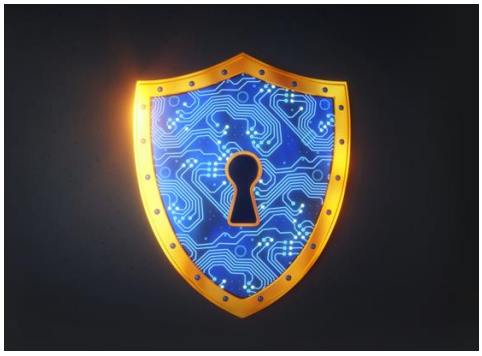
Honeywell
THE POWER OF CONNECTED | Industrial Cyber Security

# CyberVantage Penetration Testing for ICS Defenses

Service Note

**Actively engage your industrial control system (ICS) environment's defenses from a hacker's perspective. Uncover risks, validate security postures, and safely exploit weaknesses before malicious outsiders get the chance.**

CyberVantage Penetration Testing actively exploits your industrial control system environment to reveal potential security concerns and weaknesses. Using offensive tactics, techniques, and tools, Honeywell industrial cyber security experts act as "white hat" hackers, safely testing your network within the parameters you define. A detailed report delivers valuable recommendations for mitigating risks and vulnerabilities that may go unnoticed without active testing.



Whether targeted against a single application, a network or entire facility, penetration testing enables businesses to see what an attack would look like:

- Identifying gaps in security technology coverage
- Revealing vulnerabilities that cannot be detected by automated tools, such as insecure password storage or weak in-memory malware detection
- Testing an organization's detection and responses to see if defenders can detect and prevent an attack in progress
- Providing validation, justification, and business cases for investment in OT security.

## FEATURES & BENEFITS

FEATURES

- Experienced "white hat" hacker penetration testing
- Industrial control system expertise to test the ICS security posture
- Deep technical expertise in both operations and industrial cyber security for rigorous testing
- Highly trained personnel, safe-on-site and accustomed to sensitive operational networks
- Technical and non-technical vulnerability testing
- Independent, custom remediation recommendations based on penetration testing findings
- Documented, actionable technical steps for risk reduction
- Customizable methodologies for safeguarding tests, including white box, black box, and gray box options

BENEFITS

- Improved defenses: identifies gaps in security technology coverage
- New defense insights: reveals vulnerabilities that cannot be detected by automated tools
- Objective information: third party expert findings and recommendations
- Business case simplification: provides validation and evidence to support security investments
- Proactive risk reduction: reveals vulnerabilities from a hacker's perspective before outsiders do
- Increased knowledge: internal technical teams learn from approach and findings
- Simplified security prioritization: identifies key remediation steps to fix major industrial cyber security issues

Providing detailed evidence of whether and how security can be breached, penetration tests can be defined to the customer's exact requirements, including external, perimeter, perimeter security and process penetration testing. All test reports are designed to help those responsible for implementing security at the site understand what Honeywell experts did, how they did it, and how the site could prevent others from doing the same. Penetration testing looks for how to threaten the organization, at highest consequence, by exploiting vulnerabilities. Weaknesses might include technical and non-technical pathways, such as software vulnerabilities that have never been patched, or phishing emails that easily bypass existing defenses.

**Testing for a Reason**

Successful penetration testing begins with a clear understanding of the goal(s) to achieve, then scoping related rules of engagement. Goals may include the need to provide a risk ranking to the organization, based on an entire plant network or select applications, or perhaps a select plant physical location. Others may be insight into technical and non-technical vulnerabilities and misconfigurations, reporting back, for example, on context for how observed vulnerabilities might be exploited to cause the greatest damage.

Goals also typically include gaining a specific set of remediation steps to resolve weaknesses. For organizations seeking to validate security posture, goals may focus on emulating threats, and performing an entire "dress rehearsal" covering protective, detective, and corrective actions.

**The Right Experts for Safe Testing**

Uptime and safety of the industrial control system always remains the first priority. Honeywell penetration testers are well trained and experienced at performing within production environments, and are deeply knowledgeable about operations and industrial cyber security technicalities.

Safeguards to prioritize the availability of the ICS are an important aspect of the exercise, and can include Black, Grey, or White Box configurations, escorted digital access, and table top or paper exercises.

**Expert ICS Exploitation Walkthroughs**

Based on successful past engagements, Honeywell penetration testers can help define and recommend approaches. Walkthroughs of ICS exploitation provide rich insights and feedback to inform future security actions. Honeywell Penetration Testing commonly performs walkthroughs for various exploitation types:

- Perimeter Credential Re-Use, in which a user attempts to find and obtain credentials, then use the same credentials for accessing the business LAN and demilitarized zone (DMZ) layers of the network. Understanding system credential loss and misuse helps improve policies, such as requiring different credentials for each security zone. Perimeter walkthroughs also help uncover any sensitive ICS Information that may have been inadvertently leaked to the business network. Malicious actors often use easier-to-access business networks to perform information gathering in advance of sophisticated, targeted attacks. Data from this type of testing provides business case evidence to support improved security measures, such as multi-factor authentication.

- Common Local Administrator Password – Acting as a hacker who has obtained the common local administrator password enables us to test what lateral movement could occur within the DMZ, to identify potential consequences. This viewpoint assists in selecting and implementing remediation to either prevent or slow down attacker actions. Any new networks can be assessed to identify usernames, groups or services – any information that hackers might further exploit. By understanding the real-life likelihood of passwords falling into malicious hands, companies can better defend such key information through techniques such as password hashing and limiting use of hash

*Uptime and safety of the industrial control system always remains the first priority. Honeywell penetration testers are well trained and experienced at performing within production environments*

pass-through features. Better detection methods can also be instituted to act on noise generated by hackers, as learned through the penetration testing.

- Domain Trust Extension – Access to ICS assets can be tested by exploiting the organization's domain trust configuration. This enables hackers to completely bypass important security functions at the DMZ layer. Penetration testing also exploits beneficial security technology features for malicious advantage, such as testing anti-virus file transfer mechanisms and automated updates. Lateral movement is also attempted. These active engagements across your environment can improve design and implementation of network segments. Use it to improve easily exploitable defenses and shore up issues such as service account credentials and insecure file transfer systems.

**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-18-04-ENG
October 2018


Honeywell