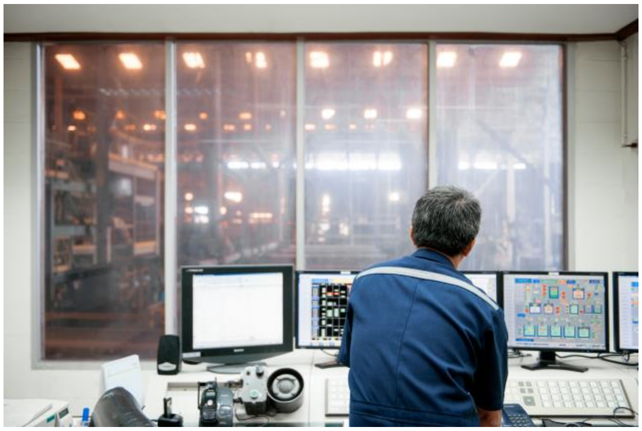
HONEYWELL FORGE CYBERSECURITY+ | CYBER INSIGHTS

PRODUCT INFORMATION NOTE

When it comes to protecting industrial assets from cyber attacks, knowledge is power. However, turning data into information and knowledge is an ongoing challenge for many in the operational technology (OT) space, especially if information technology (IT) solutions are their only tools. What is needed are OT-specific solutions, such as Honeywell Forge Cybersecurity+ | Cyber Insights, designed by OT cybersecurity professionals to help better protect the unique OT environments worldwide. With actionable and targeted OT cybersecurity insights, this on-premise and vendor-neutral solution is designed to provide customers with access to real-time data on assets, threats and vulnerabilities to help them reduce cyber risks and maintain normal operations.



GET BETTER VISIBILITY TO OT CYBERSECURITY POSTURE

Honeywell Forge Cybersecurity+ | Cyber Insights is one of the most comprehensive cybersecurity solutions for OT and IoT networks. It is designed to 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 help investigate suspicious activity. As one of the leading solutions for improving OT network security, the solution is capable of providing superior insights into a site's assets, vulnerabilities, cybersecurity threats and operational failures.

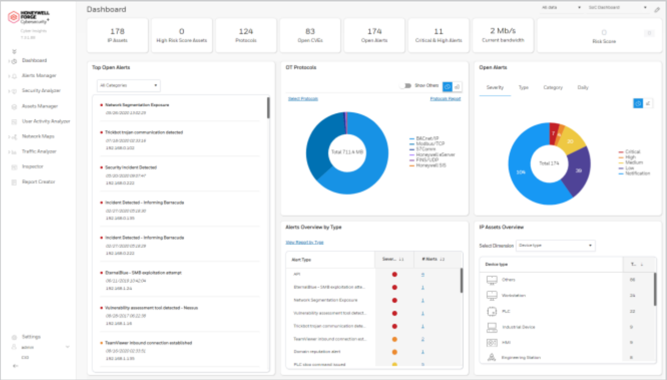
KNOW WHAT'S CONNECTED TO YOUR NETWORK

Knowing what assets are on the network is a fundamental starting point for any cybersecurity program. It is true that this can be done manually, but not as a practical method to discover newly added devices without a delay. Cyber Insights with its OT-specific network monitoring capabilities is designed to not only provide a comprehensive and accurate inventory of all the assets in the network when first run, but also to detect new additions to the network and to provide an alert for further investigation. If the newly added node was a malicious rogue node, being able to quickly address the intrusion can significantly help reduce the risk of negative impact on the process and safety of operations.

Another common challenge for industrial facilities is the ability to keep track of assets that are getting close to their end-of-life. Cyber Insights is designed to help with this task by showing the assets' current lifecycle status and end-of-life date based on vendor-provided information to better help the site plan their upgrades and migrations.

DETECT THREATS FASTER, MANAGE VULNERABILITIES BETTER

Information on lower-level assets such as controllers and PLCs can be hard to get in OT environment without disrupting the process. Cyber Insights is designed to use passive network monitoring or, if preferred, active polling using native protocols to collect details on these assets and compare against the known vulnerabilities in the National Vulnerability Database (NVD). To provide even more useful information to help prioritize remediation work orders, Cyber Insights allows the identified vulnerabilities to be further filtered to only show known exploited vulnerabilities (KEV). This feature together with the CVSS scoring from the NVD are designed to help the OT cybersecurity team to focus on addressing the weaknesses that need the most urgent attention and leave the lesser concerns to be dealt with later.



Cyber Insights is also designed to compare the data it collects against the MITRE ATT&CK for ICS framework. Seeing a site's current security data mapped against attack tactics and techniques observed in the real world can be useful when trying to decipher whether an individual event is just that, an isolated event - or part of a malicious chain of events in progress. When investigating an alert, Cyber Insights is capable of allowing a site's OT cybersecurity team to trace the alert to the user whose actions caused it to occur – and to see what else the user had been up to.

