Honeywell
THE POWER OF CONNECTED | Industrial Cyber Security

CyberVantage Assessments for Industrial Control System Resilience

Service Note

Expert technical reviews of your process control network and related systems can help safely expand your operations, increase cyber security resilience, and standardize industrial cyber security best practices to drive optimal efficiencies and teamwork.

Operational networks need to flex and expand to support your business, but only in a safe and responsible manner. To determine priorities, allocate technology budgets effectively, and introduce standards safely across the process control network, you need to understand the current state of cyber security and the detailed steps required to reach your desired destination.

Honeywell assessments support the range of business needs of today's industrial operations:

Network Growth – Assessments to inform how and where to safely adapt ICS systems or perform upgrades as you merge or change plant facilities; implement competitive innovation strategies such as OneWireless or mobile worker programs; increase network scale to deliver to new territories; or implement new controls and automation technologies that may inadvertently affect your legacy infrastructure.

FEATURES & BENEFITS

FEATURES

- A variety of assessment types to meet your needs
- Deep technical expertise in both operations and industrial cyber security
- Experience from 6000+ PCN engagements
- Safe-on-site personnel
- Global assessment capabilities
- Peer benchmarking
- Independent opinions
- Actionable technical steps and business summary deliverables, to support different stakeholders
- Ability to perform remediation work, to rapidly follow up assessments with implementation progress
- Future design work options

BENEFITS

- Proactively remediate major industrial cyber security issues
- Gauge or document compliance independently
- Prioritize security work for your team or for trusted providers
- Educate business leaders on the latest best practices specific to your PCN
- Influence decision-makers with objective industrial security recommendations
- Operationalize secure digital transformation or plant modernization plans
- Validate risk levels with peers or other departments
- Standardize security across multiple plants
- Verify other assessments
- Identify issues including
  - Unauthorized users
  - Unaddressed software vulnerabilities
  - End of service equipment
  - Outdated encryption methods
  - Non-compliant remote access connections
  - Lack of proper cabling

Risk Reduction – Cyber security threats are a board and C-suite level priority, and assessments help you get ahead of security directives. Thorough, expert reviews can help identify security concerns; improve compliance; adapt to changing threat levels; increase behavioral learning to better detect and respond to threats; and implement data baselining to monitor security progress over time.

Collaboration – Agility in a world of sophisticated cyber threats is essential for safe operations. When teams have access to key information, defined and automated processes, and a framework for security, they are better able to work together to limit attack damage and protect production. Assessments can be used to drive realistic OT/IT convergence; inform policies that fit your company culture; prioritize security work across teams; and document best practices that support a consistent corporate standard.

Assessments for Every Need

Honeywell provides several types of specialized technical assessments to support your desired business outcomes. Meeting with a CyberVantage consultant can help identify which specific package of services is best suited to reach your goals.

Industrial Network Assessments

Network assessments not only provide visibility into your current process control network infrastructure, but also deliver the foundational knowledge for developing your five-year network management plan. Before you embark on network upgrades, accept new design recommendations from outside your team, or try to implement any new equipment within your operational environment (including Experion on FTE), use a Network Assessment to understand status, and benefit from recommendations by Honeywell's highly experienced assessors. If you already have ad hoc assessments performed by other organizations, Honeywell Network Assessments can be used to validate findings or offer alternative perspectives.

Network Assessments include a safe, comprehensive review of your ICS Ethernet network communications infrastructure, from Level 5 and down, and can include Level 3.5 Demilitarized Zone (DMZ) network and firewall devices. Experts in operational environments review your installed infrastructure and the network devices in your present configuration. Our boots on the ground also visually inspect environmental conditions at your site to identify issues such as lack of enclosures or poorly situated HVAC systems.

Network Assessment deliverables include a Logical Diagram of your existing ICS infrastructure (typically in Visio format), showing current ICS connectivity and depicting switches, routers, and firewalls. The Network Assessment Report documents observations, best practices, and site-specific recommendations in an actionable format, useful to share with your stakeholders to drive the changes you need. These reports articulate executive level summaries to help leadership understand how your network compares to others that Honeywell has assessed (anonymously), overall network condition, and key priorities for action. Reports also include detailed information for your technical team, describing the nature of issues uncovered, why they are important to address, and any equipment or bill of materials that can be procured to address these issues – all specific to your environment. Unique to Honeywell, Network Assessment Reports can also specify how to optimally upgrade to Experion on FTE in the future, including FTE community assessment, ICS connectivity represented as Honeywell Levels, and detailed Honeywell materials lists.

