# HONEYWELL FORGE MANAGED SECURITY SERVICES
# ADVANCED MONITORING & INCIDENT RESPONSE

HONEYWELL FORGE

# THE CONNECTED ENTERPRISE: WHAT IT/OT CONVERGENCE MEANS FOR YOUR BUSINESS

> Emerging cyber vulnerabilities are a serious threat to the industrial environment and critical infrastructure. It's harder than ever to identify sophisticated, multi-vector attacks on an Industrial Control Systems (ICS). Almost half of industrial businesses have experienced a cyber incident in the last 12 months.[1]

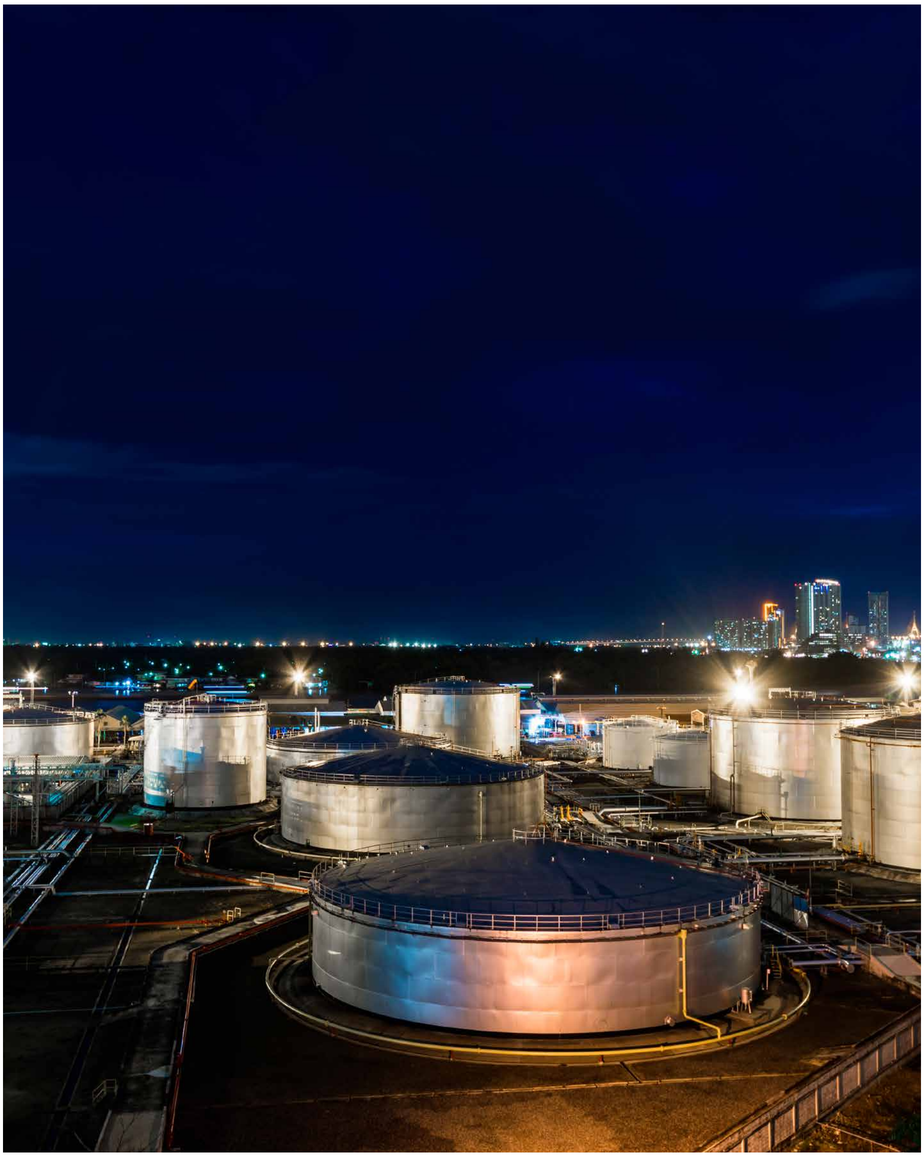
Many industrial organizations lack the staff, budget and skills to manage cyber threats proactively, and may have limited visibility into ICS assets. With so many potential threats to these assets, prioritization is a challenge.

