LEVERAGING MANAGED SECURITY SERVICES TO HELP PROTECT CRITICAL OT ASSETS

Honeywell

MANAGED SECURITY SERVICES

Honeywell Managed Security Services are designed to provide rapid threat detection at a lower cost, providing an effective strategy to drive value in improving security for an industrial operation and its critical OT assets.

Remote access, work from home, increased online meetings, a shortage of security talent, digitalization and the pressure to reduce risk are all compelling reasons for industrial operators and asset owners to seek assistance in protecting their enterprises. Recognizing the complexity of this task, industrial organizations continue to boost connectivity to enable digital transformation, remote operations and support. While advantageous, this connectivity also makes them more vulnerable to a cyber-attack, with threat actors exploiting vulnerabilities such as the software supply chain or profitable ransomware campaigns. That's why asset owners are increasingly turning to a managed security services model for their security needs. This approach is designed to allow them to use their in-house resources to focus on core revenue-generating production, while a managed security services provider delivers services designed to continuously monitor and provide security for the network utilizing best practices informed by proficient professionals from across the globe.

CYBERSECURITY SERVICES MODEL

Not all companies have the resources to hire in-house cybersecurity specialists. Honeywell Managed Security Services addresses this by having our experienced professionals handle increasingly sophisticated security threats, reducing and sometimes removing the need for asset owners to build their own domain, firewall or SIEM teams.

A key goal of a managed security services program is finding and helping to remediate anomalous cyber behavior before an actual incident occurs through early threat detection. Asset owners need 24/7 OT cybersecurity know-how and rapid response to current and emerging cyber threats, continuously monitoring, identifying potential threats early and analyzing signs of compromise in an OT environment before significant damage can occur. The security as a service model manages and monitors identified logs, devices, networks and assets, all from a security operations center (SOC). It is also designed to help organizations proactively identify and help mitigate cyber threats and attacks in the very early stages.

The need for experienced cybersecurity support is underscored by the ISC2 - Cybersecurity Workforce Study, 2023[1]. This report found that 67% of organizations face a shortage of cybersecurity staff, and a staggering 92% have skills gaps. This widespread lack of resources coincides with a challenging threat landscape: 75% of cybersecurity professionals find the current environment the most difficult in the past five years, and only 52% are confident in their organization's ability to respond to cyber incidents.

In general, many companies have no real means for ongoing preventative security operations, which could head off an incident before it happens.

CASE IN POINT

One global oil and gas provider recognized their need for ongoing cyber protection. They struggled to find qualified staff and lacked the budget and skills to manage cyber threats proactively and effectively. Additionally, they had limited visibility into their ICS assets. Sophisticated attacks were growing in prevalence, making continuous threat detection for their OT assets paramount, but they didn't have the time or budget to build their own security program. They needed more protected remote access, content and data transfer, patch and antivirus management, threat detection, 24x7 monitoring, threat alerts and reporting, incident investigation, log collection and analysis and remote monitoring support.

Honeywell Managed Security Services are designed to provide these capabilities to improve the company's ability to protect its control systems, meet compliance requirements and strengthen connections for smooth operations.

Organizations are increasingly sensing that attacks are on the horizon without having proper personnel in place. This drives many to retain a provider that employs 24x7 monitoring by professionals skilled in detecting anomalous behavior. A managed security provider may also deliver cost advantages and economies of scale.

CYBERSECURITY WORKFORCE GAP

Even if an asset owner wishes to start its own security department, the global cybersecurity workforce gap makes securing the necessary talent a difficult and expensive task. This challenge is highlighted in the ISC2 - Cybersecurity Workforce Study, 2023[2], which reports that the gap between needed and available workers has grown by 12.6% year over year, even as the cybersecurity workforce itself has expanded by 8.7%. With a managed security provider, an asset owner can receive threat detection and response services supported by an advanced SOC with readily available services scalable for any industrial organization.

TYPICAL SOC IS DESIGNED TO

- Identify potential threats early
- Hunt for anomalous behavior
- Analyze signs of compromise
- Monitor, identify and respond to security events
- Collect log information through an agentless method
- Correlate advanced data tailored to ICS/OT assets
- Improve security for connectivity to collectors
- Collect, store and normalize event data security informatio
- Create built-in security analytics integrated with threat intelligence feeds
- Enable in-depth security incident investigation
- Create quantifiable operational metrics
- Initiate investigations performed by recognized industrial cybersecurity professionals
- Provide actionable countermeasures for incident response
- Create comprehensive, customizable reports allowing for greater insight

GROWING ICS VULNERABILITIES

Industrial Control Systems (ICS) are becoming increasingly vulnerable to cyberattacks, making proactive threat detection and response crucial. Recent analyses show that memory corruption errors are particularly common, highlighting the risks of outdated ICS software that wasn't designed with modern security protocols in mind.

The number of ICS vulnerabilities disclosed each year continues to skyrocket. In the first eight months of 2023 alone, CISA issued 240 advisories specifically targeting industrial control systems[3]. This alarming trend doesn't even consider vulnerabilities in other connected devices and systems.

Ransomware remains the most pervasive threat, with attackers becoming more sophisticated and causing widespread disruptions through data theft, network infiltration and financial extortion[4]. In worst-case scenarios, ransomware can cripple critical systems within hours of infection.

HOW TO IMPROVE SECURITY FOR YOUR INDUSTRIAL CONTROL SYSTEMS:

Adopt Frameworks:

Security frameworks like MITRE ATT&CK® and its ICS-specific counterpart provide valuable blueprints for understanding adversary tactics and techniques. They are a powerful tool to develop a more robust security posture.

