Microsoft Security

Microsoft Defender for IoT secures American utility's OT network

Power and utilities companies are turning their attention to the growing attack surface area within their operational technology (OT) footprint – including power plants and connected customer devices like solar, storage and EVs, and their vast transmission and distribution networks.

After a major American utility gained visibility into its IT network with a Security Information and Event Management (SEIM) system, the company turned its attention to the OT network running their energy plants. Without a complete picture of which OT devices were connected to their networks, this US power company was vulnerable to cyberattacks that could cause safety or environmental incidents, or even bring down the company.

Their timing could not have been better as the company was constructing a new liquified natural gas terminal. Microsoft Defender for IoT was deployed and operational even before the terminal network went live. The company now has wholistic protection across their OT/IT infrastructure, and in both their new and old facilities.

Continuous visibility into all connected assets

Microsoft Defender for IoT lets the company see what assets they have and gives them insight into how they are connected and how they are communicating with one another. This dynamic inventory of connected devices facilitates the creation of prioritized to-do lists to more effectively mitigate vulnerabilities and protect crown jewel assets.

By continuously monitoring the network, Microsoft Defender for IoT generates real-time alerts when one of those devices begins communicating with an unauthorized device, either inside or outside of the network. Security Operation Center (SOC) staff are also notified as new devices are connected, unauthorized programing changes are made to programmable logic devices, destructive malware is found or cyber reconnaissance activity is detected.

The company's SOC can also integrate information from Microsoft Defender for IoT and their SIEM to more effectively combat threats that can cross IT/OT borders. This unified approach enables the company to leverage existing investments in human capital, runbooks and workflows to enhance security monitoring and governance.

Microsoft Defender for IoT also streamlined the company's workflow for North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) compliance monitoring and reporting. Producing inventories of assets can now be done automatically, more frequently and much more quickly than when done manually.

Continuous visibility into all connected assets

The Defender IoT platform also has the added benefit of helping break down the organizational silos between the IT and operations departments. The SOC integration workshops held by the US power company helped their teams better understand the needs and vocabularies of their counterparts. This made closer working relationships possible, which led to a more secure company overall.

With the closer coordination between the two sides of the house, Microsoft Defender for IoT is now used to enhance day-to-day operations in addition to providing vital cyber security protections. For example, when the platform detected a network packet storm, IT engineers used Microsoft Defender for IoT's Event Timeline to pinpoint the specific devices causing trouble. When OT engineers checked, they found misconfigurations that were saturating the network and consuming too much bandwidth.

Perhaps most importantly, the company now has centralized command-and-control over all their OT networks. The team has all network topology and activity in a single view and can use that data to make their networks more efficient. Anomalies are detected, flagged and resolved more quickly, and better security procedures are rapidly put into place to prevent intrusions.

As the power and utilities industry continues its digital transformation, and as OT and IT networks continue to converge, it is increasingly essential to protect assets across the business. Thanks to Microsoft Defender for IoT, this Fortune 500 company is now better able to protect their networks, and the consumers who depend on them, from cyberattacks.

For more insights on how Microsoft Defender for IoT benefits the power and utility industry, visit the power and utility landing page today.

Microsoft Security