Microsoft

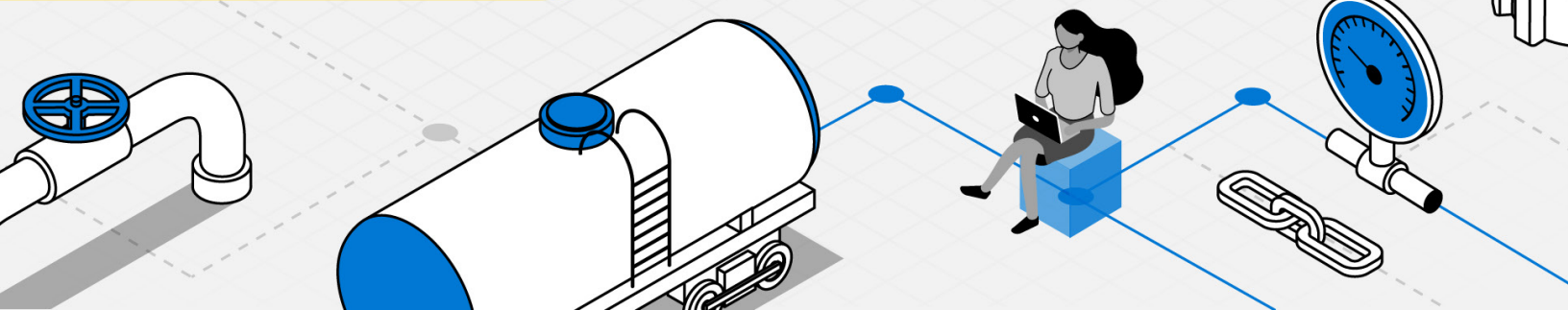
The Convergence of IT and Operational Technology:

Cyber Risks to Critical Infrastructure on the Rise

Cyber Signals

December 2022

Microsoft identified unpatched, high-severity vulnerabilities in 75% of the most common industrial controllers in customer OT networks.[1]



Introduction

The pervasiveness, vulnerability, and cloud connectivity of Internet-of-Things (IoT) and Operational Technology (OT) devices represent a rapidly expanding, often unchecked risk surface affecting a wider array of industries and organizations. Rapidly increasing IoT creates an expanded entry point and attack surface for attackers. With OT becoming more cloud-connected and the IT-OT gap closing, access to less secure OT is opening the door for damaging infrastructure attacks.

