CYBER INSIGHTS HELP IDENTIFY AND REMOVE UNAUTHORIZED ASSET ON INDUSTRIAL NETWORK

Case Study

Overview

A large manufacturing facility in the United States experienced a serious cybersecurity breach when an unauthorized asset was connected to their industrial network on their level two environment. While other security technologies in place failed to catch the issue, Honeywell Forge Cybersecurity+ | Cyber Insights was able to quickly detect the rogue device and alert the customer to take immediate action.

CUSTOMER CHALLENGE

As a maker of advanced technology used in the automation industry, this industrial company was faced with a critical challenge of maintaining safe and continuous operations while actively monitoring its operation technology (OT) network for signs of a cyber breach. To help overcome this challenge, the company had deployed a number of security technologies and controls including a Security Operations Center (SOC) to help monitor its OT network. To support Its SOC, the company had acquired Honeywell's Cyber Insights to help identify all assets connected to the network as well as monitor network traffic.

For more information on Cyber Insights:
Contact you local Honeywell representative or visit us at www.becybersecure.com

Anonymous Cyber Case Study | Rev 1 | 09/24

Honeywell

CYBER INSIGHTS WAS THE ONLY SOLUTION AT THE CUSTOMER SOC THAT UNCOVERED AN UNAUTHORIZED REMOTE CONNECTION

One day in the summer of 2024, the company's onsite cybersecurity leader received an alert that was generated by Cyber Insights. It called out the need to investigate a "TeamViewer connection established" on the industrial network at level two. Multiple security controls including the DNS, firewalls and other third-party solutions, as well as a multitude of other logs ingested by the SOC, did not Identify the alert that Cyber Insights had uncovered.

> *"We are very impressed that only Honeywell Cyber Insights was able to uncover this unauthorized asset and connection on our industrial network."*
>
> Cybersecurity Site Leader

After a quick investigation, it was determined that an employee was using their home device to access TeamViewer remote desktop into a NUC (short for "Next Unit of Computing", a small box-shaped computer) located on a non-managed VLAN. This device was neither purchased by the company nor was it on the known inventory of assets kept by the company's IT team. In fact, it was a rogue device that had need been known before. As a result, it was not being scanned or ever seen by the company's SOC VM discovery in weekly scans or by the IT team's daily vulnerability scans. It was onboarded with Microsoft Defender for Endpoint to receive policies, and most importantly, not the SOC team.

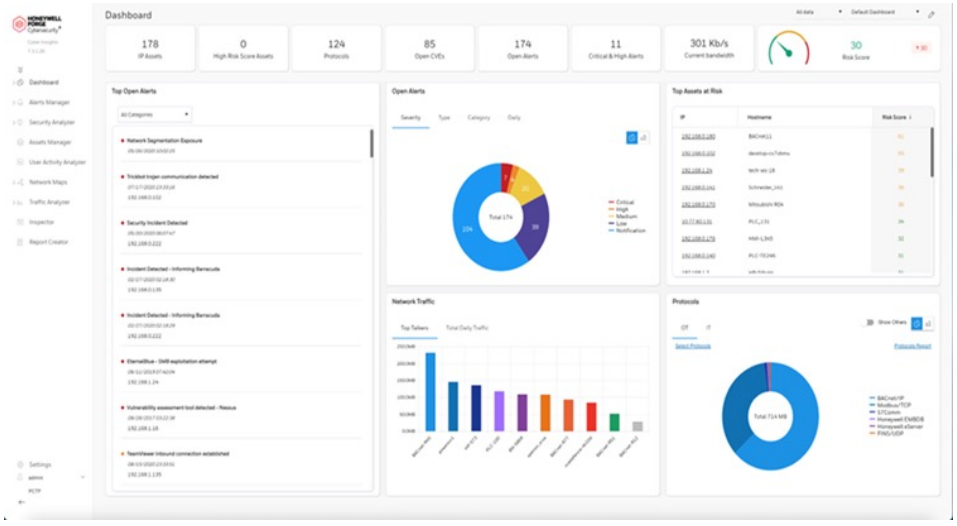
The device was 100% rogue in all senses of the word. Honeywell's Cyber Insights solution was the only cybersecurity solution utilized by the customer that identified it as external to internal traffic, as it was using a Remote-Control Desktop it was flagged. All the company's other tools/monitoring technologies in place failed to detect the rogue device. With the help of Cyber Insights, the IT team then performed an analysis of the asset and determined it was not listed in their inventory based on MAC Address. As a result, the team took action to block it from the network.

AN EMPLOYEE WAS THE CULPRIT

After further investigation, it was revealed that that a company employee had set up the connection to the unauthorized device on the network, which was against company policies. Although no real harm came to the network, the opposite may have come true if this was a disgruntled employee or some other attacker able to social engineer their way onto the network at the facility. "Thanks to Honeywell's Cyber Insights, we were able to quickly identify the rogue asset, it's details including MAC and IP connection, to then take fast action in terminating any connection to the internet and the OT network," said the customer's OT cybersecurity Leader on site. "We are very impressed that Cyber Insights was able to uncover this unauthorized asset and connection on our industrial network when our other cybersecurity solutions did not".

GET BETTER INSIGHT INTO YOUR CYBERSECURITY POSTURE WITH CYBER INSIGHTS

Honeywell's Cyber Insights is one of the most comprehensive cybersecurity solutions for OT and IoT networks. It is designed to help customers discover and inventory all the assets in the network, provide comprehensive information about the site's cybersecurity posture – including known exploited vulnerabilities and active threats relevant to the site - and then investigate suspicious activity.



Cyber Insights is a software solution and the foundation for must-have visibility into cyber risk/posture

For more information on Cyber Insights:
Contact you local Honeywell representative or visit us at www.becybersecure.com

Anonymous Cyber Case Study | Rev 1 | 09/24

Honeywell