Honeywell | OT Cybersecurity

OT PENETRATION TESTING

SERVICE NOTE

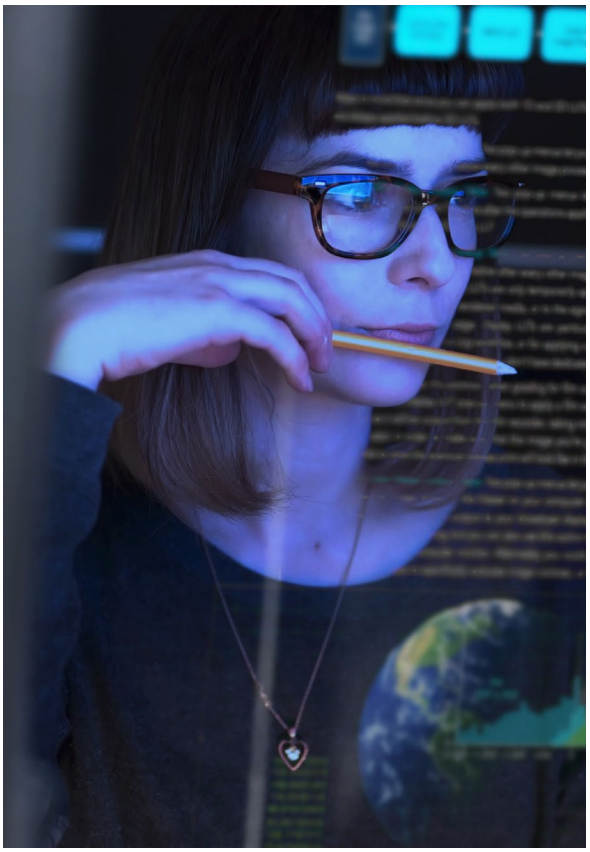
> Actively engage your industrial control system environment's defenses by experiencing a real-life simulation of a cyber attack. Uncover risks, validate security postures, and exploit weaknesses before malicious outsiders get the chance.

Honeywell's operational technology (OT) penetration testing is designed to actively exploit your industrial control system (ICS) environment to reveal potential security concerns and weaknesses. Using offensive tactics, techniques and tools, Honeywell's industrial cybersecurity team acts as white hat hackers, testing your defenses within the parameters you define with your operations' safety as a top priority. 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 organizations to see what a real-life attack could look like. Using the MITRE ATT&CK framework and NIST Guide SP800-115, Honeywell's penetration testing identifies gaps in security technology coverage, reveals vulnerabilities that cannot be detected by automated tools, and tests the organization's detection and response capabilities for preventing an in-progress attack.

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 security and process penetration testing. All test reports are designed to help those responsible for implementing security at the site understand what Honeywell penetration testers did, how they did it, and how the site could prevent others from doing the same.

Honeywell's penetration testing is designed to identify various ways an organization could be threatened with the highest consequences by malicious actors exploiting existing weaknesses. 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.



Honeywell's OT penetration testing helps industrial companies in reducing cybersecurity risks by finding vulnerabilities from a hacker's perspective before outsiders do. In addition, uptime and safety of the industrial control system always remain the testers' first priority.

Testing for a Reason

Successful penetration testing begins with a clear understanding of the goals to achieve, and 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. Another goal may be insights 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 their security posture, goals may focus on emulating threats, and performing an entire “dress rehearsal” covering protective, detective and corrective actions.

Safety First, Always

Uptime and safety of the ICS always remain the first priority for Honeywell engineers, and that is why Honeywell’s penetration testers are well trained and experienced in working within production environments. Honeywell’s penetration testing can include black, grey or white box configurations, escorted digital access, and tabletop or paper exercises, all with safeguards designed to prioritize the availability of the ICS.

ICS Exploitation Walkthroughs

When done by experienced OT penetration testers, ICS exploitation walkthroughs can provide rich insights and valuable recommendations for future cybersecurity improvements. Honeywell’s penetration testing commonly includes walkthroughs for various exploitation types, such as perimeter credential re-use, common local administrator password, and domain trust extension.

With the perimeter credential re-use technique, for example, the penetration tester attempts to obtain credentials and use these for accessing the business local area network (LAN) and demilitarized zone (DMZ) layers. 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 gather key information to build out their sophisticated, targeted attacks. Data from this type of testing provides business case evidence to support improved security measures, such as multi-factor authentication.

Immediate and Longer-Term Benefits

While Honeywell’s penetration testers use their advanced skills, tools and techniques to break through the site’s defenses, some customer security teams use this opportunity to test their own capabilities to detect active threats. This helps the security team to improve, for example, by making modifications to their existing SIEM, and to be better prepared for a real attack.

The penetration testers also report on how well your existing malware protection tools caught the intentionally deployed payloads. Some of the findings can be addressed relatively quickly, such as allowing an application control software to block unknown files, as opposed to only monitoring their presence.

The final report, which is reviewed with you, documents the weaknesses identified in the security posture during the engagement and recommendations on how to address these. The recommended improvements by Honeywell are mapped to the NIST framework and include information about their criticality, complexity and estimated cost to help you prioritize your next steps.

Hiding Is Not an Option

Malicious actors have increased their attack efforts against industrial companies, with the goal of causing disruption or physical damage. Skillfully conducted industrial penetration testing helps you discover security weaknesses in a real-life scenario and identify the highest priority remediations needed to reduce your risk of a targeted attack. It is better you know your gaps before the unethical hackers do.

FEATURES AND BENEFITS

- Performed by highly trained ethical hackers, accustomed to sensitive OT networks and experienced in industrial on-site safety
- Provides insight to organization’s detection and response capabilities for preventing an in-progress attack

- Helps with proactive risk reduction by finding vulnerabilities from a hacker’s perspective before outsiders do
- Provides objective, custom recommendations based on findings

- Simplifies security prioritization by identifying key remediations for fixing major industrial cybersecurity issues
- Helps the organization’s security operations team to enhance the detection and monitoring capabilities

About Honeywell Security Consulting Services

Honeywell Security Consulting Services provide over 30 specialized industrial cybersecurity offerings and custom consulting to help process control industries safely operate and connect. Honeywell consultants are versed in both industrial operations and cybersecurity to help companies best assess their risks, design robust architectures, better protect networks and endpoints, and improve situational awareness and incident response. Customers can leverage Honeywell Centers of Excellence to safely simulate, validate and accelerate their cross-vendor industrial cybersecurity solutions in state-of-the-art facilities staffed by highly-skilled professionals.

Why Honeywell?

Honeywell has more than 100 years of industrial experience and over 20 years of industrial cybersecurity domain expertise. We are the leading provider of cybersecurity solutions, protecting the availability, safety and reliability of industrial facilities worldwide. Honeywell's complete portfolio includes cybersecurity software, managed security services, industrial security consulting, and integrated security solutions. We combine industry-leading expertise in cybersecurity and decades of experience in process control, for the best solutions in an operational technology environment.

For More Information

To learn more about Honeywell's Cybersecurity Consulting Services, visit www.becybersecure.com or contact your Honeywell Account Manager.

Honeywell Connected Enterprise

715 Peachtree Street NE
Atlanta, Georgia 30308

www.honeywellforge.ai

SV-18-05-ENG
May 2022

Honeywell