Plant owners/operators need a layered, defense-in-depth security strategy to keep their control system safer, meet compliance requirements and better secure the connections required for smooth operations and enhanced performance.

Honeywell's new Advanced Monitoring & Incident Response (AMIR) service meets the challenges of today's plants. We enable you to more safely connect networks, assets, devices, and people in the industrial environment and keep them more secure.

With round-the-clock support, expert Operational Technology (OT) security analysis and a sophisticated Security Information and Event Management (SIEM) technology platform, AMIR is a powerful solution to keep your plant and people better protected.

**Threats to Your Control Assets**
Industrial control systems, assets and devices increasingly connect to enterprise and Information Technology



(IT) systems, bringing improved visibility, better planning and more productivity—but also greater risk.

With thousands of connected devices, vulnerabilities have multiplied. Programmable Logical Controller (PLC) and Supervisory Control and Data Acquisition (SCADA) devices have been joined by connected network devices, workstations, cameras, tablets, and phones. Virus, malware or misconfiguration in any one of these devices could result in a route to critical ICS systems, putting continued production and safety at risk.

IT/OT convergence means operations have gained all the benefits of connectivity common in the IT environment—and all the dangers.

## THE NEED FOR A NEW TYPE OF SECURITY

Plants need a new type of security to help defend against today's expanded attack surface. Traditional SIEM solutions used by IT teams analyze data from antivirus and firewalls to identify threats, but they are poorly suited to OT systems.

Devices in the industrial network are often invisible to such solutions, and IT security tools can even threaten the continued production and smooth running of the plant they are designed to protect. Many endpoint agents aren't supported by ICS devices; untested patches can risk operational outages; and vulnerability scanning can cause controllers to crash and reset.

Industrial operators need solutions to collect and analyze all their data from across the OT environment, as well as OT-specific tools to safely provide visibility and control across the business.

## THE CASE FOR A MANAGED SECURITY SOLUTION

To address the threat to their operations, industrial organizations need a Security Operations Center (SOC) that is specifically designed to detect and respond to threats and monitor and adapt to the threat landscape.

Establishing an in-house SOC solution requires significant and ongoing investment. The costs of recruitment, salaries, training, utilities, maintenance, and licenses are unpredictable and can quickly mount up. Moreover, surveys consistently show a global shortage of cybersecurity talent. For experts with OT experience, there is even greater demand. At best, organizations face escalating salary costs; at worst, skills gaps and a lack of competencies that undermine the effectiveness of the cybersecurity strategy.

A managed threat detection and response solution can provide industrial operators and infrastructure businesses with cost-effective, and more robust cybersecurity allowing them to focus on their core business. It answers the key challenges of establishing an effective and efficient SOC solution:

- Cost certainty and control, eliminating Capital Expenditure (CAPEX) costs and fixing Operational Expense (OPEX) spending with a single, regular subscription fee
- Round-the-clock monitoring and incident response, with systems protected 24/7 and experts always on call *
- Continually updated with the latest technology and threat analysis to guard against the evolving threat landscape
- Access to experienced cybersecurity professionals with deep domain knowledge and OT expertise

# INTRODUCING AN ADVANCED MONITORING AND INCIDENT RESPONSE SERVICE

> With Honeywell's AMIR Service, we connect to plants and systems across your business and gather security data from firewalls, antivirus software, routers, hardware, control systems, equipment, and other connected devices.