We are all cybersecurity defenders

Security Snapshot

78

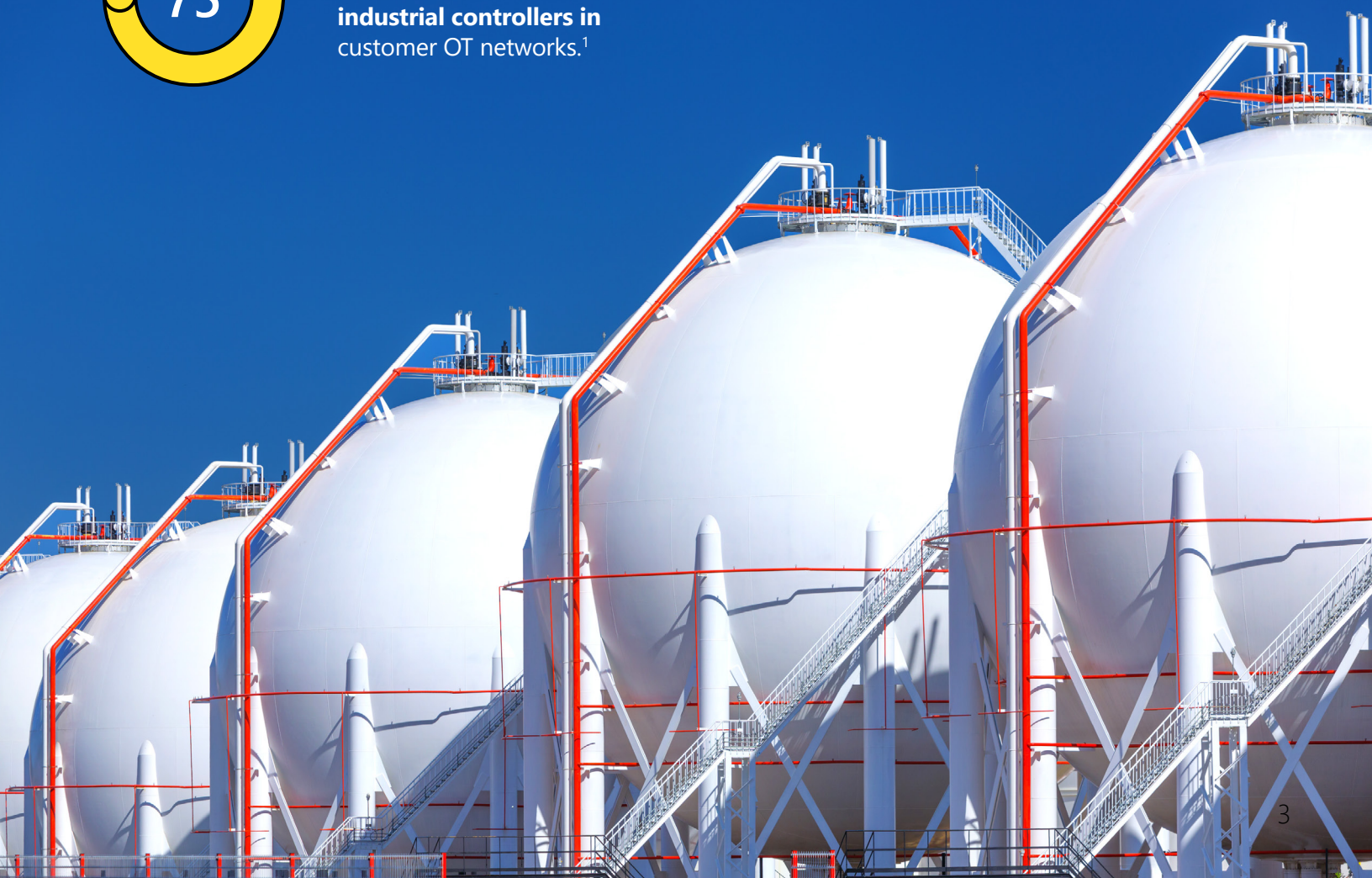
78% increase in disclosures of high-severity vulnerabilities from 2020 to 2022 in industrial control equipment produced by popular vendors.[1]

1M

Over 1 million connected devices publicly visible on the Internet running Boa, an outdated and unsupported software still widely used in IoT devices and software development kits (SDKs).[1]

75

Microsoft identified unpatched, high-severity vulnerabilities in **75% of the most common industrial controllers in** customer OT networks.[1]



Adversaries compromise internet-connected devices to gain access to sensitive critical infrastructure networks

Over the past year, Microsoft has observed threats exploiting devices in almost every monitored and visible part of an organization. We have observed these threats across traditional IT equipment, OT controllers and IoT devices like routers and cameras. The spike in attackers' presence in these environments and networks is fueled by the convergence and interconnectivity many organizations have adopted over the past few years.

