Eliminate security blind spots in your IoT/OT network with Microsoft Defender for IoT

By: Ariel Saghiv - Senior Program Manager - Microsoft Defender for IoT

When Lhoist, a global leader in the mineral industry, turned on Microsoft Defender for IoT for the first time, they said it was like a blurry image coming into focus. With Microsoft Defender for IoT, an agentless network detection and response platform, all the activity in Lhoist’s complex IoT and ICS/OT network—all the devices, traffic, bandwidth usage, protocols, links and more—were brought into a single, comprehensive view. With 80 plants in more than 25 countries, and any number of heavy machinery and industrial automation equipment in each plant, just getting a handle on which devices were connected to the network would have been a major undertaking just a few years ago.

For a CISO who wishes to secure their entire enterprise, including both IT and OT environments, having visibility into the relationships between devices is as important as having a complete inventory of every connected device. Security professionals can use these insights and data to dig deep and see what connections exist between devices, enabling them to implement Zero Trust security architectures that can protect the entire network, enrich asset details in case of a security incident and enjoy a number of ancillary benefits along the way.

Protection begins with seeing the full picture

By passively monitoring the network, Microsoft Defender for IoT’s agentless platform gathers data and presents it as a visual representation of every connection and device along with important context that your Defenders need. Icons represent individual networked devices, and lines between them represent established connections. Selecting a connection brings up a dashboard showing the quantity of data being transferred between any two given points, when that data was transferred and any protocols used.
The latest version Microsoft Defender for IoT has rich details about the relationships between devices.

With continuous monitoring and rapid detection and response across cyber-physical systems, Microsoft Defender IoT knows when a new connection is established or when unusual communications take place. It then uses artificial intelligence and the knowledge gained from tens of trillions of signals analyzed each day to determine if it is legitimate and should be allowed to proceed, if suspect and should be flagged for further review, or if dangerous and should be shut down immediately. Those who monitor the network know immediately when two devices are communicating for the first time, or if one is communicating with something outside of the network on the broader internet.

Obtaining complete visibility is useful not only in securing networks and devices, but also in the case of ransomware or other attacks, should they occur. Upon receiving an alert, SecOps analysts can investigate and determine if an attack is happening. If one is, they can shut it down before the cyber criminals reach any crown jewel assets and before any widespread damage occurs.

If a network breach does occur, Microsoft Defender for IoT can help alert SecOps staff before the hackers accomplish their objective. With enhanced visibility tools, the attack vector can be followed during a post-mortem to improve security moving forward and to prevent a second attack. Microsoft Defender for IoT can show how the attackers entered the system, which lateral steps they took to bridge from the IT to OT network, what systems or proprietary information they had access to and how they ultimately shut the system down.

Visibility is a critical first step towards Zero Trust.
As the number of devices, manufacturers, connections and security capabilities grow, so does the difficulty in securing them all. With the comprehensive data picture and visual representation Microsoft Defender for IoT provides, SecOps can understand and determine which segmentation plans are needed, whether or not they are already in place, and if they are effective. Gaining visibility on this level, from the broad overview down to the granularity of an OT system’s backplane details, is what is needed to build advanced Zero Trust architectures within the network.

Ancillary benefits to securing essential devices

In the 21st century, networked IoT/OT devices have exploded and are expected to reach 30.9 billion devices by 2025. According to the Ponemon Institute, their incredible growth trajectory is a concern for security professionals. Additionally, Ponemon found that most security leaders agree that industrial systems were not designed with security in mind and that they are one of the least secure endpoints on a network.

As the benefits of connecting corporate IT networks to OT networks becomes more clear, the traditional airgap between them is rapidly disappearing. As those devices are then secured end to end from internal and external threats, it frequently has the added benefit of encouraging closer working relationships between CISOs and their COO counterparts. The two sides collaborate to maintain the practical advantages of connected networks while, at the same time, ensuring those networks do not become unprotected gateways to cyberattacks.

Lhoist has found additional benefits to monitoring and securing their networked industrial automation equipment beyond closer working relationships and network security. Their operations team now has the enhanced ability to optimize device performance and identify malfunctioning devices before they fail.

Microsoft Defender for IoT will not only alert SecOps staff when there is a potential security breach, but also let Lhoist’s production staff know when machinery is not optimized, misconfigured or malfunctioning. Together the teams found sources of congestion and unnecessary traffic such as older industrial protocols that nobody knew were still in use. They also discovered multiple subnets that should not be connected to the same switch.

Identify, protect, detect, respond, recover

Gaining visibility into all the assets, both IT and OT, connected to a network is an essential step in protecting them and it’s actually the first step in the National Institute of Standards and Technology’s (NIST) cyber-security framework which is a timeless model and approach that organizations across industries would do well to follow.

For more information on the NIST frameworks and how they can protect corporate networks, read our ebook, IT and OT convergence is happening, but is security ready? What is a CISO to do?
Gaining visibility into all the assets, both IT and OT, connected on a corporate network is an essential step in protecting them. The National Institute of Standards and Technology (NIST) has developed a framework of five pillars that all CISOs across industries would do well to follow:

1. Identify: Identify the threats that pose a risk to your organization.
2. Protect: Once vulnerable assets are identified, take steps to secure them.
3. Detect: Continually monitor all assets for unusual or suspicious activity.
4. Respond: Prepare plans in advance to respond to any detected threat.
5. Recover: Know what steps will be needed to fix impacted infrastructure and improve security moving forward.

Once assets are identified and protected, CISOs can focus on detection. Soon after Rubin Management, a major New York property management company, deployed Microsoft Defender for IoT, the platform flagged 60 new, unauthorized IoT/OT devices, trying to connect to the internet. Microsoft Sentinel, a cloud-native security information and event management (SIEM) tool, immediately responded by isolating the devices to ensure they didn’t send or receive data from the internet according to the terms of an automated playbook. Microsoft Defender for IoT also creates a detailed attack plan so that CISOs can understand what took place and restore systems to their pre-attack state.

Across industries, CISOs have found value not only in the visibility and protection capabilities of Microsoft Defender for IoT, but they have enjoyed other benefits as well. Eliminating blind spots is a first, crucial step to getting started but of course there is much more you can do.

To continue your journey towards better visualizing and securing your IT/OT environment, visit https://aka.ms/MSDefenderForIoT.