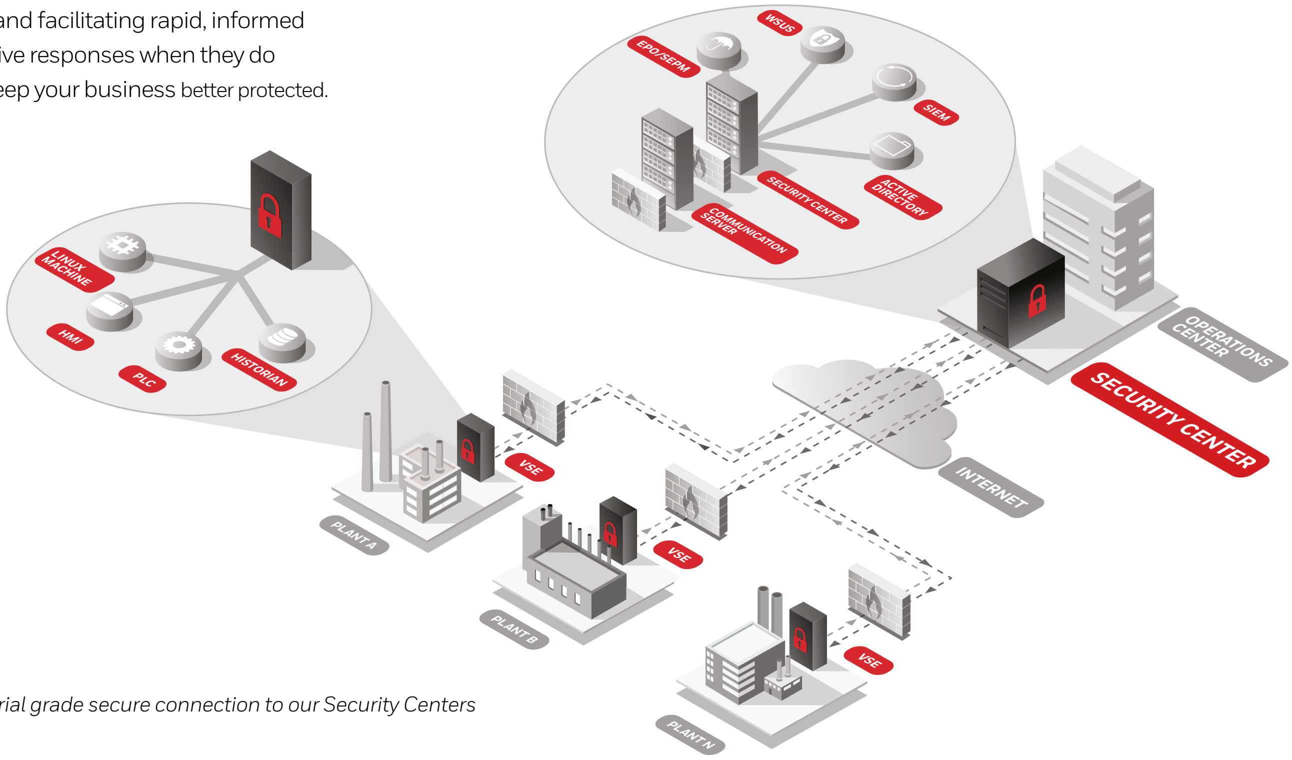
Using Honeywell's end-to-end AMIR solution, industrial organizations can improve their security posture—regardless of their level of cybersecurity maturity. The AMIR solution operates as the brain of an OT security program, constantly monitoring and alerting Honeywell SOC analysts of possible threats.

Aggregated, automatically monitored and rigorously analyzed, AMIR is used to detect anomalies and investigate signs of threats that might be indicative of malware, hackers, internal security breaches or configuration errors. It helps identify and address issues early on, preventing security incidents and facilitating rapid, informed and effective responses when they do occur to keep your business better protected.

