Honeywell | Industrial Cybersecurity

Honeywell Forge Managed Security Services

Advanced Monitoring and Incident Response

Service Note

Honeywell provides 24/7 security monitoring, threat detection, and incident response for today's demanding Industrial Control System and Operational Technology environment.

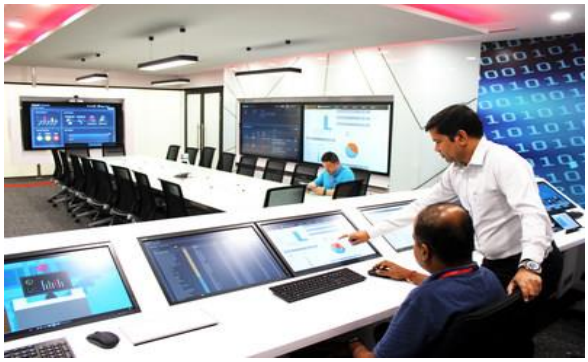
In today's threat landscape, emerging cybersecurity vulnerabilities pose a serious hazard to Industrial Control System (ICS) and Operational Technology (OT) environments. Cyberattacks on critical infrastructures are relentlessly becoming more sophisticated and targeted, making it difficult to identify critical cybersecurity events across a diverse and highly complex industrial infrastructure. The effects of a successful attack may result in operational shutdowns, damaged equipment, financial loss, intellectual property theft, and substantial health and safety risks. As such, it is imperative that industrial organizations monitor the right data sets to build an effective threat defense and improve their overall security posture.

Plant operating companies of all sizes must implement real-time cybersecurity threat monitoring and incident response to ensure greater vigilance over control systems and networks and plant operations. This requires a Security Operations Center (SOC) capability dedicated to critical ICS assets.

Experience has shown that 24/7 threat monitoring, detection and incident response, delivered as a managed security service, allows plant owners/operators to accelerate the detection of cybersecurity-related disruptions and reduce the impact before they cause downtime. This approach is one of the fastest ways to go from zero to sprinting, increasing the likelihood of detecting a potential threat actor.

Furthermore, a proactive cybersecurity managed solution can be implemented at a fraction of the cost of an in-house equivalent solution.

Honeywell's Solution



AMIR solution includes:

- *24/7 threat monitoring and correlation of security events*
- *Investigation and analysis of key indicators of compromise*
- *Incident response support to act on security events in a timely manner*
- *Threat intelligence and incident reporting*
- *Detailed reporting that includes actionable countermeasures and remediation guidance*

Complements other MSS Services offerings:

- *Secure Remote Access*
- *Patch and Anti-Virus Automation*
- *System and Performance Monitoring*

FEATURES & BENEFITS

- 24/7 threat monitoring and detection
- Threat visibility and remediation support
- Advanced correlation tailored to ICS/OT assets
- Log management and monitoring
- Incident response support
- OT security technology stack for automated incident identification
- In-depth investigation by industrial cybersecurity experts
- Detailed reporting of incidents with analysis and recommendations
- Advanced orchestration capabilities
- Continuously evolving skills and process improvements
- Support and augmentation of in-house expertise
- Remediation support
- Reduced risk exposure

Designed for the OT environment, Honeywell's Advanced Monitoring and Incident Response (AMIR) service helps to improve OT cybersecurity and increase operating resilience. The service provides 24/7 OT cybersecurity expertise and rapid response to current and emerging cyber threats by continuously monitoring and identifying potential threats early, hunting for anomalous behavior and analyzing signs of compromise in an OT environment.

Honeywell's AMIR solution helps accelerate cybersecurity threat detection by enabling proactive security monitoring along with threat intelligence and analysis. The result is greater visibility into cybersecurity threats, while minimizing the risk of severe operational, financial and reputational damage—enabling you to detect and protect your organization against today's cyber-attacks.

Figure 1. Honeywell provides an end-to-end AMIR solution for the industrial sector.

AMIR is a Security as a Service (SaaS) within the Honeywell Forge Managed Security Services (MSS) portfolio. There are more than 500 Forge MSS sites worldwide, leveraging proprietary OT-specific technology, with 15+ years of experience in industrial cybersecurity, and thousands of ICS projects delivered around the globe.