Network Assessments deliver the high-value control network status milestone you need to translate your network improvement ideas into actionable, safe next steps.

The deliverables can also serve as an objective, third party perspective, helping you influence key decision makers and attain the investments required to run a high-performance operation.

The CyberVantage Security Consulting Services provide capabilities to enable safer connected plants, digital transformation, and Industrial Internet of Things (IIoT) efforts. Delivered by consultants with expertise in both operational technology (OT) and industrial cyber security, the services help organizations reduce the risk and possible impact of incidents by helping them improve industrial cyber security maturity levels.

Industrial Cyber Security Assessment

When it's time to understand your control system vulnerabilities and potential weak spots, an Industrial Cyber Security Assessment from Honeywell can provide the expert information you need.

The Industrial Cyber Security Assessment includes a holistic technical review of the industrial control system infrastructure at a particular point in time. The focus is on analyzing common cyber security processes, procedures and safeguards used to protect your ICS from internal and external threats. Select experts from Honeywell's 200+ industrial cyber security team assess your ICS security from Level 5 and down, from the process control network, through to the Level 3.5 - Demilitarized Zone (DMZ), including network and firewall performance.

Unlike IT or point product vendor assessments, Honeywell Industrial Cyber Security Assessments consider people, process and technology issues that can impact your ICS cyber security posture. This includes a physical site review to uncover issues such as control room doors left unlocked, passwords in the line of sight, and other security compliance violations. With deep expertise across IEC 62443 compliance requirements and other industry-specific regulations such as NERC-CIP, as well as invaluable experience in control system networks, Honeywell assesses your ICS environment, documenting observations and recommendations to reduce cyber security risks.

Bearing holistic industrial cyber security needs in mind, our experts also review network equipment from third parties such as switches, routers, and firewalls; review infrastructure configurations; and check installation processes. With ample experience performing these specialized assessments, Honeywell consultants can adeptly identify design gaps, technology gaps, and any deficiencies in cyber security implementation.

All the vulnerabilities, severity levels, and remediation details are included in an Industrial Cyber Security Assessment Report, an important deliverable to help you align stakeholders and interdependent groups affecting your company's cyber security readiness.

Operations engineers also use the report to discover and remediate work prior to corporate audits, or to influence corporate security policies that can impact their PCN. The report specifies best practices and site-specific recommendations to help mitigate and prioritize any identified threats or vulnerabilities, and notes how and where steps can serve as a foundation for ensuring a best practices architecture.

For threats and vulnerabilities identified, the report helps educate why these are issues, and their potential impact on your operations. Implementation personnel can leverage report details to perform important remediation work. Honeywell's Industrial Cyber Security team is also available to rapidly act on report findings to mitigate your risks.

Industrial Threat Risk Assessment

Compared to an Industrial Cyber Security Assessment, the Industrial Threat Risk Assessment goes even deeper into risk to help those organizations seeking advanced levels of cyber security preparedness. It delivers risk information that serves as the basis for security operations, indicating what security efforts are justifiable, and which are worth prioritizing, based on risk.

The Industrial Threat Risk Assessment delivers a detailed security evaluation of your industrial control system's ability to withstand targeted attacks from skilled, motivated and well-sourced attackers, such as nation-states, terrorist groups, hacktivists, and insiders. It identifies the most critical risk scenarios, and uses these attack sequences as basis for further analysis. The Industrial Threat Risk Assessment takes into consideration SL2 plus level 1 csHAZOP.

Organizations interested in advanced cyber security maturity levels, such as critical infrastructure providers and national service providers, use Industrial Threat Risk Assessments as an essential part of their organizational rigor, and as a precursor to further detailed security testing, such as penetration testing or validation testing (White Box Tandem test validating the security controls in place). Those with a defined risk matrix and a GRC team are especially able to leverage Industrial Threat Risk Assessment findings for granular security decision making.

Operations teams use Industrial Threat Risk Assessment findings as the basis for developing their security management frameworks and related processes.

This can include determining what, if any, technologies can reduce risk, and how people and process can be adapted for additional improvements.

Since risk is relative to your company's risk appetite and tolerance, risk scenarios are extremely useful for understanding what potential actions will or will not lower risk across your specific technical environment. The Industrial Threat Risk Assessment also analyzes any controls that have been implemented to reduce risk, checking their protection capabilities, as well as their detection and response capabilities. By using measured performance information based on your unique network and system configurations, our reports provide risk indicators that usefully guide your security management efforts.

