HONEYWELL FORGE

CYBER THREAT DETECTION AND MANAGEMENT

Simplified for the ICS/OT environment

Whitepaper

TABLE OF CONTENTS

MANAGED SECURITY SERVICES

Honeywell Forge Managed Security Services can provide threat detection capabilities faster and at lower cost making it an effective strategy to drive value in better-securing an industrial operation and helping to safeguard critical OT assets.

Remote access, work from home, an onslaught of daily online meetings, a dearth of security talent, digitalization, and the pressure to reduce risk are all solid reasons for industrial operators and asset owners to just throw up their hands and say, “I need help to secure my enterprise, but where do I start?”

In addition to all of that complexity, industrial organizations continue to boost connectivity to accelerate digital transformation and remote operations, remote services and support, but at the same time, threat actors know a company’s soft spots and continue to attack by hitting unguarded areas like the software supply chain or focusing on highly profitable ransomware attacks.

That is why more industrial companies are making the move to a managed security services model for their security needs. This way asset owners can have their networks analyzed by a managed security services provider which allows the asset owner to focus on making its revenue generating product or products. Meanwhile, the managed security services provider uses best in class practices from experts across the globe to better protect the network 24 hours a day, seven days a week.

CYBERSECURITY SERVICES MODEL

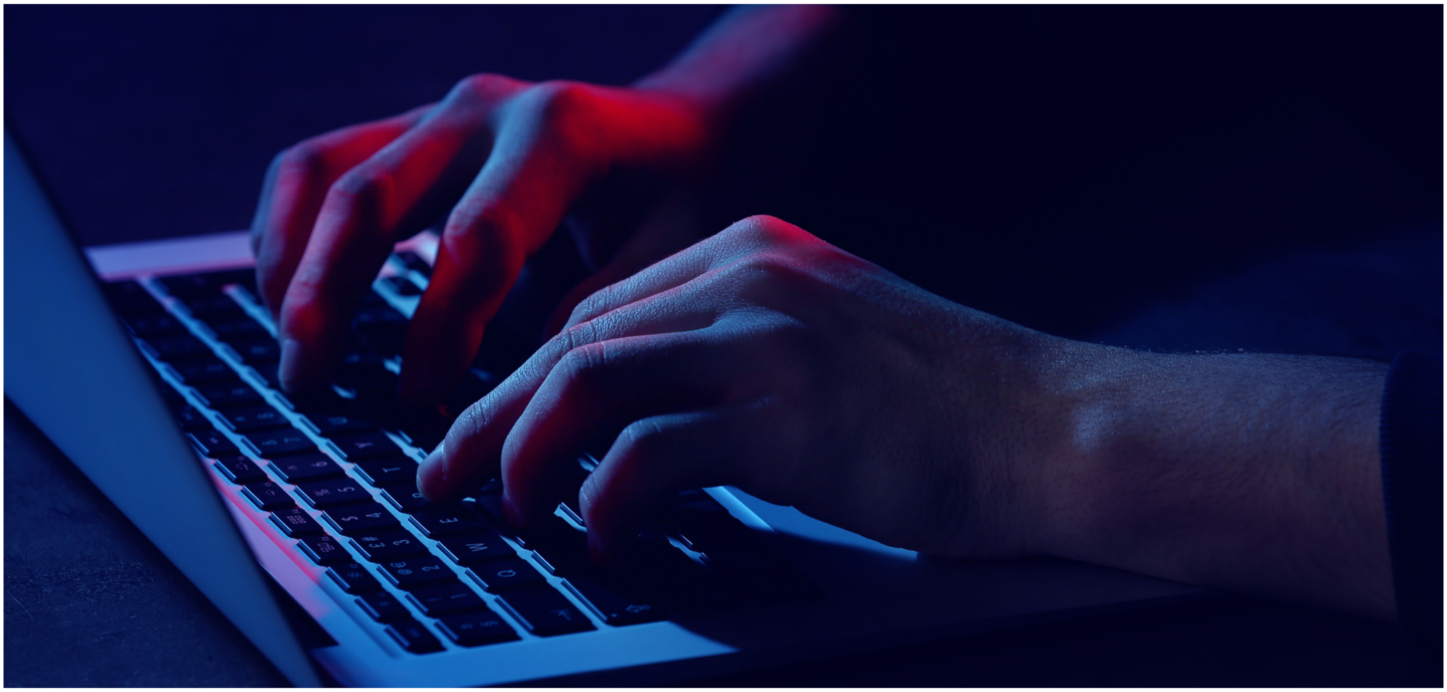
Not all companies can afford to hire in-house cybersecurity experts. With Honeywell Forge Managed Security Services, our experts handle increasingly sophisticated security threats without the need to hire in-house domain, firewall, or security information and event management (SIEM) teams of their own.

Finding and helping remediate anomalous cyber behavior before an actual incident occurs through early threat detection is the goal of a managed security services program . Asset owners need 24/7 OT cybersecurity expertise and rapid response to current and emerging cyber threats by continuously monitoring and 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 logs, devices, network and assets all from a security operations center (SOC). It also proactively identifies and helps mitigate cyber threats and attacks in the very early stages.

Not all companies can afford to hire in-house cybersecurity experts – or even easily find them. With Honeywell Forge Managed Security Services, companies don't have to hire in-house cybersecurity experts to handle the increasingly sophisticated security threats that target specific areas. A managed security services provider can help the asset owner from having to hire a domain expert, a firewall expert, or a security information and event management (SIEM) expert, just to name a few.

In the "Managed Security Services Trends 2020" report by the Herjavec Group[1], which covered multiple industries including manufacturing, 14 percent of respondents said they have no skilled security analysts or incident response personnel in-house and 27 percent of organizations said they can only perform ad-hoc monitoring as the need arises. 24 percent have a team for responding to security incidents when they occur, but they do not perform continuous threat detection. 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 knew they needed ongoing cyber protection.

ANONYMOUS CASE

One global oil and gas provider knew they needed ongoing cyber protection. The problem is they were having a hard time finding staff and they didn't have the budget and skills to manage cyber threats proactively and effectively. In addition, they had limited visibility into ICS assets. With sophisticated attacks occurring with greater prevalence, the need for continuous threat detection for its OT assets was paramount, but they didn't have the time and budget to build their own security program. The company's strength was being an oil and gas provider; they were not a security company.

The company needed more secure remote access; more secure content and data transfer; patch and antivirus management; managed threat detection; 24x7, 365 monitoring; threat alerts and reporting; incident investigation; log collection and analysis, and remote monitoring support.

The company implemented these capabilities through the Honeywell Forge Managed Security Services program to keep its control system safer, meet compliance requirements and better secure the connections required for smooth operations and support.

With more manufacturing organizations sensing attacks are on the horizon and them not having proper personnel in place, it makes more sense to bring on a provider that employs 24x7 monitoring with specific expertise that can constantly check for anomalous behavior before it escalates.

From a cost benefit analysis, with a managed security provider, there is an economy of scale.

Like the oil and gas provider, if an asset owner decides to build its own security department, it will be expensive and time consuming. For a much lower cost, a managed security provider can apply everything it has learned from previous incidents with other clients. When security operations center experts discover an indicator of compromise, it can automatically share the information and pass potential remediations and mitigations on to all participants. While all individual industrial operators remain anonymous, operations center experts share what they learn to the entire community, which then benefits from continuous learning.

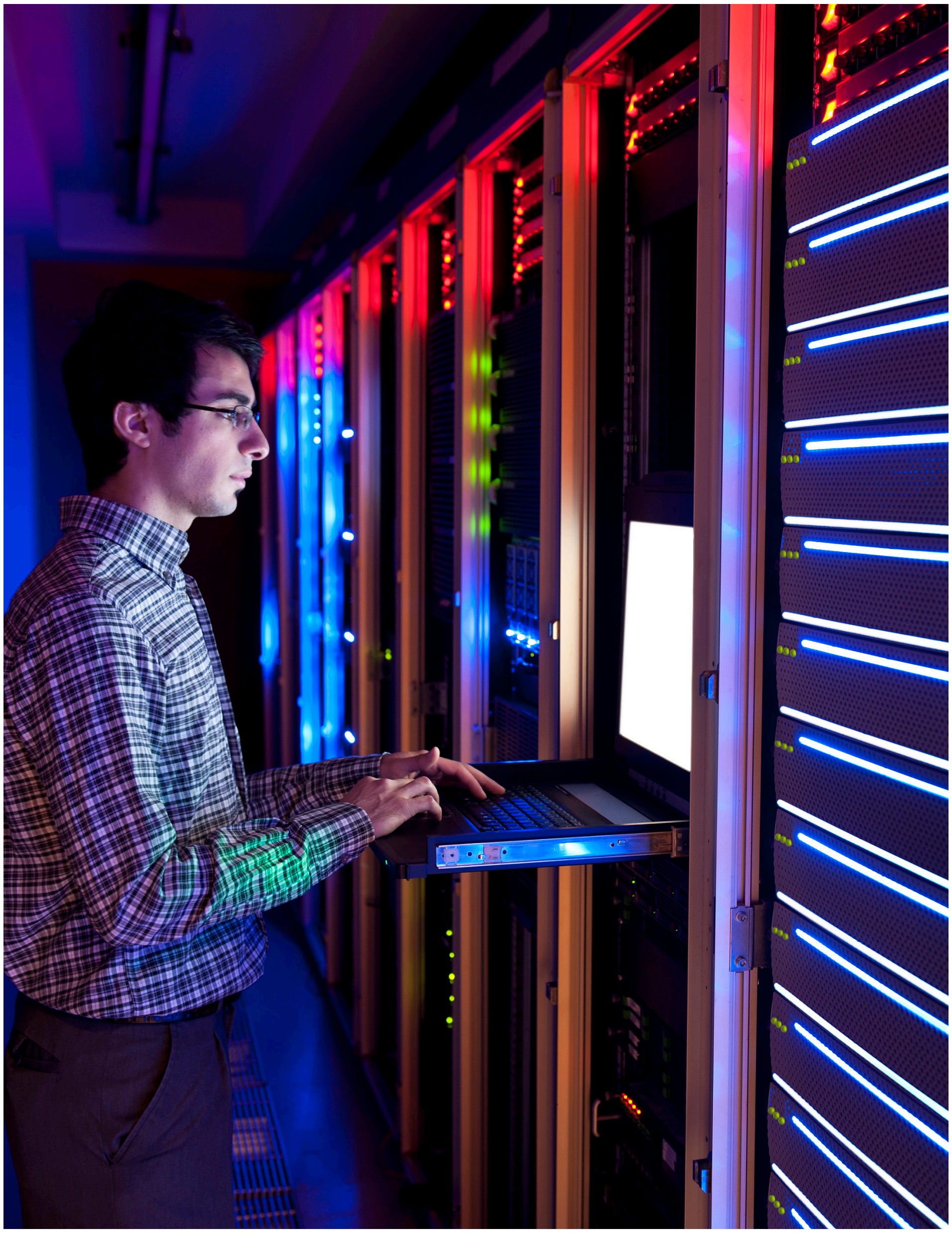
CYBERSECURITY WORKFORCE GAP

Even if the asset owner wanted to start its own security department, it would be difficult as the cybersecurity workforce gap has increased since last year, primarily due to a global surge in hiring demand, according to (ISC)2 Cybersecurity Workforce Study[2]. Using the workforce estimate of the 11 global economies in the report, there is a global workforce gap of 3.1 million, which hits the industrial space hard. Also, in the study, 64 percent of organizations represented have a shortage of staff dedicated to cybersecurity. That lack of skilled cybersecurity personnel is the top concern among survey respondents. In addition, 56 percent of cybersecurity professionals said their organization is at moderate or extreme risk due to cybersecurity staff shortage.

So, with a managed security provider it is possible to receive threat detection and response services supported by an advanced SOC with ready-to-deploy services scalable for any industrial organization.

THE SOC WILL:

- 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
- Secure connectivity to collectors
- Collect, store and normalize event data security information
- Create built-in security analytics where it integrates and correlates with threat intelligence feeds
- Allow for security incident investigation with in-depth analysis of abnormal behavior
- Create quantifiable operational metrics
- Initiate investigations performed by recognized industrial cybersecurity experts
- Provide actionable countermeasures for incident response
- Create comprehensive, customizable reports allowing for greater insight



GROWING ICS VULNERABILITIES

With threat detection and response services, it is possible to detect the growing number of ICS-specific vulnerabilities where an attacker could take advantage of unpatched software or devices on the network.

