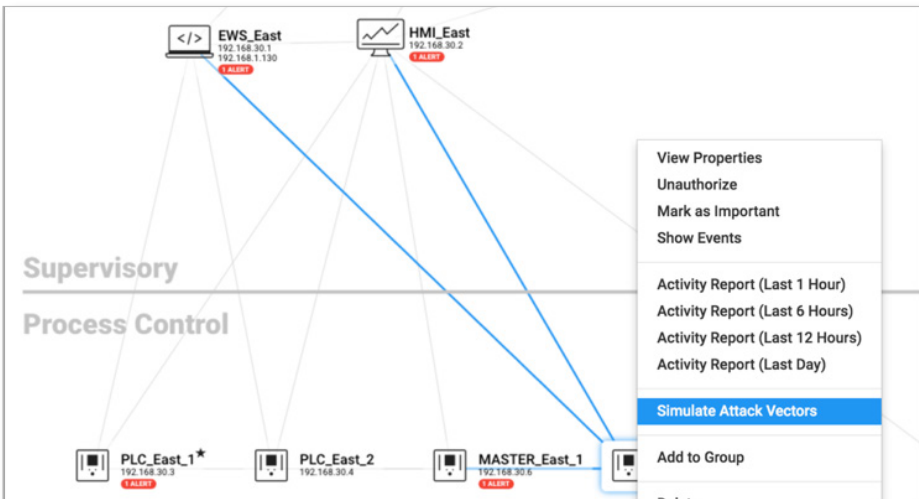
Security Score 80%

**★ 1 Unhandled Alert exists**

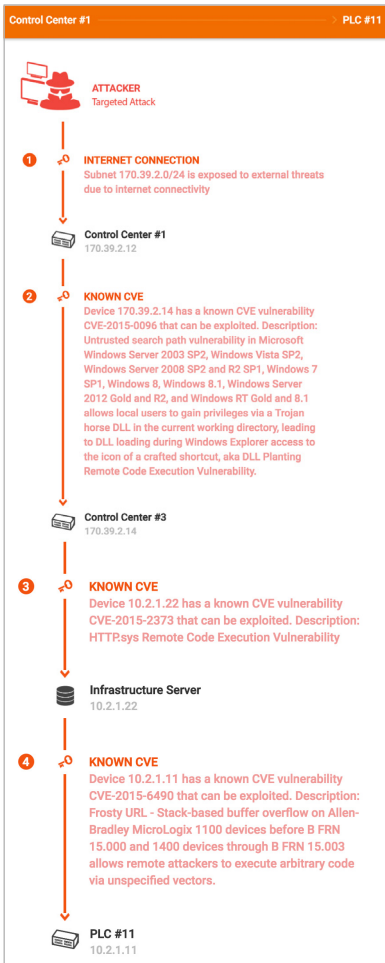
*Known vulnerabilities for Windows 7, which no longer receives security patches after January 2020.*

### 5.3 Illuminate the Most Likely Attack Paths

Once you have mapped and monitored the digital terrain, you can analyze the pathways and vulnerabilities in your assets and networks to determine the most likely attack paths to your “crown jewel” assets and processes.



Identify your “crown jewel” assets



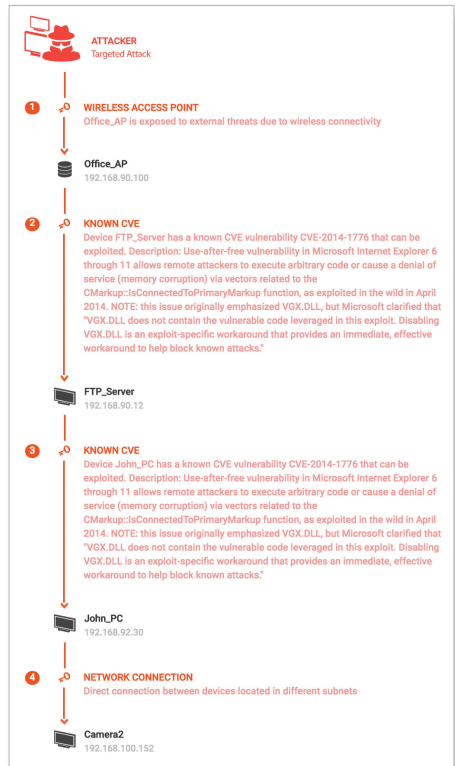
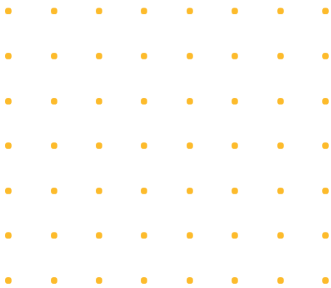
CyberX's automated IoT/ICS threat modeling technology incorporates proprietary analytics to continuously predict the most likely paths of attacks on IoT/ICS networks. Understanding these paths and implementing mitigations for them, combined with continuous monitoring of their choke points, are primary aspects of mounting an Active Cyber Defense.

