Honeywell | Service Note

HONEYWELL MANAGED SECURITY SERVICES

ADVANCED MONITORING & INCIDENT RESPONSE

Honeywell's Advanced Monitoring and Incident Response (AMIR) service provides 24x7 security event monitoring, detection, and response for today's demanding Industrial Control System (ICS) and Operational Technology (OT) environment.
AMIR can help protect industrial operations with real-time cybersecurity monitoring.

The stakes are high: Today's advanced cyberattacks threaten most ICS/OT systems, potentially leading to downtime, damage, and safety hazards.

Detection is key: Companies need proactive threat monitoring focused specifically on industrial environment to uncover attacks before they succeed.

Managed services are designed to deliver proficiency and effectiveness: Companies can outsource their security operations center (SOC) for 24/7 threat detection, response, and cost savings.

Act now: Don't wait for a breach. Implement a modern cybersecurity solution designed to protect your unique operations.

AMIR Can Help Protect Your OT Environment

FEATURES & BENEFITS

- **Global Threat Intelligence:** Help uncover threats worldwide, enabling proactive defense strategies.
- **Standardized Security Processes:** Support consistent protection with measurable results, tailored to OT/ICS environments.
- **Around-the-Clock Vigilance:** Help find threats with continuous system monitoring.
- **Proficient Threat Analysis:** Deep analysis by OT-specialized cybersecurity professionals for valued response.
- **Tailored Alerts and Reports:** Gain actionable insights and help maintain full situational awareness.
- **Preventative Threat Hunting:** Support to uncover hidden vulnerabilities before attackers exploit them.
- **Rapid Incident Response:** Help minimize downtime and damage with expert guidance during a breach.
- **Know Your Enemy:** Leverage deep knowledge of threat tactics and motivations to help stay ahead.
- **Advanced Security Platforms:** Harness the power of SIEM and SOAR for sophisticated threat detection and response.
- **Outcome-Focused, Cost-Effective Model:** Help achieve security goals predictably and efficiently.
- **Test Your Readiness:** Tabletop exercises help reveal strengths and areas for improvement.
- **Centralized Log Management:** Streamline analysis and accelerate threat detection.
- **24/7 Protection:** Help defend your operations **24/7/365**.
- **Accelerated Remediation:** Help resolve issues rapidly with expert support.
- **Minimize Risk:** Support proactive reduction of your organization's exposure to cybersecurity threats.
- **Stay Ahead of the Curve:** Continuously adapt and improve your security posture.
- **Extend Your Team:** Augment in-house capabilities with the help of specialized OT cybersecurity professionals.

Honeywell's **AMIR** provides advanced monitoring and incident response services specifically designed to safeguard OT environments, delivering:

- **24/7 Threat Vigilance:** Designed for round-the-clock monitoring by OT cybersecurity professionals to detect potential threats at the earliest stages.
- **Proactive Threat Hunting:** Designed to seek out anomalies and signs of compromise, going beyond basic monitoring.
- **Rapid Response:** Designed for accelerated response through threat intelligence and analysis, to help in protecting against operational, financial, and reputational damage.

AMIR, part of the Honeywell Managed Security Services (MSS) portfolio, leverages:

- **Deep OT Knowledge:** 15+ years of industrial cybersecurity experience and knowledge of specialized OT protocols.
- **Proven Global Delivery:** Trusted by over 500 sites worldwide supported by Honeywell MSS
- **Cost-Effectiveness:** Designed to help avoids the high cost of building and staffing an in-house OT SOC.

CASE STUDY 1:

Enhancing Cybersecurity Resilience at a Major European Refinery

Customer Challenge:

- The refinery recognized the growing threat of cyberattacks targeting OT environments. They lacked the internal staffing and expertise to continuously monitor their industrial network for potential intrusions or malicious activity.

Honeywell Solution:

- Honeywell deployed its Advanced Monitoring and Incident Response (AMIR) service to support 24/7 active monitoring of the OT environment for signs of a cyber breach.

Benefits:

- Helped reduced the refinery's vulnerability to cyberattacks by providing continuous 24/7 active monitoring and early threat detection.
- Helped enhance operational resilience by offering a solution that is designed to quickly identifying and respond to potential incidents, AMIR helped strengthen the refinery's ability to maintain production and avoid costly downtime.
- Helped provide a cost-effective alternative to building an in-house security operations center (SOC) dedicated to OT cybersecurity.

