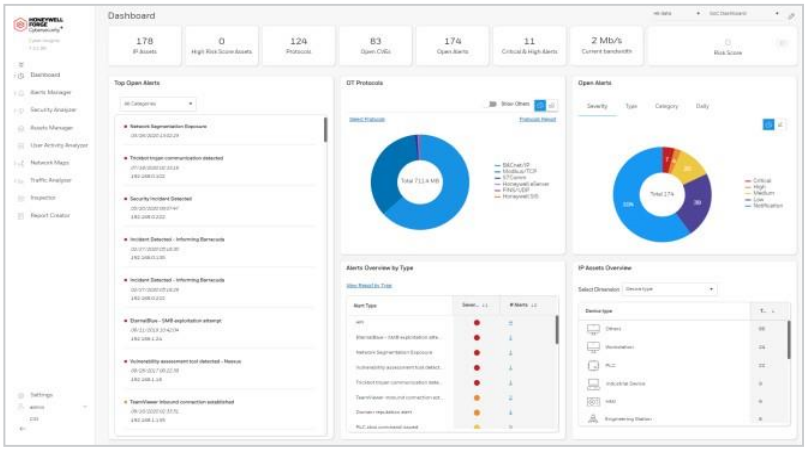
HONEYWELL CYBER INSIGHTS

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 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-premises and vendor-neutral solution is designed to provide customers with access to near 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 Cyber Insights is one of the most comprehensive cybersecurity solutions for OT and IoT networks. It is designed to discover and inventory all 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.

KNOW WHAT'S CONNECTED TO YOUR NETWORK

Knowing what assets are on the network is a fundamental starting point for any cybersecurity program. While this can be done manually, it is not a practical method for discovering newly added devices without delay. Cyber Insights, with its OT-specific network monitoring capabilities, is designed to not only provide a comprehensive and accurate inventory of all assets in the network when it is first run, but also to detect new additions to the network and provide alerts for further investigation. If the newly added node is 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 keeping track of assets nearing their end-of-life. Cyber Insights is designed to assist with this task by showing the assets' current lifecycle status and end-of-life date based on vendor-provided information, helping the site plan their upgrades and migrations more effectively.

DETECT THREATS FASTER, MANAGE VULNERABILITIES BETTER

Information on lower-level assets such as controllers and PLCs can be hard to obtain in an 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 them against the known vulnerabilities in the National Vulnerability Database (NVD). Cyber Insights includes the integration of Google Threat Intelligence (GTI) to enhance threat detection capabilities. Windows CVE data is also incorporated to expand and enrich the CVE database. To provide even more useful information for prioritizing remediation work orders, Cyber Insights allows the identified vulnerabilities to be further filtered to show only Known Exploited Vulnerabilities (KEV). This feature, together with the CVSS scoring from the NVD, is designed to help the OT cybersecurity team focus on addressing the weaknesses that need the most urgent attention, leaving lesser concerns to be dealt with later.

Revised: September 2025

HONEYWELL CYBER INSIGHTS

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 for determining whether an individual event is isolated or part of a malicious chain of events in progress. When investigating an alert, Cyber Insights enables a site's OT cybersecurity team to trace the alert to the user whose actions caused it and obtain more detailed user activity.

Additionally, to help individual sites 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 then provides curated information to the site's OT cybersecurity team on threats that should be foremost in their minds.

ON-PREMISES AND VENDOR-NEUTRAL SOLUTION

Cyber Insights is designed to be 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. Additionally, the solution is designed to unobtrusively monitor network traffic to capture a wealth of information from Honeywell and non-Honeywell assets, transforming it into valuable intelligence without the collected data having to leave the premises. Cyber Insights is well-suited for on-premises use at individual sites. For organizations that need information from multiple sites to be shown in a single view, Honeywell Cyber Watch can be added. This complementary solution is designed to provide an aggregated view from a central location, making it easier for a multi-site organization to comprehensively view its 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 is vital to reducing cyber risk. Cyber Insights is designed for use in industrial environments to provide crucial information on a site's assets, vulnerabilities, and threats. It can also assist the site's OT cybersecurity team by providing the insights needed to help protect their operations. Cyber Insights is designed to be a readily accessible resource with current information for those needing to improve a facility's overall cybersecurity posture.

Revised: September 2025

HONEYWELL CYBER INSIGHTS

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 provide visibility into OT networks, communication patterns, and attack vectors at a single site.

Vendor-Agnostic: Vendor-neutral, on-premises 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: This system passively identifies indicators of compromise (IOCs) for early attack detection. It monitors user activity within a network, alerting on potential cybersecurity threats. Additionally, it actively polls Windows machines to check for installed or missing security patches, providing a comprehensive threat overview.

MITRE ATT&CK Framework Integration: Security events are mapped to the MITRE ATT&CK for ICS framework, enhancing analysis capabilities.

Tailored Threat Intelligence: The system delivers curated threat intelligence on reported malicious activities, relevant to specific locations, industries, and equipment. It can enrich threat data using Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Intelligence Information (TAXII) servers.

DESIGNED TO PROVIDE THE FOLLOWING:

Deployment Flexibility: Designed for easy integration into a site's existing security architecture.

Experion Certified: Compatible with Honeywell's Experion control system for industrial automation.

Enhanced Security: Supports Single Sign-On (SSO) authentication with providers such as Google, Azure Auth, and Auth2.

Seamless Integration: Integrates smoothly with the ServiceNow Configuration Management Database (CMDB).

Revised: September 2025