HONEYWELL FORGE
Cybersecurity+
Cyber Insights

SERVICE 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. To help address this, Honeywell's OT cybersecurity team designed a software-enabled solution, Honeywell Forge Cybersecurity+ | Cyber Insights, specifically for industrial process control environments. With actionable and targeted OT cybersecurity insights, this on-premise and vendor-neutral solution provides customers with access to real-time and historical data on vulnerabilities, compliance and threats to help them reduce cyber risks and manage compliance.

Get Better Visibility to OT Cybersecurity Posture – All in One Tool

In recent years, industrial companies have been under increased pressure to better protect their operations from cyber attacks. While general awareness of OT cybersecurity is increasing, many companies still struggle to find the right people and tools. Often, the standard tools that IT professionals use in enterprise environments are less helpful – and in some cases even be dangerous – in industrial environments. However, with the right tools and support, cybersecurity leads and process control network (PCN) specialists can access the information they need to help reduce the risk of a cyber incident at their facilities.

Developed by Honeywell's experienced OT cybersecurity professionals, Cyber Insights is an on-premise solution that helps industrial organizations gain much-needed visibility into their OT cybersecurity posture. It is designed to provide access to near real-time and historical data on vulnerabilities, compliance and threats related to both Honeywell and non-Honeywell assets – all in one tool.

The Cyber Insights solution is pre-configured by Honeywell to allow for rapid on-site installation and setup by Honeywell OT cybersecurity engineers, so on-site staff can quickly leverage the valuable, curated information to improve a site's cybersecurity posture. Once deployed, Honeywell OT cybersecurity engineers support site personnel and provide maintenance to help with continued, long-term benefits.

On Premise and Vendor-Neutral Solution

Cyber Insights is deployed on the PCN to provide cybersecurity information even at sites with limited or no connectivity to the corporate network. Pre-defined data is collected from Honeywell and non-Honeywell assets and transformed by Cyber Insights into valuable intelligence without the collected data having to leave the premises. If desired, organizations with a secure connection for content transfer can forward the raw or normalized log data to an off-site security operations center (SOC) or to a managed security services provider such as Honeywell.

To help a customer obtain the most comprehensive and accurate information possible without disrupting process operations, Cyber Insights uses lightweight clients on systems in the PCN to collect the necessary data. The clients are designed to collect the majority of the data in real-time after carefully checking the existing load on the system. The data, along with all other collected logs, is sent to the Cyber Insights server for analysis, further reducing the demands on the PCN.

Hunting Threats, Managing Vulnerabilities

Cyber Insights can help OT cybersecurity professionals “cut through the noise” by presenting only relevant cybersecurity information instead of low-value data. The solution collects data on security events, vulnerabilities, threats and compliance, using rules designed to bring focus on the information based on its criticality. In addition, Cyber Insights maintains a detailed inventory of monitored assets.

The comprehensive data collected from servers and workstations is compared with the vulnerabilities documented in the National Vulnerability Database (NVD). The known vulnerabilities found at the site and information about the impacted assets can be easily viewed in Cyber Insights, with the goal of helping the customer prioritize their risk mitigation actions.

Cyber Insights uses file integrity monitoring (FIM) to help customers identify indicators of compromise, by looking for changes in file permissions, content, attributes and ownership. Newly added or changed files are then checked for malicious content by Honeywell’s Global Analysis, Research and Defense (GARD) Threat Intelligence, a proprietary threat detection system designed for OT environments.

Cyber Insights helps customers match collected security events with the MITRE ATT&CK framework. The ability to map current site data with attack tactics and techniques observed in the real world helps customers identify otherwise isolated alerts as part of a potentially malicious cyber attack. Additional investigation by customers is accelerated by OT-specific threat-hunting rules created by cybersecurity professionals at Honeywell's OT Cybersecurity Centers of Excellence and Innovation.

Cyber Insights can integrate with many other security solutions already deployed at the customer’s site. Although a comprehensive OT cybersecurity solution on its own, Cyber Insights is designed to bring in data from tools such as Honeywell’s Cyber App Control, Honeywell’s Secure Media Exchange (SMX), various antivirus solutions and other OT monitoring solutions. This provides a customer with insights into the information collected by other Honeywell and third-party cybersecurity tools. Because Cyber Insights can collect, consolidate and visualize security-related data from multiple sources, both Honeywell and non-Honeywell, it can be a critical resource for OT cybersecurity leads who must have easy access to important cybersecurity information to conduct investigations.

Support for Compliance and Investigations

Organizations that must comply with either internal policies or external standards often struggle to obtain up-to-date data needed to show compliance. Cyber Insights is designed to help customers ensure that their industrial sites comply with standards such as IEC 62443 by providing programmatic access to audit logs, as well as frameworks such as NIST 800-53 that require automated tools to support near real-time event analysis. Because Cyber Insights can preserve and maintain historical data, it should be considered an essential tool for forensic investigations and compliance purposes.

Cyber Insights is also designed to monitor assets against user-defined local policies, the industry-recognized CIS benchmarks, and NIST 800-53 requirements. Having this information available in a single tool is efficient and a time-saver for cybersecurity professionals who work to stay in compliance with their site expectations and to more easily share information requested by auditors.

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 will reduce the likelihood of an operational shutdown and gain a competitive advantage. Knowing the cybersecurity posture of an industrial facility at any given time is vital to reducing cyber risk. Cyber Insights can help by providing up-to-date information, readily accessible by the people who depend on it.

Cyber Insights is designed for industrial environments to provide valuable information on vulnerabilities, threats and compliance, along with in-depth investigative capabilities, to give customers the insights needed to better protect their operations. With ongoing support and maintenance from Honeywell, on-site personnel can focus on improving the facility's overall cybersecurity posture.

- Designed to provide current and historical data on vulnerabilities, threats and compliance
- Purpose-built for OT environments
- Pre-configured for faster on-site deployment
- Supports compliance with industry standards, frameworks and best practices such as IEC 62443, NIST 800-53 and CIS Benchmarks

- Supports cyber threat hunting through file integrity monitoring, file-based threat detection, mapping MITRE ATT&CK framework and OT-specific threat hunting rules
- Customizable to address site-specific needs
- Capable of integrating with many existing security solutions already used on-site

- Helps reduce OT cybersecurity risks by enabling faster response to threats and in-depth investigations by a customer
- Supported and maintained by Honeywell’s OT cybersecurity team
- On-premise solution for reduced risk

Why Honeywell?

Honeywell has more than 100 years of experience in the industrial sector and more than 20 years of experience in industrial cybersecurity. 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.

For More Information

To learn more about how Honeywell's OT cybersecurity solutions can help you, visit www.BeCyberSecure.com or contact your Honeywell account manager.

Honeywell Connected Enterprise

715 Peachtree Street NE
Atlanta, Georgia 30308

www.honeywellforge.ai

May 2023