This threat modeling approach uses an organization's network topology information and vulnerability data, collected via passive, agentless monitoring, 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?"

Once you've identified your "crown jewel" assets, use automated threat modeling to identify the most likely paths an attacker would take to compromise them. In this example, the targeted device (PLC #11) controls a major revenue-generating production line or a physical process whose compromise could cause a major safety or environmental incident.

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 IoT/ICS network, eventually compromising PLC #11.

Of course you should also complement automated methods with “red team” exercises to identify other types of attack vectors, such as those that can be exploited via social engineering and physical access to your facility.



Example of simulating attack vectors for IoT devices such as wireless access points and CCTV cameras. The RADIATION botnet campaign discovered by CyberX<sup>15</sup> leveraged a vulnerability in surveillance cameras, while the Mirai campaign exploited default passwords in IoT devices such as cameras, routers, and digital video recorders.

<sup>15</sup> <https://cyberx-labs.com/resources/radiation-report/>

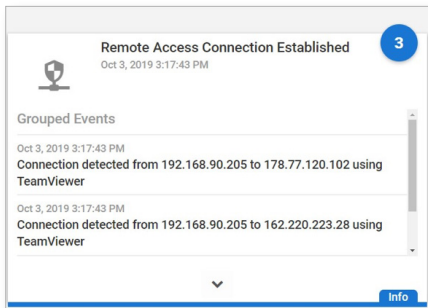


## 5.4 Mitigate & Protect

Once you have an idea of the most likely attack paths, you can take the following actions to mitigate and protect your organization.

### 5.4.1 Reduce number of digital pathways to a minimum

Triage digital pathways into your network 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. Use firewalls or unidirectional diodes to eliminate unauthorized internet connections – or simply turn off ports or unplug cables.



*Alert message indicating the establishment of a remote access connection, which may or may not be authorized.*

### 5.4.2 Secure incoming pathways

Ensure that those connections that are necessary pass through an administrator-created and monitored “De-militarized Zone” or DMZ in your network. Once this is complete, eliminate any connections between IT and OT that don’t pass through a DMZ, such as unauthorized subnet connections and dual-homed devices.

Ensure that external connections into your environment – such as from 3rd-party contractors – use Virtual Private Networks with 2-factor authentication, and credentials managed by a privileged access control solution such as CyberArk.

Once you have done this, continuously monitor your network to ensure that your SOC is alerted whenever unauthorized connections are established.

### 5.4.3 Implement continuous IoT/ICS network security monitoring

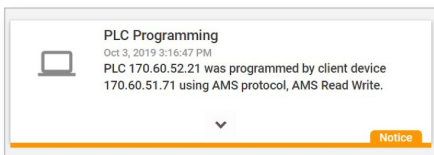
- Continuous monitoring with IoT/ICS-specific behavioral anomaly detection is essential for early detection of targeted and zero-day attacks that signature-based solutions miss
- Continuously update with the latest IoT/ICS threat intelligence

- Integrate OT monitoring with existing SOC workflows and security stacks (SIEMs, ticketing, orchestration, analytics) for unified IT/OT security monitoring and governance
- Integrate monitoring with next-generation firewalls to create granular asset-based micro-segmentation policies, and rapidly block threats such as malware-infected hosts

## 5.5 Practice Cyber Hygiene

### 5.5.1 Implement continuous IoT/ICS network security monitoring

There are certain requirements that should become automatic, the way brushing and flossing your teeth is automatic to your dental hygiene. What counts as “hygiene” is necessarily different in



*Implement continuous network security monitoring with behavioral anomaly detection (BAD) to rapidly identify suspicious or unauthorized activities. In the TRITON attack on the safety systems of a petrochemical facility, for example, the adversary inserted a remote access trojan (RAT) into the safety controllers using standard PLC programming functions.*

IoT/ICS environments than “hygiene” in IT environments.

For example, installation of antivirus and a regular patch/upgrade schedule is de rigueur in IT environments, but not necessarily possible in IoT/ICS environments. Many IoT/ICS endpoints are unmanaged and un-agentable, and some OSs are so outdated that patching them would potentially introduce instability causing intolerable effects on production or even safety.

Having said that, there are a few practices that most experts agree should be non-negotiable. A few examples include:

1. Default passwords should be changed the moment devices come online. The Mirai botnet, for example, leveraged default passwords that had never been changed in IoT devices.
2. USB devices and employee laptops that haven’t been cleaned or checked must never be inserted into the production network (including mobile phones connected for charging purposes).
3. No worker should be allowed to surf the internet from within an IoT/ICS network.

### 5.5.2 Identify & address network and endpoint vulnerabilities

- Eliminate flat networks with granular, policy-based segmentation rules that incorporate knowledge of which devices should be permitted to communicate with other devices.
- Remove weak passwords
- Eliminate unused open ports, such as remote access ports
- Patch Windows, Linux, and controller firmware when feasible given operational constraints

### 5.5.3 Create a manageable OS upgrade schedule

IoT/ICS systems are more difficult to upgrade than corporate IT systems. Many IoT/ICS networks run 24x7 and have limited or even no 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 management attention and resources.

The inescapable truth is that no matter how difficult they are to upgrade, legacy Windows systems introduce risk to your organization's people, production and profit.

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.

If you cannot update your Windows systems, ensure that you are aware of legacy Windows systems in your sites and implement compensating controls such as continuous monitoring and granular segmentation.

## 5.6 Leverage IoT/ICS Threat Intelligence

Just as military strategists today advise that we know ourselves (or equivalently, what assets are on our networks and what traffic behaviors are “normal”), they also advise that we know our enemy. This means staying apprised of the latest threats including IoT/ICS-specific malware, campaigns, and adversary groups.


You can do this by participating in your industry-specific Information Sharing and Analysis Center (ISAC). You can do this by hiring consultants with threat-hunting experience to examine your networks and websites. You can also do this using security updates from organizations that specialize in tracking IoT/ICS-specific threats.

ID: 2 📄 📥 📤 📄 📌 ✕

### Malware detected - WannaCry


Malware | Apr 12, 2019 3:49:54 PM ( 4 days ago )

Illegal SMB message was sent from SMB client 192.168.92.30 to server 192.168.92.31, using a reserved operation not allowed in the protocol. These messages are used by known malware as Double Pulsar backdoor and WannaCry ransomware.



John\_PC

↔



Bill\_PC

**Mitigation**

- Back up all important data before initiating any actions.
- Isolate the infected device.
- Search for malware in the device and quarantine it.

**Notifications**

- PCAP file exists.

Block Source
Handle

Real-time alert for known malware such as WannaCry and TRITON. Behavioral anomaly detection (BAD) is also required to detect zero-day malware based on its suspicious or anomalous behavior rather than predefined signatures.

## 5.7 Enable Cooperation Between OT & IT Teams

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

One way to do this is to simply communicate to teams in IT and OT 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.

Of course, the top priorities of plant personnel are preventing safety incidents, minimizing unplanned downtime, and continuously improving operational efficiency. By providing continuous real-time visibility into IoT/ICS assets and network behavior, network monitoring enables them to quickly spot and address risky behaviors that can cause downtime and safety incidents. It also helps them rapidly identify malfunctioning or misconfigured equipment that reduces operational efficiency, such as a misconfigured device that’s continuously in broadcast mode.

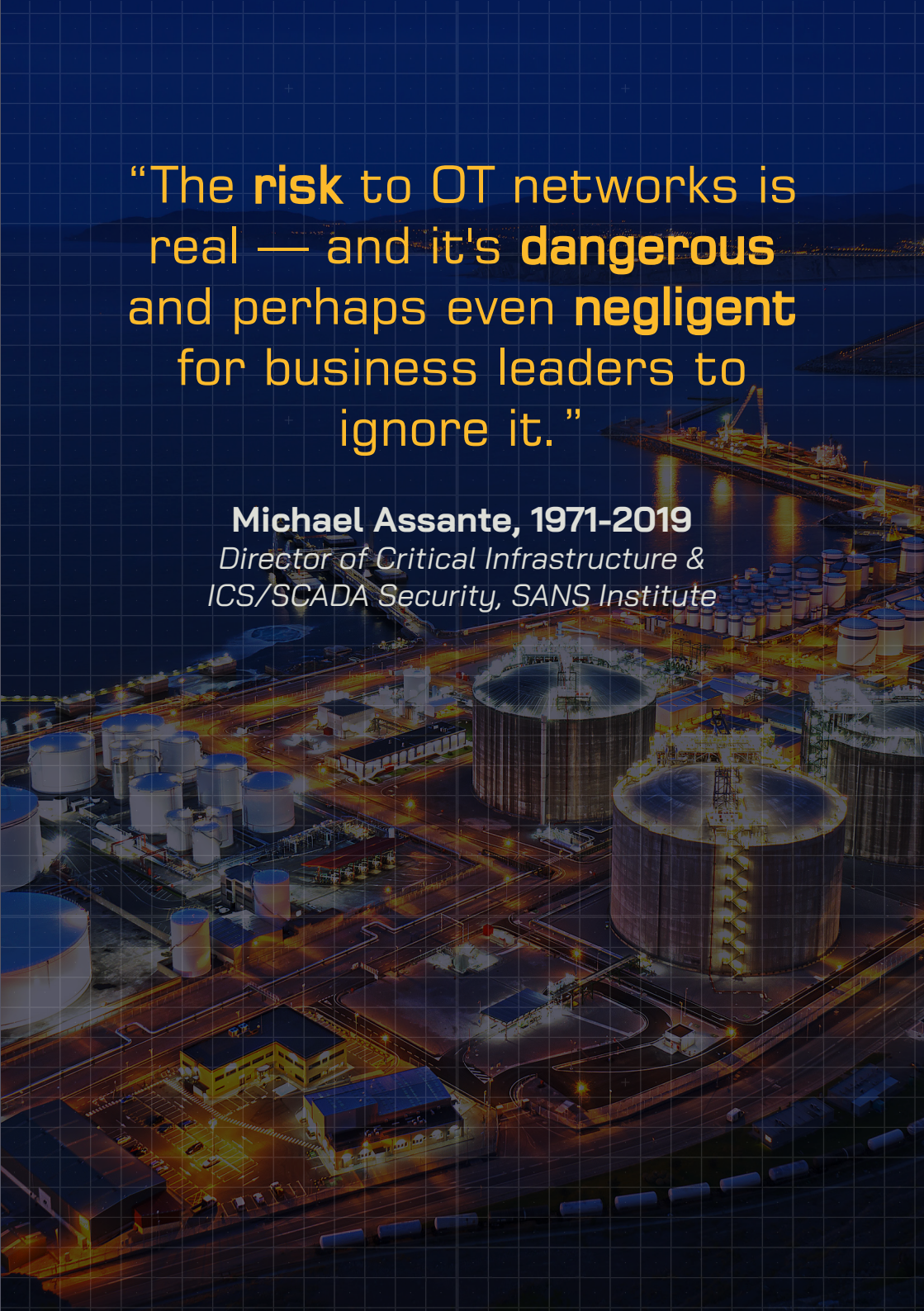
Another way to foster cooperation is to integrate OT personnel into your Security Operations Center (SOC), so that you can modify your incident response workflows for the unique characteristics of OT. Another is to assign IT security people to the OT organization for temporary assignments, so they learn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

In a SANS webinar, one pharmaceutical executive recommends getting OT personnel visibility in board meetings in which safety and security metrics are discussed<sup>16</sup>.

Finally, as one manufacturing executive noted at a recent best practices seminar, use the “Power of the Pub” to bring people together. Whether sharing a beer or breaking bread, getting people out of their silos and into social situations together often helps foster communication in ways no other top-down policy or procedure can.

---

<sup>16</sup> <https://cyberx-labs.com/webinars/sans-webinar-a-cisoss-perspective-on-presenting-ot-risk-to-the-board/>

An aerial night photograph of an industrial facility, likely a refinery or chemical plant. The scene is illuminated by warm yellow lights from buildings and piping. Several large, cylindrical storage tanks are prominent, some with ladders and platforms. In the background, a large ship is docked at a pier, with its lights reflecting on the water. The entire image is overlaid with a dark blue grid pattern.

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

**Michael Assante, 1971-2019**  
*Director of Critical Infrastructure &  
ICS/SCADA Security, SANS Institute*

---

# APPENDIX

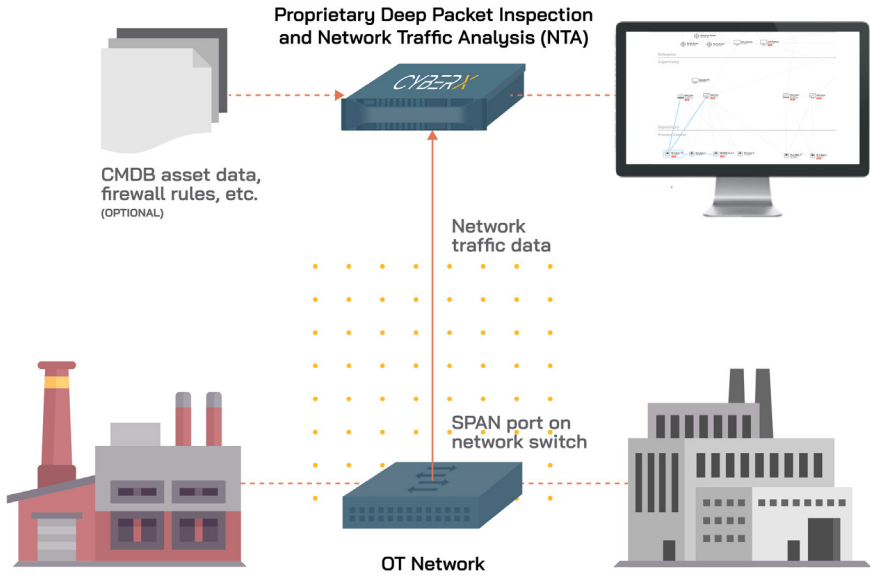
---

# REPORT METHODOLOGY

The network traffic data used in this analysis was collected through passive (agentless) monitoring of IoT/ICS networks.

Unlike traditional vulnerability assessment tools used in IT environments, this approach has zero impact on IoT/ICS networks and systems. Passive monitoring entails connecting a CyberX collector appliance (physical or virtual) to the IoT/ICS 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 page.

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% IoT/ICS vendor agnostic, and our algorithms are designed to support all industrial automation and IoT protocols (Modbus, Siemens S7, GE SRTP, OPC, BACnet, etc.) and devices (Rockwell Automation, Schneider Electric, GE, Siemens, etc.).



CyberX collected traffic data from 1,821 production IoT/ICS networks using passive agentless monitoring. We used patented deep packet inspection (DPI) and 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.



# About Section 52, CyberX's IoT/ICS Threat Intelligence Team

CyberX's Section 52 provides threat intelligence that enhances the built-in analytics of CyberX's cybersecurity platform and helps clients to stay one step ahead of potential attacks.

Section 52 is composed of world-class domain experts and data scientists who previously staffed a national military CERT defending against daily nation-state cyberattacks. The team is also on-call to perform emergency incident response for clients that have experienced an IoT/ICS compromise.

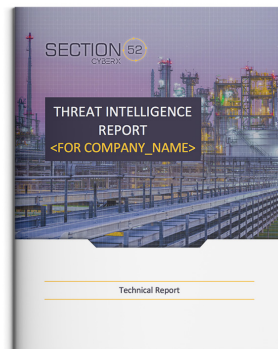
The threat intelligence report shown on this page was produced using Ganymede, CyberX's automated threat extraction platform. Ganymede continuously ingests large amounts of data from a range of open and closed sources, including the darknet and cyber threat intelligence sharing, to deliver the most robust, data-driven analysis possible.

Using machine learning and statistical models, Ganymede generates a graph database of monitored threat actor

traffic, IOCs and malicious samples. Samples are also detonated in CyberX's proprietary malware analysis sandbox.

Section 52 threat analysts are used in the final phase to review and correlate the results based on their extensive field experience.

By enabling Section 52 analysts to automatically analyze large quantities of malware samples and correlate threat indicators, this approach is significantly more scalable than traditional threat intelligence approaches that rely on human analysts and manual techniques.



# ABOUT CYBERX

## We know what it takes.

CyberX delivers the only cybersecurity platform built by blue-team experts with a track record defending critical national infrastructure. That difference is the foundation for the most widely deployed platform for continuously reducing IoT/ICS risk and preventing costly production outages, safety and environmental incidents, and theft of sensitive intellectual property.

---

Founded in 2013, CyberX is the only IoT/ICS security firm with a patent for M2M-aware threat analytics and machine learning technology. CyberX also delivers the only IoT/ICS security platform addressing all five requirements of the NIST CSF and all four requirements of Gartner's Adaptive Security Architecture.

---

Notable CyberX customers include 2 of the top 5 US energy providers; a top 5 global pharmaceutical company; a top 5 US chemical company; multiple government agencies including the US Department of Energy; as well as national electric and gas utilities across Europe and Asia-Pacific. Integration partners and service providers include industry leaders such as IBM Security, Splunk, Palo Alto Networks, CyberArk, Cisco, ServiceNow, Toshiba, HPE/Aruba, Optiv Security, DXC Technology, Singtel, 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 IoT/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.io](https://CyberX.io) or follow [@CyberX\\_Labs](https://twitter.com/CyberX_Labs).

**CYBERX**  
BATTLE-TESTED CYBERSECURITY