Constant Vigilance:

With legacy ICS software often vulnerable, thorough monitoring and vulnerability management are crucial.

Proactive Response:

Threat detection and response services identify potential attacks before they cause major damage.

Seek Experienced Help:

Managed security providers with extensive experience in ICS security and frameworks like MITRE ATT&CK® can be invaluable allies for businesses lacking internal resources.

PROACTIVE CYBERSECURITY APPROACH

While an in-house security team focuses primarily on incident response, a managed security services provider proactively monitors systems to help an organization detect anomalous behavior before a major incident occurs. Some providers offer cyber threat hunting capabilities, actively seeking out signs of intrusion. The goal is to maximize uptime, resilience and the potential to prevent attacks entirely. The use of managed security service providers may also enable an organization to obtain this assistance at a fraction of the cost of building an equivalent in-house program.

FINDING THE RIGHT MANAGED SECURITY SERVICE PROVIDER

When seeking an OT-centric managed security service, manufacturers should consider providers who offer:

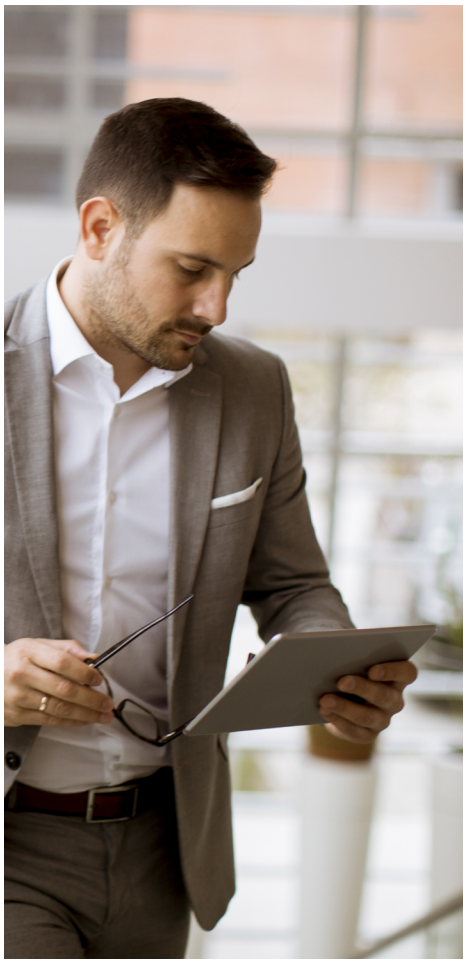
- 24/7 security operations center capabilities for full visibility into operations
- A plan for containment actions in the event of an attack
- Containment methods that integrate with your organization's policies and procedures
- Technology compatible with your existing security controls and IT environment
- Experience with similar organizations, industry verticals and locations
- State-of-the-art analytics technology for accurate diagnosis of anomalous behavior
- The capability to help you detect and eliminate threats through their knowledge of tactics, techniques and procedures (TTPs) of threats, and threat actors
- A plan to ensure open communication between the provider and the asset operator
- A plan to establish and communicate a clear security program for everyone in the organization

MSS AMIR

Honeywell Managed Security Services with Advanced Monitoring and Incident Response (AMIR) is designed to deliver 24/7 OT cybersecurity proficiency and rapid response, continuously monitoring, detecting potential threats, hunting for anomalies and analyzing compromises before significant damage occurs. Honeywell AMIR is staffed by experienced cybersecurity professionals with OT-specific knowledge, complementing your existing IT/OT cybersecurity programs. Vendor-neutral support for both Honeywell and non-Honeywell ICS assets is designed to provide a comprehensive solution for your control systems. Honeywell AMIR is part of the Honeywell Managed Security Services (MSS) end-to-end solution, designed to improve security for your OT environments and ICS assets. AMIR is being deployed globally to enhance and mature cybersecurity programs for industrial companies.

THE RIGHT PROVIDER WILL EASE THE BURDEN

Asset owners need to accelerate digital transformation initiatives while tackling cybersecurity challenges consistent with industry best practices. This may include improved security for remote access, addressing workforce shortages, and managing the complexities of IIoT and risk reduction.



HONEYWELL INDUSTRIAL CYBERSECURITY

Honeywell Industrial Cybersecurity better protects industrial assets, operations and people from digital-age threats. With more than 15 years of OT cybersecurity expertise and more than 50 years of industrial domain expertise, Honeywell combines proven cybersecurity technology and industrial know-how to maximize productivity, improve reliability and increase safety. We provide innovative cybersecurity software, services and solutions to better protect assets, operations and people at industrial and critical infrastructure facilities around the world. Our state-of-the-art cybersecurity centers of excellence allow customers to safely simulate, validate and accelerate their industrial cybersecurity initiatives.

[1],[2] – ISC2 - CYBERSECURITY WORKFORCE STUDY 2023

[3] – CISA - ICS Cybersecurity Alerts & Advisories

[4] – ENISA - Threat Landscape 2023

For more information

www.honeywellaidc.com

About Honeywell

Honeywell is an integrated operating company serving a broad range of industries and geographies around the world. Our business is aligned with three powerful megatrends – automation, the future of aviation and energy transition – underpinned by our Honeywell Accelerator operating system and Honeywell Forge IoT platform. As a trusted partner, we help organizations solve the world's toughest, most complex challenges, providing actionable solutions and innovations through our Aerospace Technologies, Industrial Automation, Building Automation and Energy and Sustainability Solutions business segments that help make the world smarter, safer and more sustainable. For more news and information on Honeywell, please visit www.honeywell.com/newsroom.

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308
www.becybersecure.com

Whitepaper | Rev 1 | 07/2024

THE FUTURE IS WHAT WE MAKE IT

Honeywell