The AMIR Service complements the customer's current IT/OT program, builds upon their existing infrastructure (no need to "rip and replace"), and provides an effective cybersecurity managed solution at a fraction of the cost of an equivalent in-house solution, which requires building and managing an OT-specific SOC with 24/7 "eyes on the glass" monitoring to reduce the risk of cyber-attacks.

Delivered through secure remote access, Honeywell's AMIR service covers a broad range of data sources and OT-specific communication protocols. This solution contrasts with other third-party MSS providers or in-house solutions that rely on basic monitoring, which lack a proactive approach to securing critical assets, as well as IT SOC vendors who do not have OT domain knowledge, including expertise in different protocols and assets.

AMIR allows you to harness the power of Security Information and Event Management (SIEM) and Security Orchestration and Automated Response (SOAR) technologies, combined with human heuristics and operational expertise provided by experienced Honeywell MSS global delivery teams. The outcome is a simplified, easy to deploy security monitoring, threat detection and incident response solution that proactively correlates, detects and responds to security events in a timely and cost-effective manner.

Honeywell's recognized experts in cybersecurity for Distributed Control System (DCS) and Supervisory Control and Data Acquisition (SCADA) architectures deliver the comprehensive AMIR solution. These services merge human decision-making and machine intelligence to provide an efficient, scalable and modular approach for a wide range of control system infrastructures and corporate cybersecurity objectives.

Our Approach

Honeywell's end-to-end AMIR solution operates as the brain of your OT security program, securely collecting and analyzing event log data 24x7 from multiple sources, including firewalls, IDS/IPS, routers, switches, Windows, Linux, Honeywell Experion® PKS and other lower level ICS assets. It proactively automates and orchestrates the detection of suspicious and anomalous behavior, alerting Honeywell cybersecurity analysts immediately if deeper forensic investigative analysis is required. Industrial facility personnel receive a detailed security incident report on the specific cybersecurity event, which offers threat insights to help site personnel oversee and protect crucial OT assets.

The AMIR service is integrated with Honeywell's proprietary security remote connectivity solution powered by the Honeywell Forge Cybersecurity Suite, which is a secure remote connectivity solution for OT/ICS environments that provides a single secure, TLS-

Many industrial control system users require assistance in identifying compromised systems and networks, effectively containing any incident caused by malware attacks, and then rapidly preventing a new incident or attack.

Honeywell's Advanced Monitoring and Incident Response service is designed to improve your security posture and reduce cyberattack surfaces.

encrypted connectivity tunnel used to enable a secure and trusted channel for transferring security event log data to the AMIR service. Advanced monitoring security logs and event information then connect with the AMIR security technology stack to create a versatile layered defense security program for the OT environment.

The key features of the AMIR service include:

Log Collection

- Centralized, agent-based log collection method

Universal Data Collector

- Collects, stores and normalizes security event data

Built-in Security Analytics

- Integrated and correlated with various threat intelligence feeds

Secure Connectivity to Collectors

- Integrated with proprietary connectivity

Threat Monitoring

- Real-time threat monitoring, event correlation and expert analysis of malicious ICS activity

Security Event Monitoring

- Monitor, identify and respond to security events

Security Incident Investigation

- In-depth analysis of abnormal behavior

Security Incident Response

- Provide actionable countermeasures

Customer Reporting

- Comprehensive reports with insights and recommendations

Ticketing & Case Workflow

- Quantifiable operational metrics

Ad-Hoc Threat Hunting

- Proactive actions to better detect possible security gaps and breaches

Honeywell's cybersecurity experts at our global SOC monitor and analyze activity on networks, servers, endpoints, databases, applications, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise.

Our incident response strategy employs a comprehensive priority matrix that ranks incidents based on their impact and urgency. The impact can range from extensive/widespread to minor/localized, and the urgency can vary from critical to low. In-house users receive real-time alerts by text or email of important security issues.

For More Information

Learn more about how Honeywell's AMIR solution can improve cybersecurity, by visiting www.becybersecure.com or contact your Honeywell Account Manager, Distributor or System Integrator.

Honeywell Process Solutions

2101 CityWest Blvd.
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

Honeywell