In addition and to help sites to better protect themselves against targeted cyber attacks, Honeywell threat researchers continuously investigate reported cyber threats and exploits against specific industries, locations and assets. This intelligence is fed into Cyber Insights, which can then provide curated information to the site's OT cybersecurity team on threats should be foremost in their mind.

ON PREMISE AND VENDOR-NEUTRAL SOLUTION

Cyber Insights is deployed on the control network to provide cybersecurity information even at sites with limited or no connectivity to the corporate network. Cyber Insights is certified for use on Honeywell's Experion® PKS control system for industrial automation. As well, the solution is designed to unobtrusively monitor network traffic to capture a wealth of information from Honeywell and non-Honeywell assets and transform it into valuable intelligence without the collected data having to leave the premises. As such, Cyber Insights is well suited for on-premises use at individual sites. For organizations that need the information from the individual sites to be shown in a single view, Honeywell Forge Cybersecurity+ | Cyber Watch can be added. This complementary solution is capable of providing an aggregated view from a central location, making it easier for a multi-site organization to have a comprehensive view into their cybersecurity posture.

PROTECT OPERATIONS IN AN EVER-CHANGING THREAT LANDSCAPE

As the cyber threat landscape expands with more specific attacks on OT, companies that can best identify threats and vulnerabilities earlier can reduce the likelihood of an unplanned shutdown or safety incident caused by a malicious actor. Knowing a site's current cybersecurity posture at all times is vital to reducing cyber risk. Cyber Insights is designed to be used in industrial environments to provide crucial information on a site's assets, vulnerabilities and threats to give the site's OT cybersecurity team the insights needed to better protect their operations. Cyber Insights is designed to be a readily accessible resource with up-to-date information for those who need to focus on improving a facility's overall cybersecurity posture.

FEATURES AND BENEFITS

DESIGNED TO PROVIDE THE FOLLOWING:

Better Asset Management: Designed to provide fully automated asset discovery and inventory for comprehensive visibility into a control network's OT and IoT devices, including their lifecycle status and end-of-life (EOL) information.

Comprehensive Visibility: Designed to deliver visibility into OT networks, communication patterns, and attack vectors at a single site.

Vendor Neutral: Vendor neutral on-premise solution, designed by OT cybersecurity professionals for OT environments.

Improved Risk Management: Designed to support better cybersecurity risk management and improved cyber hygiene with detailed security information and existing vulnerabilities based on the NVD.

DESIGNED TO PROVIDE THE FOLLOWING:

Near Real-time Detection of Threats and Anomalies: Designed to passively identify indicators of compromise (IOCs), providing early attack detection. It is also designed to monitor user activity inside a site's network, looking for and alerting on any signs of potential cybersecurity threats.

MITRE ATT&CK Framework: Designed to map security events to the MITRE ATT&CK for ICS framework for better analysis.

Tailored Threat Intelligence: Designed to provide curated threat intelligence on reported malicious activities and their relevancy to specific locations, industries and equipment.

DESIGNED TO PROVIDE THE FOLLOWING:

Deployment Flexibility: Ease of deployment, designed to integrate into a site's existing security architecture.

Experion Certified: Certified for use on Honeywell's Experion control system for industrial automation.

WHY HONEYWELL?

Honeywell has more than 100 years of experience in the industrial sector and more than 20 years of experience in industrial cybersecurity and thousands of projects delivered world-wide. We provide cybersecurity solutions that protect industrial assets' availability, safety and reliability worldwide. Honeywell's complete portfolio includes cybersecurity software, managed security services, industrial security consulting and integrated security solutions. We combine industry-leading cybersecurity experience with decades of process control knowledge to provide the premier industry solutions for an operational technology environment.

This document is a non-binding, confidential document that contains valuable proprietary and confidential information of Honeywell and must not be disclosed to any third party without our written agreement. It does not create any binding obligations on us to develop or sell any product, service or offering. Content provided herein cannot be altered or modified and must remain in the format as originally presented by Honeywell. Any descriptions of future product direction, intended updates, or new or improved features or functions are intended for informational purposes only and are not binding commitments on us and the sale, development, release or timing of any such products, updates, features or functions is at our sole discretion.

All pictures shown in this document are for illustration purposes only; the actual product may vary.

Honeywell® is a trademark of Honeywell International Inc. Other brand or product names are trademarks of their respective owners.

For More Information
To learn more about Honeywell OT
Cybersecurity, visit HoneywellForge.ai or
contact your Honeywell account manager.

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308

www.HoneywellForge.ai

October 2023

Honeywell