In a review of the second half of 2020, Nozomi Networks in its "OT/IoT Security Report"[3] analyzed 151 ICS industrial advisories containing new vulnerabilities. The results showed memory corruption errors such as out-of-bound read, out-of-bound write and stack-based buffer overflows represented 58 percent of vulnerability types described in industrial advisories. The report continued by saying this will likely continue, considering the software stacks in ICS environments were not designed with today's connectivity in mind and its consequence in terms of security exposure. All of that points to the need for constant vigilance for network monitoring.

In addition, a common threat to manufacturing is ransomware.

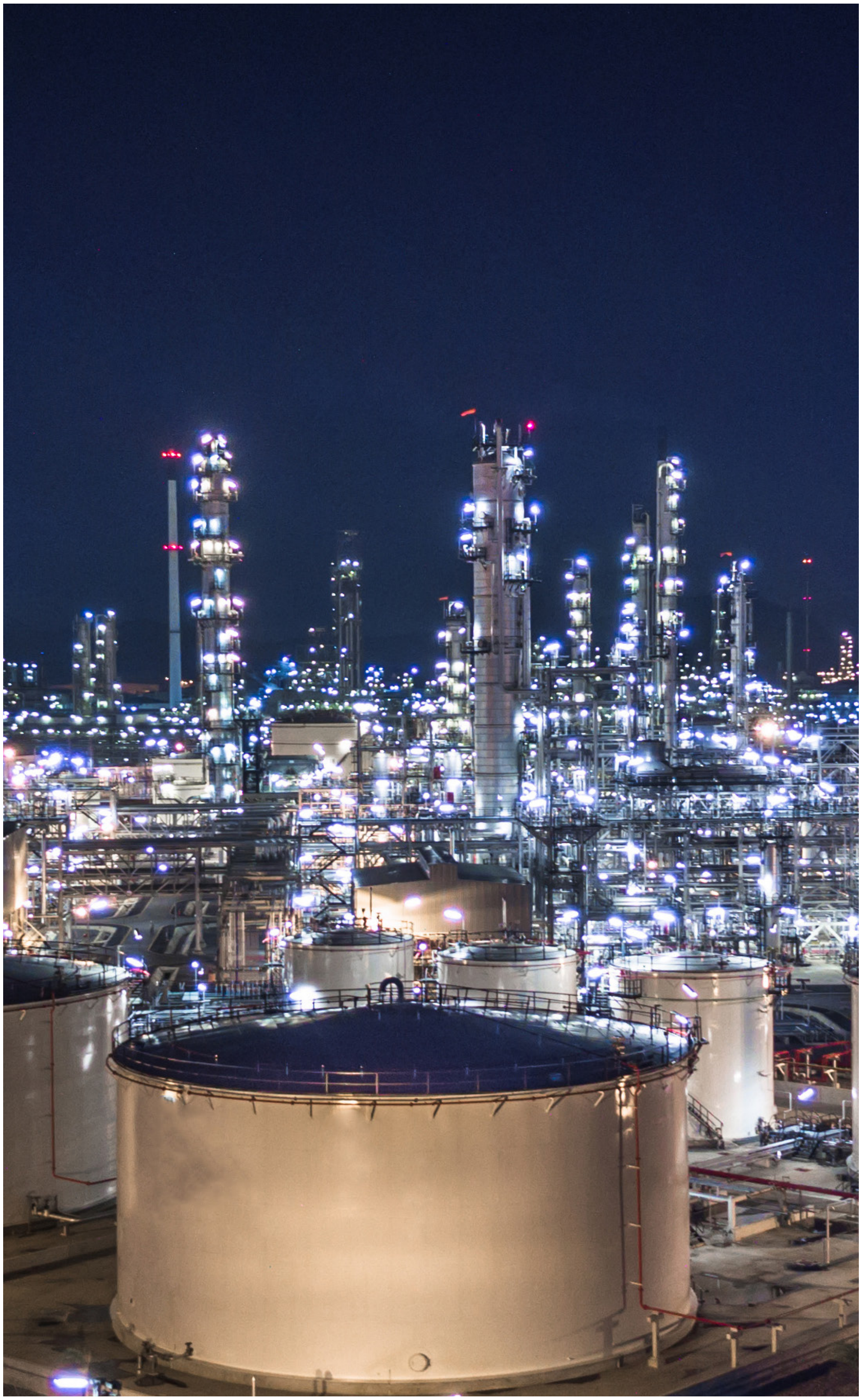
In the Nozomi report, researchers found ransomware continues to dominate the threat landscape, growing in sophistication and persistence. In addition to demanding financial payments, Ryuk, Netwalker, Egregor and other ransomware gangs are exfiltrating data and deeply compromising networks for future nefarious activities. Depending on the targeted network, the length of time from initial infection to ransomware execution can be as quick as a couple of hours.

