Evolving approaches to cyber security in the age of IT/OT convergence
By Ariel Saghiv - Senior Program Manager - Microsoft Defender for IoT

For decades, industrial control systems (ICS) and operational technology (OT) have been employed in plants, job shops and other facilities around the world. As digital transformation has advanced in energy, manufacturing and other industries in more recent years, IT and OT networks have begun to converge.

There are a multitude of benefits from connecting OT and IT networks, but a substantial number of risks as well. Many machine, device and control mechanisms were not originally designed with security in mind. This creates easy access points for hackers to infiltrate systems and seize control, demand ransoms or otherwise damage a facility or company.

The benefits of networking OT and IT devices are numerous...

The traditional air gap between IT and OT networks is increasingly a thing of the past. Today, there are more vectors of attack from systems that control data and those that run machinery, switches and other industrial control systems than ever before.

Equipment can now be observed and operated remotely, providing a boon for those for COOs and their teams. Whether on site or around the world, production can be monitored, malfunctioning equipment can be detected and problems can be resolved quickly and easily.

…but it creates huge new security gaps.

While OT networks that are increasingly connected to the IT network make life easier on the operations side, they often have the unintended consequence of making a CISO’s job more difficult. These systems were engineered to perform a specific function in the physical world but, all too often given the traditional air gap and assumptions about network segmentation, were not designed to be secured against hackers.

OT devices often operate in relative isolation. They frequently use niche protocols to communicate and, given the silos that often exist in large organizations, are a security blind spot for CISOs and even the operations team. Given this, they present soft targets for hackers and cybercriminals who can use them to move laterally throughout the network until they find a more interesting asset to attack. Companies who do not take adequate steps to harden network borders and the devices themselves are at risk of espionage, ransomware and even physical attacks.

CISOs are taking steps to secure their soft cyber perimeters

Boards are increasingly assigning CISOs the responsibility of securing OT networks in addition to their traditional IT responsibilities. In organizations that have not yet taken this step, forward-
thinking CISOs are proactively communicating to their boards the importance of protecting the business by taking these steps. If they don’t, a hacker who breaches a converged OT and IT environment can cause substantial damage to physical plants, human safety, brand reputation and the bottom line.

**Microsoft Defender for IoT** provides continuous, agentless monitoring of all devices and systems on a network, whether they are OT or IT. Microsoft Defender for IoT can usually deploy in less than a day and can begin monitoring network signals, endpoints and user identification signals immediately with extended detection and response capabilities from Microsoft’s Section 52.

In addition to security, Microsoft Defender for IoT also offers a number of operational and cultural benefits as well. If a device begins to malfunction, the first signs of it may appear on the network. Microsoft Defender for IoT will alert the SOC team of the issue so that the operations team can reconfigure the device and keep it running at peak performance. Bringing the IT and OT teams closer together helps to tear down silos, improve corporate culture and enhance business outcomes.

**Microsoft Defender for IoT can add value the very first hour**

The operational and security results from deploying Microsoft Defender for IoT can be dramatic. A global manufacturer in the energy industry saw their attack surface area, and thus risk, quickly grow as they continued to add OT and non-OT devices to their OT network. With more than 150 facilities worldwide, simply getting a handle on what unmanaged industrial IoT (IIoT) devices they had in service proved to be a challenge.

Once Microsoft Defender for IoT was switched on, the team was able to see what the Global Director of Manufacturing Technology called a “mess” in the network. He added that the asset and network map that Microsoft Defender for IoT generated in the first hour was equally valuable in those early days.

Within weeks, however, it became clear that some facilities were far more secure than others. In those where additional security was needed, the operations teams pushed back against the mitigations recommended by Microsoft Defender for IoT until they understood the reasons behind the changes they were being asked to make. When the SOC team explained the relationship between their unsecured OT equipment and the risk of an attack, including one that may result in plant downtime, the OT engineers were convinced of the need for changes.

**OT environment protection in a connected world**

With each passing day, our world grows more connected. With 37 billion IIoT devices predicted to be in service by 2025, the number of targets for cybercriminals to exploit is going to increase dramatically. This growth is taking place around the globe and in a wide swath of industries,
likely including yours. Taking steps to secure unmanaged assets through an effective, easy-to-deploy platform like Defender for IoT is the minimum each CISO should do to protect their people, profits and production today.

For more information on how Microsoft Defender for IoT can help secure your IT/OT network, visit our landing page today.