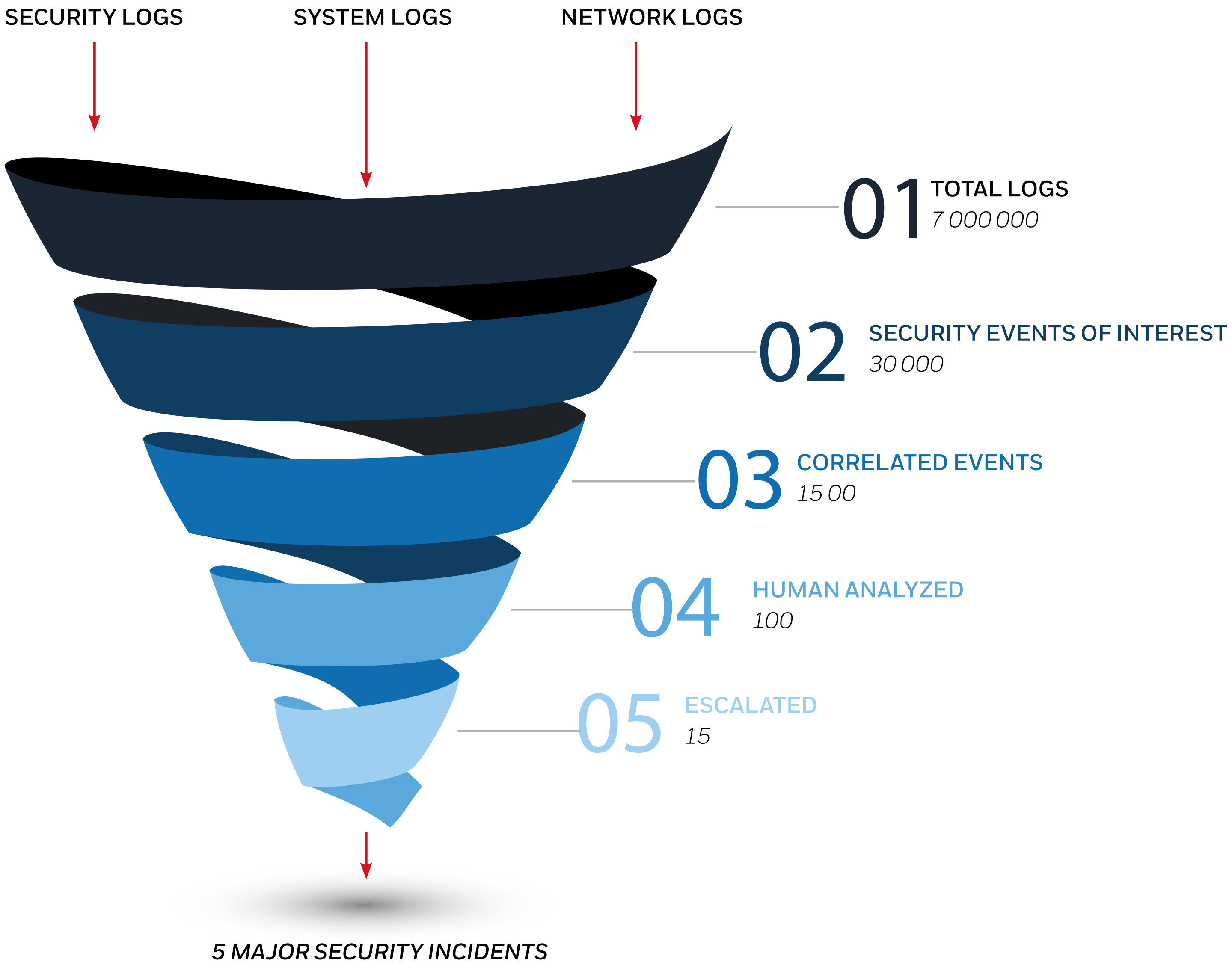
## How it works

Connecting through a secure tunnel to a Virtual Security Engine (VSE) Service Node at each site, Honeywell's Universal Data Collector gathers billions of logs from sources across the plant.

Centralized in Honeywell's Global and Regional Security Operations Centers (SOCs), this data is fed through our advanced Security Orchestration, Automation and Response (SOAR) platform, combining automated monitoring and expert analysis to quickly identify serious security incidents.