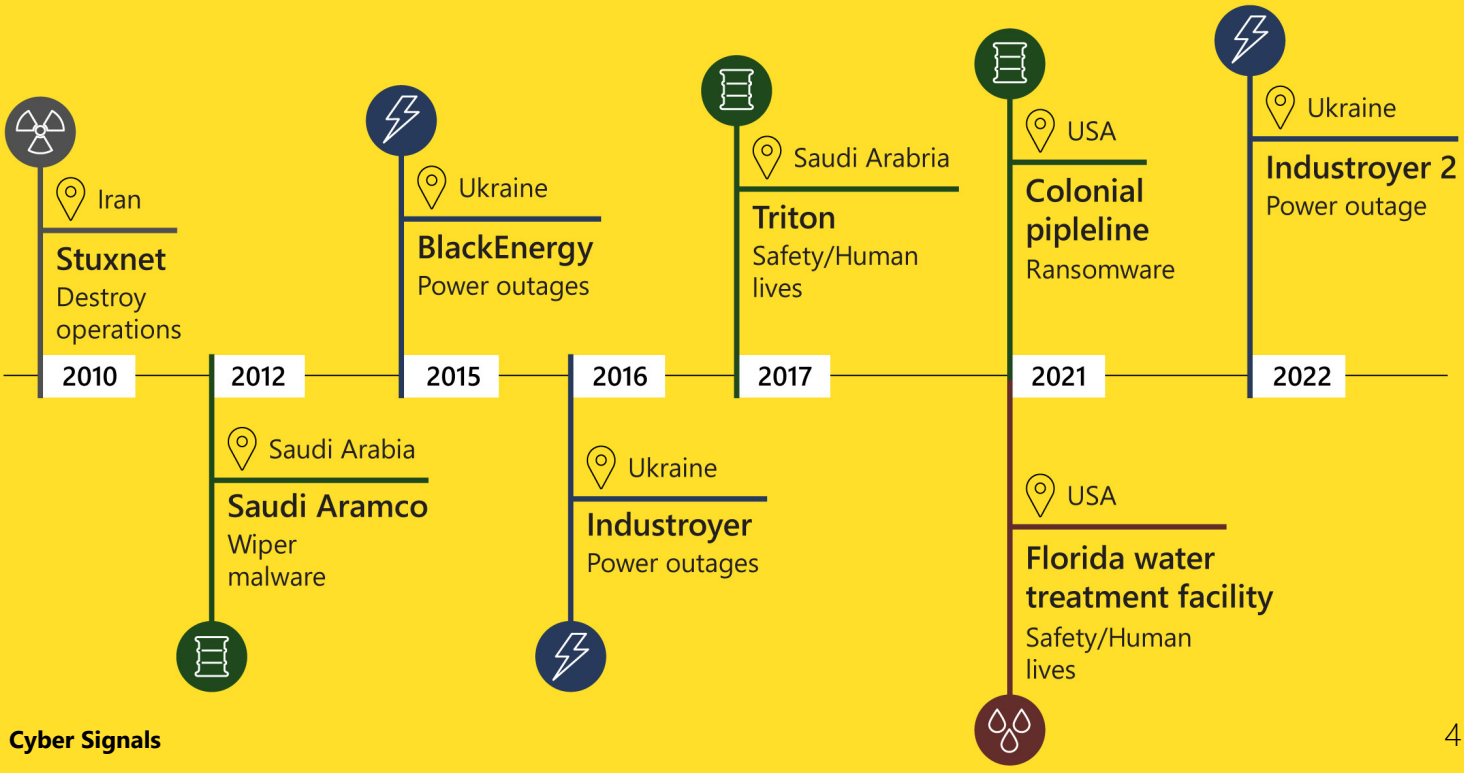
The International Data Corporation (IDC) estimates there will be 41.6 billion connected IoT devices by 2025, a growth rate higher than traditional IT equipment. Although security of IT equipment has strengthened in recent years, IoT and OT device security has not kept pace, and threat actors are exploiting these devices.

It is important to remember attackers can have varied motives to compromise devices other than typical laptops and smartphones. Russia's cyberattacks against Ukraine, as well as other nation-state sponsored cybercriminal activity, demonstrate that some nation-states view cyberattacks against critical infrastructure as desirable for achieving military and economic objectives.

Seventy two percent of software exploits utilized by "Incontroller," what the Cybersecurity and Infrastructure Security Agency (CISA) describes as a novel set of state-sponsored, industrial control system (ICS) oriented cyberattack tools, are now available online. Such proliferation fosters wider attack activity by other actors, as expertise and other barriers to entry diminish.

As the cybercriminal economy expands and malicious software targeting OT systems becomes more prevalent and easier-to-use,

Real world IoT/OT attack examples



Threat briefing

threat actors have more varied ways of mounting large-scale attacks. Ransomware attacks, previously perceived as an IT-focused threat, are today affecting OT environments, as seen in the Colonial Pipeline attack, where OT systems and pipeline operations were temporarily shut down while incident responders worked to identify and contain the spread of ransomware on the company's IT network. Adversaries realize that the financial impact and extortion leverage of shutting down energy and other critical infrastructures is far greater, compared to other industries.

OT systems include almost everything supporting physical operations, spanning dozens of vertical industries. OT systems aren't solely limited to industrial processes, they can be any special purpose or computerized equipment, such as HVAC controllers, elevators, and traffic lights. Various safety systems fall into the category of OT systems.

Microsoft has also observed Chinese-linked threat actors targeting vulnerable home and small office routers in order to compromise these devices as footholds, giving them new address space less associated with their previous campaigns, from which to launch new attacks.

While the prevalence of IoT and OT vulnerabilities presents a challenge for all organizations, critical infrastructure is at increased risk. Disabling critical services, not even necessarily destroying them, is a powerful lever.

IoT devices offer significant value to organizations looking to modernize workspaces, become more data-driven and ease demands on staff through shifts like remote-management and automation. However, in critical infrastructure networks—if not properly secured—they increase the risk of unauthorized access to operational assets and networks, giving attackers a gateway to plan large-scale attacks on sensitive equipment and devices.

Recommendations:

Work with stakeholders: Map business-critical assets, in IT and OT environments.

Device visibility: Identify what IoT and OT devices are critical assets by themselves, and which are associated with other critical assets.

Perform a risk analysis on critical assets: Focus on the business impact of different attack scenarios as suggested by MITRE.

Define a strategy: Address the risks identified, driving priority from business impact.

Defending against attacks

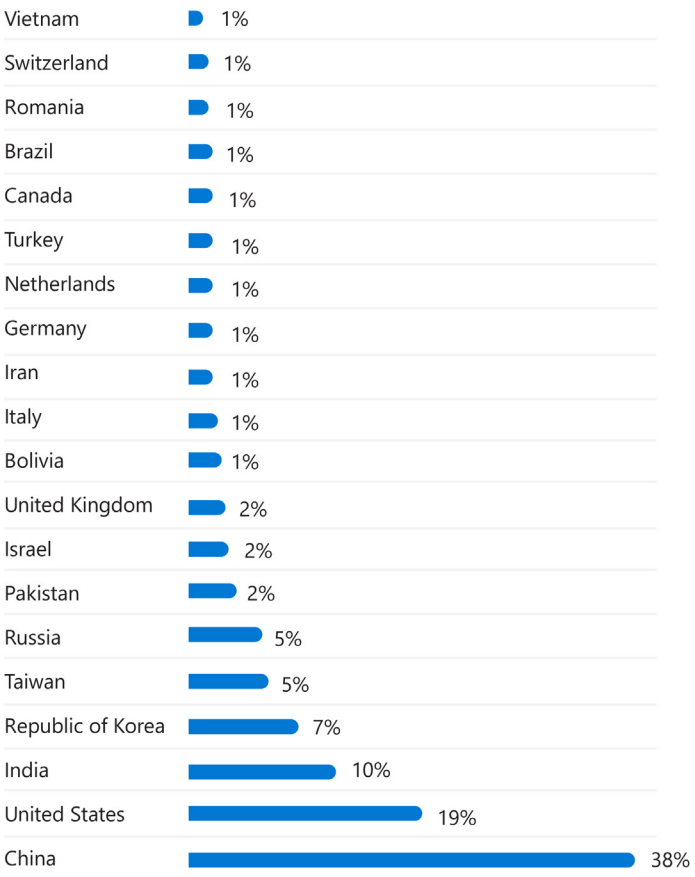
IoT introduces new business opportunities – but also great risk

As IT and OT converge to support expanding business needs, assessing risk and establishing a more secure relationship between IT and OT require consideration of several control measures. Air-gapped devices and perimeter security are no longer sufficient to address and defend against modern threats like sophisticated malware, targeted attacks, and malicious insiders. The growth of IoT malware threats, for example, reflects this landscape's expansion and potential to overtake vulnerable systems. Analyzing 2022 threat data across different countries, Microsoft researchers found the largest share of IoT malware, 38 percent of the total, originating from China's large network footprint. Infected servers in the United States put the U.S. in second place, with 18 percent of observed malware distribution.

Advanced attackers are leveraging multiple tactics and approaches in OT environments. Many of these approaches are common in IT environments but are more effective in OT environments, like discovery of exposed, Internet-facing systems, abuse of employee login credentials or exploitation of access granted to third-party suppliers and contractors to the networks.

The convergence between the IT world's laptops, web applications and hybrid workspaces, and the OT world's factory and facility-bound control systems, brings severe risk consequences by affording attackers an opportunity to "jump" air gaps between formerly physically isolated systems. Thereby making IoT devices, like cameras and smart conference rooms, risk catalysts by creating novel entryways into workspaces and other IT systems.

Top countries originating IoT malware infection during 2022



Percentages of observed outbound malware infection attempts. Country of origin (location identification) does not infer nation-state sponsored activity (actor attribution). Microsoft threat analysis of 2022 data.

In 2022 Microsoft assisted a major global food and beverage company, using very old operating systems to manage factory operations, with a malware incident. While performing routine maintenance on equipment that would later connect to the Internet, malware spread to factory systems via a compromised contractor laptop.

Unfortunately, this is becoming a fairly common scenario. While an ICS environment can be air-gapped and isolated from the Internet, the moment a compromised laptop is connected

Defending against attacks

to a formerly secure OT device or network it becomes vulnerable. Across the customer networks Microsoft monitors, 29 percent of Windows operating systems have versions that are no longer supported. We have seen versions such as Windows XP and Windows 2000 operating in vulnerable environments.