One way to understand and help thwart the escalation of threats, is to review and understand the MITRE ATT&CK® Framework, which multiple cybersecurity service providers employ. The framework provides a map of tactics and techniques commonly used by attackers. The techniques it documents allows asset owners to understand complex attack scenarios, providing actionable insight to defenders. Furthermore, the framework provides a common language used by the security community to analyze and effectively communicate about incidents. Having a common reference point can be useful in enhancing an organization's security strategies and policies.

The "ATT&CK for ICS" framework describes incidents involving ICS networks, which can be effective in describing incidents and providing detailed insight into threat actors' behavior. For those that have deeper resources to deploy, the framework can be used by security teams to enhance security strategies and policies. For those that don't, a managed security provider that deploys the MITRE framework would be an excellent alternative to pursue.

With data hitting asset owners from all angles, it is vital to understand the right data sets that will ensure the system remains up and running, and that means having experts stay on top of it at all times.

PROACTIVE CYBERSECURITY APPROACH



While an in-house security team would be quick to respond to an incident, by the time an incident occurs, it may already be too late. A managed security services provider, on the other hand, conducts proactive monitoring on the asset owner's legacy system. The provider would look at, and collect, log files and sys files, and discover anomalous behavior way before anything major happens. Some even offer cyber threat hunting capabilities. It would be able to view if a hacker is already sniffing around and moving across the network. The idea is to remain up and running and as resilient to an attack as possible – or even avoid an attack by finding the breadcrumbs and piecing them together before an incident occurs, which can all happen at a fraction of the cost of an in-house equivalent program.

What the provider is looking to do is go beyond the basics of knowing about an attack, but instead create a proactive approach by being able to view suspicious behavior in advance.

FINDING THE RIGHT MANAGED SECURITY SERVICE PROVIDER

When looking for an OT-centric managed security services, a manufacturer should ensure the provider has:

- 24/7 security operations center capabilities to provide 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 that allows for an accurate diagnosis of anomalous behavior
- The ability to detect and eliminate threats through its inherent knowledge and with the assistance of threat data along with the experience of understanding tactics, techniques and procedures (TTPs) of threats, and threat actors
- A plan to ensure the lines of communication between the provider and the asset operator remain fluid and open
- A plan to make sure everyone in the organization understands the security program in case of an incident

THE RIGHT PROVIDER WILL EASE THE BURDEN.

For asset owners to thrive in today's fast-paced global environment, they need to accelerate their digital transformation initiatives and let experts tackle cybersecurity issues like remote access, work from home, a lack of qualified personnel, IIoT and risk reduction that can overwhelm any organization.

MSS AMIR

Honeywell Forge Managed Security Services with Advanced Monitoring and Incident Response (AMIR) 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 before significant damage can occur.

Staffed by cybersecurity experts with specific OT experience, Honeywell AMIR completes your existing IT/OT cybersecurity programs to ease the burden of your cybersecurity needs. In addition, Honeywell AMIR is vendor neutral, supporting both Honeywell and non-Honeywell ICS assets for a complete solution regardless of the brand name on your control system.

Honeywell AMIR is part of Honeywell Forge Managed Security Services (MSS), an end-to-end security as a service solution that helps better protect OT environments and ICS assets. The AMIR offering is already being deployed at multiple sites world-wide to help companies to evolve their cybersecurity maturity.

SOURCES:

(1) “Managed Security Services Trends 2020”

(2) (ISC)2 Cybersecurity Workforce Study, 2020

(3) Nozomi Networks in its “OT/IoT Security Report”

For more information

To learn more, visit:
www.becybersecure.com
Or contact your Honeywell
Account Manager, Distributor, or
System Integrator.

INFOSEC AWARDS
WINNER
CYBER DEFENSE MAGAZINE
2020

CYBER SECURITY
EXCELLENCE AWARDS
★ WINNER ★
2020

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell Connected Enterprise

715 Peachtree Street NE
Atlanta, GA 30308
www.honeywell.com

Honeywell