*An industrial grade secure connection to our Security Centers*



SECURITY LOGS

SYSTEM LOGS

NETWORK LOGS

01 TOTAL LOGS
*7 000 000*

02 SECURITY EVENTS OF INTEREST
*30 000*

03 CORRELATED EVENTS
*15 00*

04 HUMAN ANALYZED
*100*

05 ESCALATED
*15*

***5 MAJOR SECURITY INCIDENTS***

*SOAR: Identifying the threats that matter*

# BENEFIT FROM AN END-TO-END APPROACH

> Honeywell's AMIR Service provides an organized and comprehensive framework for monitoring and addressing a critical ICS/OT security breach or cyberattack.

## WHAT'S INCLUDED: SOLUTION HIGHLIGHTS

AMIR is a managed threat detection and response service supported by an advanced SOC with ready-to-deploy services scalable for any industrial organization.

- Log Collection: Centralized agentless log collection method
- Advanced Correlation: Tailored to ICS/OT assets
- Secure Connectivity to Collectors: Integrated with proprietary connectivity solution
- Universal Data Collector: Collects, stores and normalizes security event data
- Security Event Monitoring: Monitors, identifies and responds to security events
- Built-in Security Analytics: Integrated and correlated with various threat intelligence feeds
- Security Incident Investigation: In-depth analysis of abnormal behavior
- Ticketing & Case Workflow: Quantifiable operational metrics
- In-depth Investigation: Performed by recognized industrial cybersecurity experts
- Security Incident Response: Providing actionable countermeasures
- Reporting and Insights: Comprehensive, customizable reports