In a detailed report and related deliverables, the Industrial Threat Risk Assessment provides:

- Key risk indicators and an associated score
- Key mitigations
- A vulnerability assessment
- Threat / risk scenarios
- Threat likelihood
- Attack sequence diagrams and consequence scores
- A resilience score
- A risk register
- KRI / KPI scores
- Mitigation planning
- Mitigation
- A compliance overview
- Compliance with IEC 62443
- Compliance with any other specified reference.

Audits

Audits can objectively verify compliance or non-compliance based on a specific set of requirements. Honeywell's industrial cyber security team regularly performs audits of third party implementations, Honeywell's own security technologies, broad process control networks, and targeted processes or technologies.

Audits vary across Honeywell depending on the specific regulatory checklist the customer uses, which can be regional focused. In North America, for example, NERC-CIP audits may be requested in the Power industry. Internal or custom checklists specific to an organization care also often used, with audits ensuring policies are properly enforced. In Europe, audits are most often performed against regulatory standards frameworks.

Based on objectives you hope to achieve with your audit, Honeywell can propose an audit service engagement that provides the key technical skills and objective verifications you need.

Cyber Security Profiling

In select situations, Cyber Security Profiling can be used for a rapid, lightweight glimpse into your security profile. In short turnaround cases, or in merger and acquisition situations where diligence deadlines are tight, Cyber Security Profiling can provide basic information and an expert opinion. In most cases, customers complete a detailed cyber security maturity level questionnaire. This data, and in some cases, any existing policies or documentation, is reviewed by a Honeywell industrial cyber security consultant for overall remarks and feedback. If your objective is to reduce risk to operations and improve resilience, however, Assessments (as described in prior pages) are a better choice.

Industrial Wireless Network Services

Honeywell is one of the few providers able to provide both wired and wireless network expertise, in context of industrial cyber security. Our wireless assessments focus on existing networks, checking for a range of security issues:

- Pinholes - unauthorized, employee-initiated wireless access points in the plant
- Unmanaged Plant Wi-Fi, accessible beyond the plant walls or user base
- Externals trying to associate with plant Wi-Fi
- Weak wireless performance areas (dead spots)
- Outdated equipment.

Honeywell is the leading provider of cyber security solutions that protect industrial assets, operations and people from digital-age threats. With more than 15 years of cyber security expertise and more than 50 years of industrial domain expertise, Honeywell combines proven cyber security technology and industrial know-how to maximize productivity, reliability and safety.

If your organization has legacy Honeywell wireless equipment, it is also important to replace it with far more powerful and popular OneWireless technologies.

While our assessments support existing infrastructure needs, our wireless surveys assist in planning and designing new wireless networks. As exciting opportunities for wifi-enabled instrumentation and mobile workers continue to emerge, Honeywell surveys can identify optimal approaches to building your new wireless network.

Managing Large-Scale Cyber Security Needs

Our industrial cyber security experts regularly support large customer's global deployments and major projects across multi-national organizations. We partner with thousands of groups across Honeywell to expand and integrate our services into broader solution design, assessment, implementation, and ongoing process control network improvement needs. Depending on your project objectives and requirements, our teams can deliver a wide range of services that support safe connected plants. To learn more, talk with your Honeywell representative, or visit becybersecure.com.

Where Innovation Meets Implementation to Drive Industrial Cyber Security Excellence

Honeywell CyberVantage Security Consulting Services provide 30+ specialized industrial cyber security offerings and custom consulting to help process control industries safely operate and connect. Honeywell CyberVantage consultants are versed in both industrial operations and cyber security to help companies best assess their risks, design robust architectures, protect networks and endpoints, and improve situational awareness and incident response. Consultants can help customers leverage any of nine Honeywell Centers of Excellence to safely simulate, validate and accelerate their cross-vendor industrial cyber security solutions in state-of-the-art facilities staffed by experts.

For More Information

Learn more about how Honeywell's Cyber Services can improve your enterprise security, visit becybersecure.com or contact your Honeywell Account Manager.

Honeywell Process Solutions

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Skimped Hill Lane Bracknell,
Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road, Zhangjiang Hi-Tech Industrial Park, Pudong New Area,
Shanghai 201203

www.honeywellprocess.com

SV-18-03-ENG
October 2018

Honeywell