Because older operating systems often don't get the updates required to keep networks secure, and patching is challenging in large enterprises or manufacturing facilities, prioritizing IT, OT, and IoT device visibility is an important first step for managing vulnerabilities and securing these environments.

A defense based on Zero Trust, effective policy enforcement, and continuous monitoring can help limit the potential blast radius and prevent or contain incidents like this in cloud connected environments.

Investigating OT equipment requires specific unique knowledge and understanding the state of security of industrial controllers is crucial. Microsoft released an open source forensics tool to the defender community, to help incident responders and security specialists better understand their environments and investigate potential incidents.

While most think of critical infrastructure as roads and bridges, public transportation, airports, and water and electrical grids, CISA recently recommended that space and the bioeconomy become new critical infrastructure sectors. Citing the potential for disruption within various sectors of the U.S. economy to cause debilitating impacts on society. Given the world's reliance on satellite enabled capabilities, cyberthreats in these sectors could have global implications well beyond what we've seen thus far.

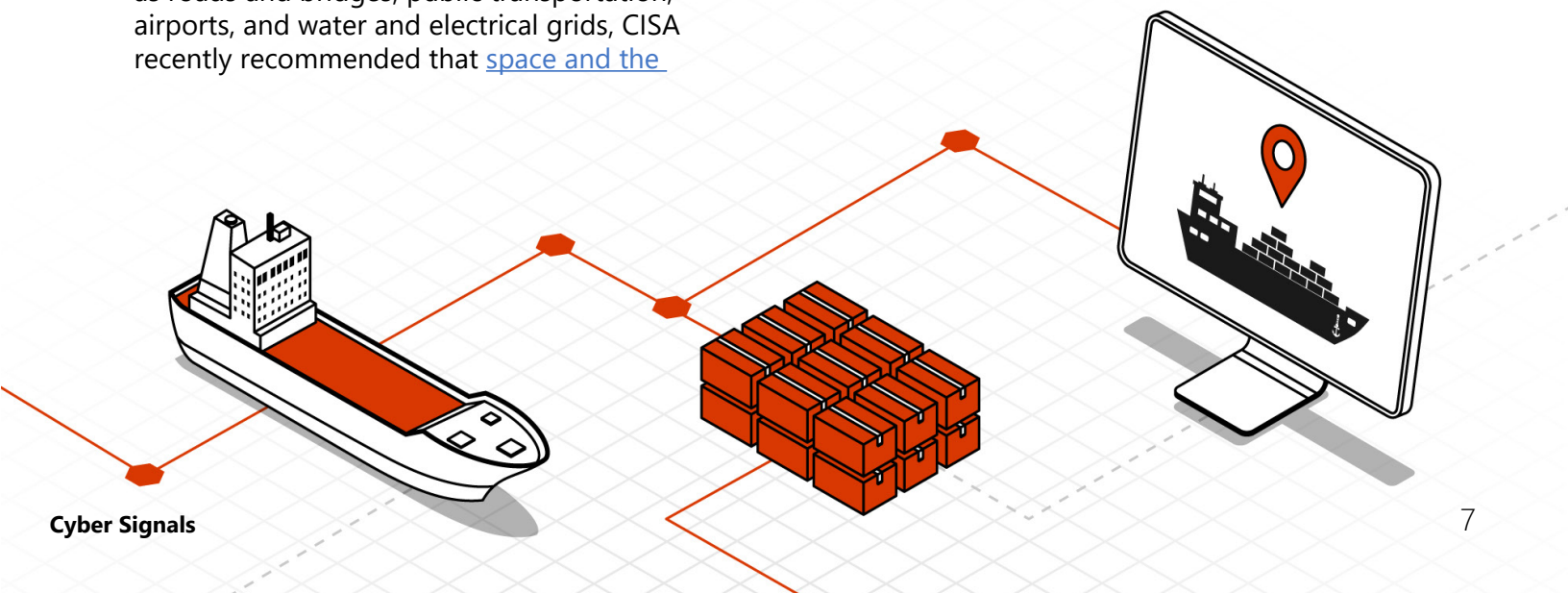
Recommendations:

Implement new and improved policies: Policies stemming from the Zero Trust methodology and best practices provide a holistic approach for enabling seamless security and governance across all your devices.

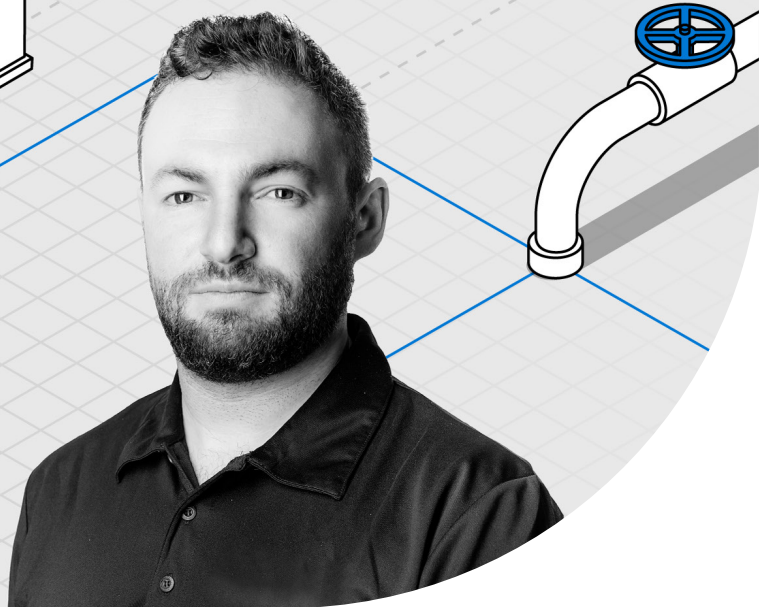
Adopt a comprehensive and dedicated security solution: Enable visibility, continuous monitoring, attack surface assessment, threat detection, and response.

Educate and train: Security teams require training specific to threats originating from or targeting IoT/OT systems.

Examine means of augmenting existing security operations: Address IoT and OT security concerns to achieve a unified IT and OT/IoT SOC across all environments.



Expert Profile



David Atch

Microsoft Threat Intelligence,
Head of IoT/OT Security Research

David Atch's security career and road to Microsoft is atypical of most, "I started in the Israel Defense Forces (IDF) in a cybersecurity role defending attacks and hunting for threats. I did a lot of incident response, forensics, and interacting with industrial control systems."

While serving in the IDF, Atch met two colleagues who would go on to found the industrial IoT and OT security firm CyberX. He was later recruited into CyberX when his IDF service ended. "I joke that I've never had a job interview. The Army doesn't interview, they just recruit you. CyberX recruited me and then Microsoft acquired the company, so I've never had a formal job interview. I don't even have a CV."

Atch's work at Microsoft focuses on matters related to IoT and OT security. It includes studying protocols, malware analysis, vulnerability research, nation-state threat hunting, profiling devices to understand how they behave in a network and developing systems that enrich Microsoft's products with knowledge about IoT.

"We're in a connected age, there's an expectation that everything should be connected to provide a real-time experience where IT software connects to a network enabling OT data to flow to the cloud. I think that's where Microsoft sees the future, where everything is cloud connected. This provides more valuable data analytics, automation and efficiency enterprises previously were unable achieve. The overwhelming speed of these devices' connected evolution, and organizations' incomplete inventory and visibility of them, often tilt the playing field to attackers," Atch explains.

That said, the best approach to combat attackers targeting IT and OT is Zero Trust and device visibility, understanding what you have in a network and what it's connected to is critical. Is the device exposed to the Internet? Does it communicate to the cloud, or can someone externally gain access? If so, do you have the means to spot an attacker's access? How do you manage employees' or contractors' access to spot anomalies?

Because patch management may be impossible in some organizations—or incredibly time consuming—and some software in the operator community is unsupported, you must mitigate vulnerabilities with other measures. For example, a manufacturer cannot easily shut down a factory to test and patch something.

"Almost every attack we've seen in the last year started from initial access to an IT network that was leveraged into the OT environment. Critical infrastructure security is a worldwide challenge and difficult to tackle. We must be innovative in creating tools and conducting research to learn more about these types of attacks.

I have to add that I don't do this work alone. The talented team of researchers, threat hunters, and defenders enable me to continue learning every day."

> **Almost every attack we've seen in the last year started from initial access to an IT network that was leveraged into the OT environment.**

Microsoft

[1] **Methodology:** For snapshot data, Microsoft platforms including Microsoft Defender for IoT, Microsoft Threat Intelligence Center and Microsoft Defender Threat Intelligence provided anonymized data on device vulnerabilities, such as configuration states and versions, and data on threat activity on components and devices. In addition, researchers used data from public sources, such as the National Vulnerability Database (NVD) and Cybersecurity & Infrastructure Security Agency (CISA). The cover stat is based on Microsoft engagements in 2022. Control systems in critical environments include electronic or mechanical devices which utilize control loops for improved production, efficiency, and safety.