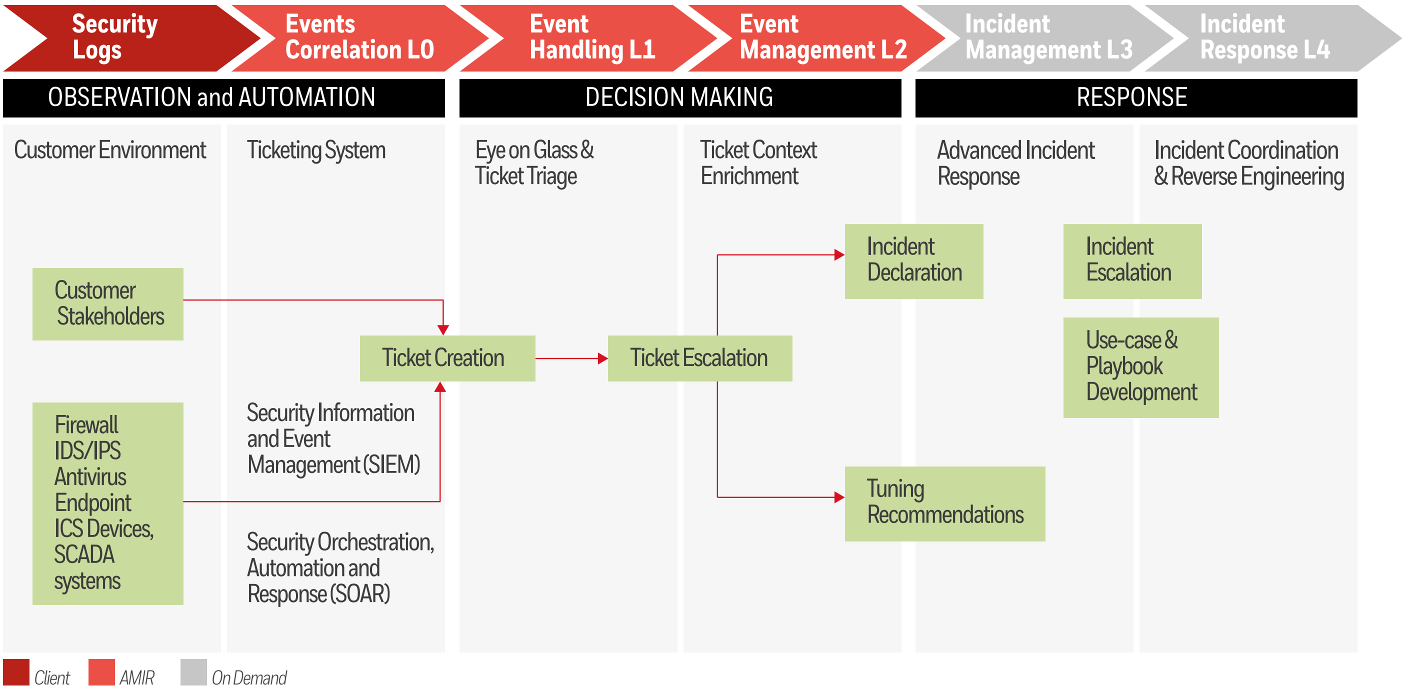
## A COMPLETE SOLUTION

AMIR is a co-managed solution, giving 24/7 protection through Honeywell's OT cybersecurity experts worldwide.*

Under Honeywell's AMIR service, our SOC monitors and better protects networks and assets 24/7. We combine robust SIEM technology with security analysis by experienced OT cybersecurity experts to rapidly respond to threats and address any vulnerabilities identified.

AMIR delivers not just monitoring and analysis, but also incident investigation, intelligence feed correlation, and ad-hoc threat hunting to better reveal security gaps and breaches. With alerts for threats and breaches, our experts rapidly address persistent risks or any events requiring support.

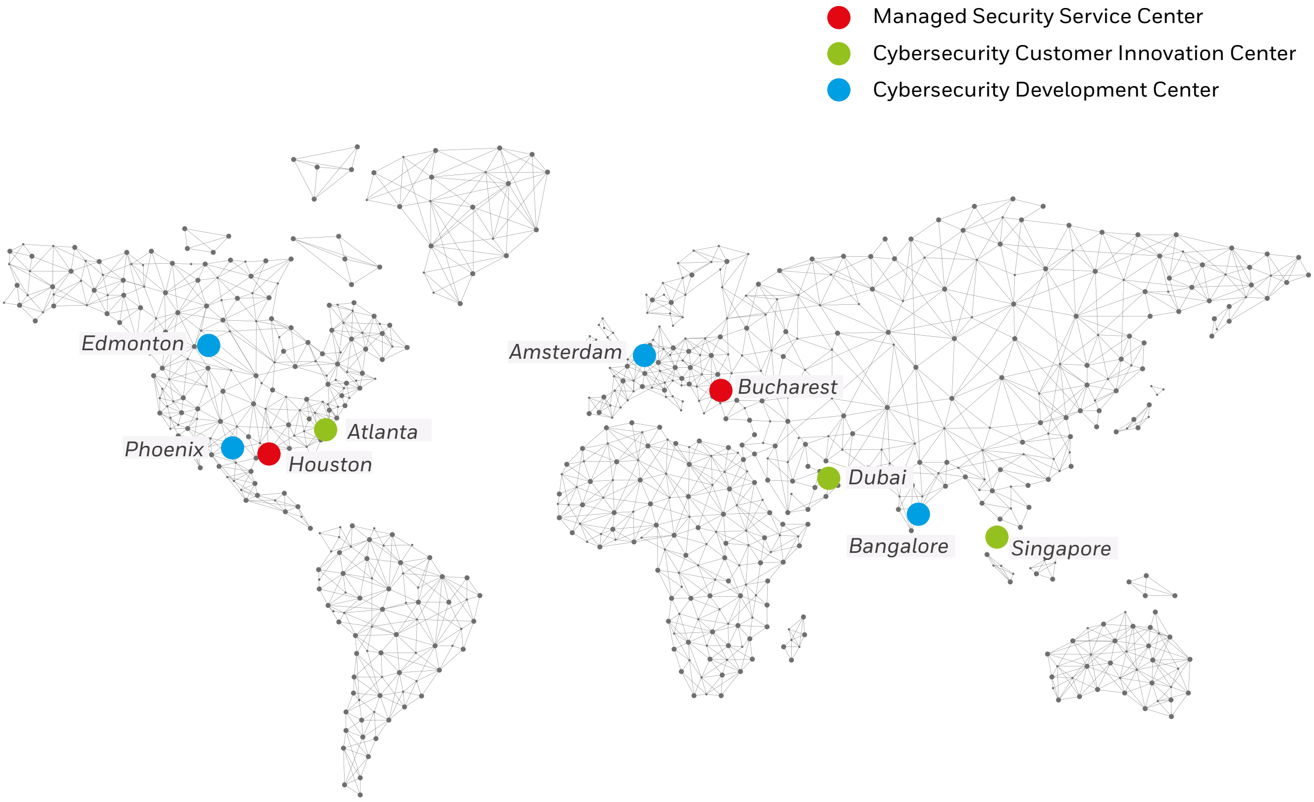
A customer dashboard, combined with ticketing and case workflow, maintain complete visibility for in-house users.