AMIR is designed to seamlessly integrate with your existing infrastructure and covers a wide range of OT data sources. Unlike IT-focused solutions or basic monitoring, AMIR is designed to combine:

- **Advanced Technologies:** SIEM and SOAR capabilities for sophisticated threat detection.

- **Experienced Analysts:** Honeywell's OT security professionals provide analysis and response guidance.

How AMIR Works:

Honeywell's end-to-end AMIR solution is designed to be the heart of your OT security program. It is designed to privately collect and analyze event log data 24/7 from various sources (firewalls, IDS/IPS, network devices, Windows, Linux, Experion® PKS, and other ICS assets). AMIR is designed to automate detection of suspicious behavior, immediately alerting Honeywell analysts when deeper investigation is needed. To help you overcome any possible cyber-attack, AMIR is designed to provide a coordinated response with clear recommendations and countermeasures to help protect your operations and assets. After an incident is detected, AMIR customers receive a detailed incident report with actionable insights to help them protect their critical assets.

AMIR Key Features

AMIR helps to safeguard your OT environment from cyber threats and it is designed to provide:

- **Centralized log collection** by gathering security data from across your OT network, providing a single, comprehensive view for enhanced threat detection.
- **Universal data collection** to seamlessly integrate with diverse data sources, normalizing security events for streamlined analysis.
- **Integrated threat intelligence** to leverage up-to-date threat feeds to correlate events with known attack patterns, ensuring early detection.
- **Private connectivity** by establishing a private, TLS-encrypted channel for safe data transfer during monitoring.
- **Near real-time threat monitoring** for around-the-clock vigilance, proficient analysis, and event correlation to spot malicious activity within your OT systems.
- **Security event monitoring** for proactive monitoring and timely response to security incidents to help minimize potential impact.
- **In-depth incident investigation** for thorough analysis of anomalies to help pinpoint the root cause and scope of potential attacks.
- **Actionable incident response** for coordinated response with clear recommendations and countermeasures to protect your operations and assets.
- **Comprehensive reporting** to offer detailed reports with valuable insights to help you understand your security posture and strengthen defenses.

AMIR helps streamline incident response and proactive threat hunting. It is designed to deliver:

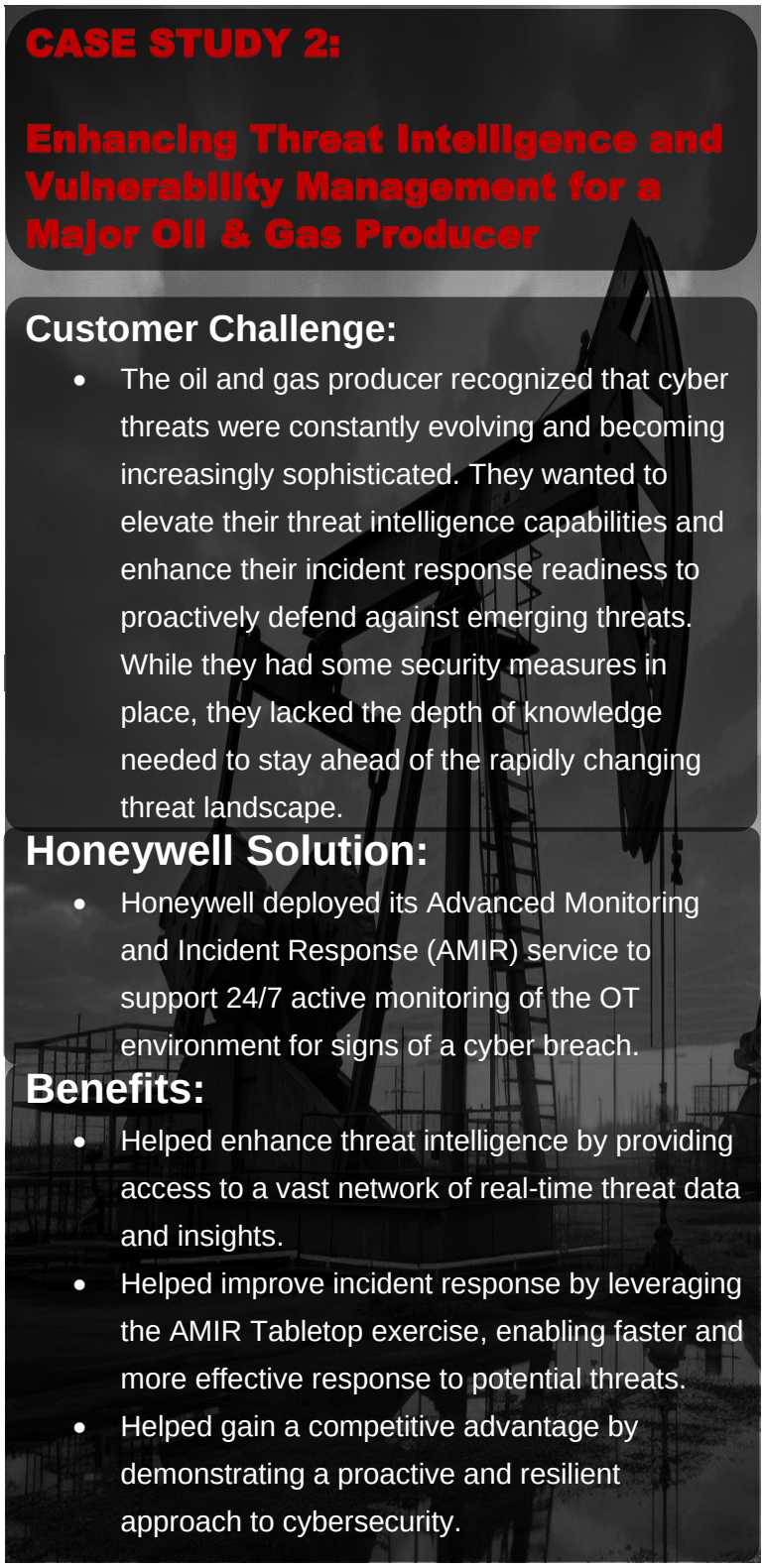
- **Efficient ticketing & workflow management** for seamless tracking of security incidents to help ensure timely resolution and clear communication.
- **Measurable results** with integrated operational metrics to demonstrate the effectiveness of the service, providing insights for continuous improvement.
- **Proactive threat hunting** to enable Honeywell cyber professionals to actively seek out potential security gaps and breaches in the customer environment(s) , proactively addressing vulnerabilities before they can be exploited.

Honeywell's Global SOC: Your Eyes on the Network

Honeywell's cybersecurity specialists at our global SOC are enabled to relentlessly monitor your systems for signs of compromise; AMIR professionals analyze activity across networks, servers, endpoints, databases, applications, and more, seeking out anomalies (eg: unusual traffic patterns, unauthorized access attempts, PLC reconfigurations, unexpected user creations, communications with unmapped devices, changes to critical control system parameters, and so on) that could indicate security issues.

Benefit from Access to Global Threat Intelligence in OT

Access to OT specific threat intelligence Honeywell uncovers from other facilities monitored in the Honeywell's' pool of AMIR customers located around the world and in multiple industries.



Prioritized Incident Response

Our response strategy uses a detailed priority matrix to which is designed to rank incidents by impact (extensive/widespread to minor/localized) and urgency (critical to low). This helps ensure the most critical threats are addressed immediately.

Near Real-Time Alerts: Stay informed with near real time text, email, or phone notifications about high-priority security events.

AMIR Complements Honeywell's MSS Portfolio for Comprehensive Protection

AMIR is designed to work seamlessly as a necessary addition with Managed Security Services:

- **Secure Remote Access:** Is designed to safeguard remote connections to critical OT assets.
- **Patch and Anti-Virus Automation:** Is designed to streamline essential security updates.
- **System and Performance Monitoring:** Is designed to ensure optimal health and efficiency of OT environment.

Honeywell: Industrial Cybersecurity. Simplified. Strengthened. Trusted.
We help protect plants and critical infrastructure with proven solutions.
end-to-end expertise, 1000+ global projects delivered, and certified professionals.
Learn how we can help safeguard your systems.

For more information
www.honeywell.com

Honeywell
855 S Mint St Charlotte, NC,
28202-1517 USA
www.honeywell.com

Honeywell