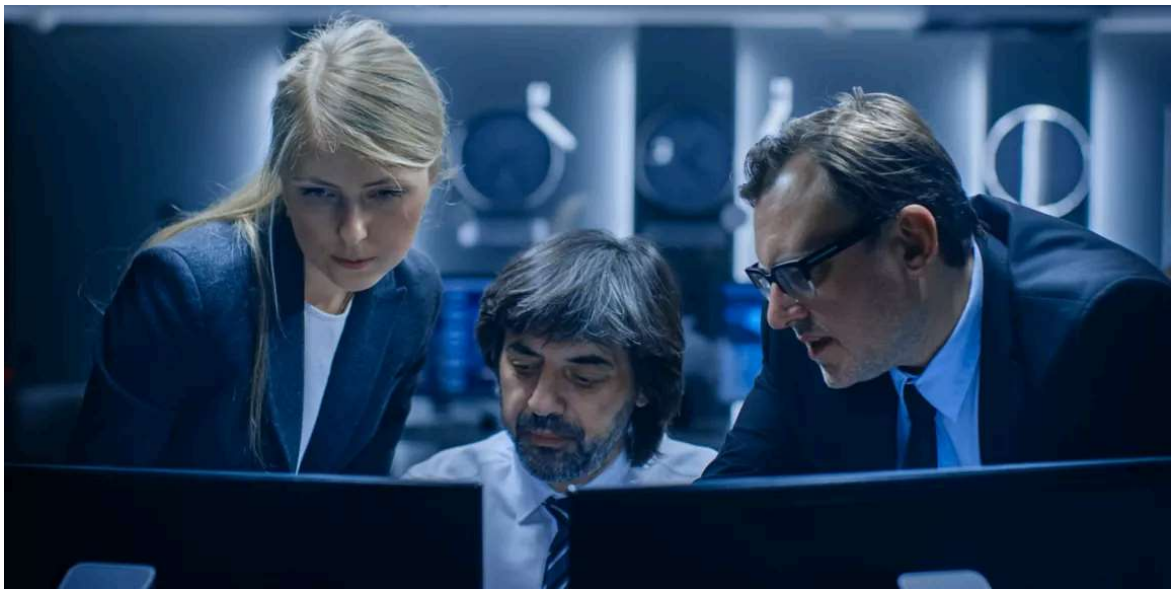

Do You Know How Vulnerable Your OT Environment Is?

The Rise of Cyber Threats to OT Systems

Operational technology (OT) systems are essential for running critical infrastructure and industrial processes. But they are also increasingly exposed to cyber threats that can disrupt operations, cause physical damage and even endanger public safety. According to a report by the Ponemon Institute, the average cost of a cyber breach in critical infrastructure is now $4.5 million, and 75% of OT organizations experienced at least one intrusion in the past year.[1]

So, how can you improve protections for your OT assets and operations from cyber attacks?

The first step is to gain visibility into your OT network and identify all the devices, systems and vulnerabilities that hackers could exploit. Without this visibility, you are flying blind and leaving your OT environment open to attacks.

A Challenge Close to Home

This is the challenge that Honeywell faced when it needed to improve security for its own manufacturing environment. With over 400 facilities that depend on OT, each of Honeywell's sites has a complex and diverse mix of OT assets, such as industrial control systems (ICS), CNC devices, test devices and more. Honeywell initially used an off-the-shelf cybersecurity solution to help monitor its OT networks. However, it soon realized that this solution was not effective enough to help detect and prevent cyber threats.

The solution could not accurately identify and classify many of the OT assets on the network, leaving almost half of them unclassified and undocumented. This created a huge blind spot for potential attackers to infiltrate and compromise the OT environment. Moreover, the solution generated a lot of noise and false positives, making distinguishing between normal and malicious activity hard. Implementing and configuring the solution at each site took a long time, which was not feasible for Honeywell's scale and scope.

Customer Zero: Cyber Insights Is Born

Honeywell switched to its own OT cybersecurity solution, based on its extensive experience in the OT space. The solution, Honeywell Forge Cybersecurity+ | Cyber Insights, is purpose-built for OT environments and designed to provide comprehensive visibility, control and resilience of OT networks.

Cyber Insights effectively met Honeywell's requirements for its OT cybersecurity solution. It is designed to discover and classify all OT assets on the network, providing a more accurate and complete inventory of the OT environment. It is also designed to be able to passively monitor and detect any malicious or anomalous activity on the network, sending alerts and flags to the security team. It was also capable of identifying each asset's version and patch status, helping to prioritize and remediate vulnerabilities.

Using Honeywell's Cyber Insights, Honeywell was able to reduce the noise and false positives that plagued the previous solution, providing a more reliable and accurate picture of the OT network. It also significantly reduced the time and effort required to implement and configure the solution at each site, making it more scalable and efficient for Honeywell's needs.

Using Cyber Insights, Honeywell improved its visibility, control and resilience of its OT environment enhancing its protection against cyber threats. This solution helped Honeywell prevent unnecessary shutdowns, revenue losses and safety risks associated with cyber attacks.

Ensure Robust Protection for your OT Environment

If you want a similar solution for your OT environment, consider Honeywell Forge Cybersecurity+ | Cyber Insights. This solution is designed to help you improve your security posture and readiness for your OT assets and operations, as well as help you prevent and respond to cyber attacks that could jeopardize your critical infrastructure.

Contact us today to learn how we can help you protect your OT environment with Honeywell Forge Cybersecurity+ | Cyber Insights.

[1] Ponemon Institute - Cost of a Data Breach Report, 2023. 2. EPA Fact Sheet, Understanding the Impact of EPA's Prosed Rules for Chemical Plants. 3. NIST2 Cybersecurity Directive 2024.

First Name: *

Last Name: *

Business Email Address: *

Company/Organization: *

Job Title: *

Topic of Interest: *

Select...

Industry: *

Select...

Direct Phone:

Country/Region: *

Select...

Feedback