Security Logs
Events Correlation L0
Event Handling L1
Event Management L2
Incident Management L3
Incident Response L4
OBSERVATION and AUTOMATION
DECISION MAKING
RESPONSE
Customer Environment
Ticketing System
Eye on Glass & Ticket Triage
Ticket Context Enrichment
Advanced Incident Response
Incident Coordination & Reverse Engineering
Customer Stakeholders
Firewall IDS/IPS Antivirus Endpoint ICS Devices, SCADA systems
Ticket Creation
Security Information and Event Management (SIEM)
Security Orchestration, Automation and Response (SOAR)
Ticket Escalation
Incident Declaration
Tuning Recommendations
Incident Escalation
Use-case & Playbook Development
Client
AMIR
On Demand

### FOLLOW THE SUN SUPPORT

With AMIR, you gain real-time visibility of threats across the enterprise and a sustainable source of OT cybersecurity expertise to help operations run safely and more smoothly:

- Site-wide visibility of security status and vulnerabilities
- Detects and proactively identifies security issues
- 24/7, follow-the-sun, on-call expertise with a global network of security centers *
- Continuous monitoring and case management
- Investigative and forensics services
- Integrates existing security and SIEM solutions
- Analysis and reports to boost your security posture.


● Managed Security Service Center
● Cybersecurity Customer Innovation Center
● Cybersecurity Development Center
Edmonton
Phoenix
Houston
Atlanta
Amsterdam
Bucharest
Dubai
Bangalore
Singapore

*Honeywell cybersecurity centers*

## EXPERIENCE IN INDUSTRIAL AUTOMATION; EXPERTS IN INDUSTRIAL CYBERSECURITY

Honeywell combines decades of experience in process automation with sophisticated cybersecurity services and solutions. We help protect the availability, safety and reliability of industrial facilities worldwide, and help securely deploy the Industrial Internet of Things (IIoT).

Our complete portfolio includes cybersecurity software, managed security services, industrial security consulting services, and integrated security solutions—all tested and tailored for the OT environment. Trust us to help make your business more connected, more reliable, more productive, and more secure.

**For more information**

To learn more about Honeywell's Industrial Cybersecurity visit www.becybersecure.com or contact your Honeywell Industrial Cybersecurity representative.

**Honeywell Industrial Cyber Security**
Honeywell, 17, Changi Business Park
Central 1, Singapore 486073

Honeywell, Emaar Business Park,
Building 2, Sheikh Zayed Road, Dubai, UAE

Honeywell, 3079 Premiere Parkway,
STE 100, Duluth, GA 30022, USA

www.honeywellprocess.com

AMIR services provide 24/7/365 monitoring, excluding any scheduled downtime, maintenance periods, or any urgent or non-scheduled maintenance events. AMIR services require a stable network connection at the customer site for continuous monitoring, Honeywell does not make any commitments around uptime or availability for the AMIR services. AMIR customers are responsible for maintaining a stable network connection.

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell