Listen to what your network is telling you: Detecting threats faster with IT/OT behavioral analytics
By Ariel Saghiv - Senior Program Manager - Microsoft Defender for IoT

Analysts estimate that there will be 37 billion industrial IoT (IIoT) devices by 2025 and, with so many connected devices, the organizational benefits and operational efficiencies industry can achieve are endless. With little visibility into those assets, however, executives are increasingly concerned with predictions like those from Gartner that suggest 75 percent of CEOs will be personally liable for cyber-physical incidents by 2024.

What, then, is a CISO to do? How can they enable the collaboration that drives their organizations forward without also allowing in criminals, corporate spies and hostile nation-states? In the midst of a global pandemic, businesses of all sizes were forced to enable remote work for their employees. Widening an organization’s digital estate in this manner inevitably introduced new attack vectors, forcing companies to shore up their vulnerable cyber borders to enhance operational resilience.

When industrial control systems (ICS) and operational technologies (OT) devices are able to be protected to a degree similar to those on IT networks, defenders can be fearless about the security in their industrial environments. After light is shed on blind spots in the network, an up-to-date behavioral analytics platform is necessary to remain ahead of the latest threats and actors. Just as important, if a threat is detected then the correct people, tools and processes must be in place to isolate and eliminate the threat.

As IT and OT converge, detecting intrusions becomes more important

In the wake of the TRITON attacks, the U.S. Cybersecurity and Infrastructure Agency (CISA) reported that many cyber criminals are using OT devices as a means to infiltrate corporate networks. The growth of IIoT devices, when combined with the lack of visibility into them, makes these devices an ideal gateway for hackers to enter a corporate network. Once in, cyber criminals can then move laterally throughout the network and potentially infiltrate IT systems. The reverse is also true: hackers can enter a network on the IT side and then seize control of OT assets.

To harden security across cyber-physical systems, on premises and in the cloud, CISA recommends creating a detailed inventory of all OT devices and then using it to prioritize those most at risk. Once complete, all identified devices need to be continuously monitored.

Microsoft’s Defender for IoT, an agentless discovery, vulnerability management and threat detection platform, provides passive, agentless monitoring with anomaly detection right out of the box. By listening to the network around the clock, no matter where individual devices are located, and no matter the size of the enterprise, threat actors can be blocked, detected and neutralized faster.

Sharper threat intelligence accelerates threat detection in OT environments

Every day, Microsoft’s Section 52 threat intelligence team has access to tens of trillions of signals, enabling the detection of threats that would otherwise slip by amidst a barrage of legitimate traffic. Microsoft not only monitors network signals, but also identity and endpoint just to name a few, providing a fuller picture and enabling the detection of threats that may slip by if only network signals were monitored. This comprehensive approach, known as Extended Detection and Response (XDR), helps Microsoft Defender for IoT stay one step ahead of
hackers by delivering intelligent, automated and integrated security across domains to CISOs and their teams.

MITRE Engenuity’s independent ATT&CK evaluations for ICS found that Microsoft Defender for IoT successfully detected 100% of major attack steps and 96% of all adversary sub-steps. MITRE simulates specific adversary behaviors and TTPs for ICS/OT applications and devices, allowing it to test solutions under real-world conditions. It also provides a common language to describe attacks on critical infrastructure in the United States and around the world, including utilities, manufacturing, pharmaceuticals, chemicals, food, oil and gas facilities, wastewater treatment plants and more.

Gartner has also given Microsoft the greatest rank on completeness of vision and scored it the highest on ability to execute in their Magic Quadrant rankings. They also praised our “strong baked-in security approach that encompasses a full stack asset-to-enterprise application approach.”

**In practice: Unknown IPs lead to an intrusion mode shutdown**

With Microsoft Defender for IoT, which is usually deployed in less than a day per site, anomalies can be detected in a matter of minutes. If, for example, an outside contractor who has access to the network connects a device that attempts to make configuration changes, Microsoft Defender for IoT can help locate and isolate the source before any damage is done.

This ability is particularly beneficial for networks that include multiple locations in far-flung geographies. When a Fortune 500 manufacturer with more than 150 facilities around the world set up Microsoft Defender for IoT, they found unexpected internal connections almost immediately.

The first real external anomaly detection test came a few months later, however, when the global IT team detected foreign IP addresses that had never been seen before. Because the security team could not identify the IPs as valid within their environment, they immediately investigated. Once everything was secure, the global team learned that the local IT security team was running a red team exercise but hadn’t informed the home office in advance.

In the wake of the incident, the global office and the local teams abroad are now better coordinated. Additionally, because Microsoft Defender for IoT encompasses both IT and OT devices when combined with a security information and event management system (SIEM), it enables joint tabletop or red team exercises with IT and operations staff. As interests converge and the line between IT and OT continues to blur, collaboration between CISOs and their COO counterparts must increase apace.

Fortunately, this manufacturer’s first attack was not a true threat, but the next one may very well be. As they learned, the convergence of IT and OT environments has greatly widened attack surface areas and increased the need for ICS/OT security that is part of integrated SIEM and XDR solutions that can stop hackers without impacting operations. It is imperative that CISOs in companies explain to their boards just how critical it is to protect valuable intellectual property, avoid costly ransoms and stay out of the headlines with advanced threat detection as part of an overall strategy to secure their industrial networks.

**Action checklist**
● Have you completed a full inventory of all connected devices?
● Are all IT and OT devices being continually monitored?
● Is the appropriate protection (e.g., segmentation) in place to ensure hackers cannot enter networks and reach crown jewel assets?

If you have said no to any of the questions above, or to learn more about how Microsoft Defender for IoT can help protect your company, visit https://aka.ms/MSDefenderForIoT.