BETTER SECURE YOUR OPERATIONAL TECHNOLOGY
BUILD IMPROVED CYBER RESILIENCE

Cybersecurity Assessments and Advisory

Honeywell

CYBER THREATS ARE CONSTANTLY EVOLVING AND YOUR FACILITY NEEDS TO KEEP PACE

We proactively test and develop methodologies to help better secure your Operational Technology (OT) systems by using our expertise, proven recommendations, leading applications, and a robust framework enabling us to assess the Cybersecurity risk of your OT environment.

We conduct our initial assessment on site. We meet with you to present a detailed report as well as an executive summary. We collaborate with you on strategies and help you identify aspects in which your OT systems, and facility infrastructure might differ from traditional information technology (IT) systems.

Finally, based on your operational needs and priorities, we give you clear, precise guidance on actions you might elect to better secure your facility.

START WITH EXPERTISE

Our talented and experienced team of Cybersecurity professionals bring you years of industry expertise.

We understand the prevailing threats you may confront, and effective ways to help reduce risks to your OT network.

BUILD RESILIENCE

The National Institute of Standards and Technology (NIST), Cybersecurity Framework (CSF) , ISO 27001 and ISA/IEC 62243 identifies the three key dimensions of Cybersecurity Management, including: people, processes, and technology. Focus on these areas helps to identify appropriate risk management measures for your critical infrastructure and OT network, helping to improve your Cyber resilience.

IDENTIFY VULNERABILITIES

Your network design and associated operating practices, enables us to highlight certain attack vector and vulnerabilities that may not have been accounted appropriately for. This evaluation may include not only an assessment of your OT network, but your connected assets as well.

We can also provide passive and active penetration testing, as needed, to simulate attacks that may uncover additional potential vulnerabilities on your OT network.

PROTECT AGAINST THREATS

Once your potential OT network vulnerabilities are better identified, we work with you to develop a mitigation plan to help guard against threats. We focus on effective and efficient steps to optimize your value and outcomes, while aligning with your existing IT/OT standards and budget. This plan provides precise feedback and guidance, ranging from the status of network configurations and design to recommended application security.

DETECT THREATS

New exploits are always in the works, based on vulnerabilities that are not yet public, which means no system is ever completely risk free. Hence, your ability to quickly identify and address unexpected activity is often critical. We can help you to evaluate potentially effective frameworks and techniques for monitoring your system, and we can also provide remote detection and reporting as an additional service.

RESPOND TO INCIDENTS

If an incident occurs, prompt containment and eradication can help to mitigate further spreading and longer recovery times.

Our team can help you develop an incident- response plan to promote this goal. We also offer an incident response service that connects you with our Cybersecurity experts to further assist in rapidly addressing incidents.

PLAN TO RECOVER

A robust Disaster Recovery Plan (DRP) is typically crucial. Together, we plan the processes and technology needed to help meet your “recovery-point objectives” (how much data loss is acceptable) and “recovery-time objectives” (how much system downtime is acceptable).

SEE THE BIG PICTURE

To conclude the assessment process, we provide you with a security maturity level associated with your OT network and health report that highlights possible risk and provides recommendations on potential solutions that may enhance the Cybersecurity of your OT environment.

HONEYWELL OFFERS TWO TYPES OF CYBERSECURITY ASSESSMENTS ESSENTIAL AND ENHANCED

ESSENTIAL

METHODOLOGY

COMPREHENSIVE	
PROCESS	Industry Standard Approach
PEOPLE	Trained ICT/Cybersecurity specialists to conduct the assessment and have industry specific knowledge
CLIENT PROFILE	Low-Medium Cybersecurity maturity level
RISK ASSESSMENT	**NIST 800-30** • Threat Identification • Vulnerability Identification • Control Recommendations Results Documentation
COMPLIANCE FRAMEWORK	• NIST-CSF 1.1
VULNERABILITY ASSESSMENT	• Automated Software Verification • Manual Software Verification • Check patch management and missing levels • Verify configuration to assess security • Review for hardening
CRITICAL CONTROLS VERIFICATION	• Standard Critical Controls
ANALYSIS DEPTH	Identifies Core cybersecurity gaps

CUSTOMER TYPE

VERTICALS	Commercial Buildings Education Hospitality Residential (Hi-Rise) Buildings Retail
BUILDING COMPLEXITY	Small-Medium
INFRASTRUCTURE READINESS	Based on Infrastructure Less than 60 nodes
EXAMPLES	**Typical Site Layout:** **A Hotel in a Large City Site** **1** Buildings **5** Applications **20** Servers **2** Control Rooms **15** Workstations

DELIVERABLES

- Detailed Report
- In-depth Analysis
- Briefing and Presentation on Findings

ENHANCED

METHODOLOGY

COMPREHENSIVE

PROCESS
Customized Approach to help meet Industry standards and customer needs

PEOPLE
Highly experienced and knowledgeable senior cybersecurity specialists trained on critical infrastructure to conduct the assessment

CLIENT PROFILE
High Cybersecurity maturity level

RISK ASSESSMENT

NIST 800-30

- Threat Identification
- System Characterization
- Vulnerability Identification
- Control Analysis
- Control Recommendations Results Documentation

COMPLIANCE FRAMEWORK

- NIST CSF 1.1
- ISO 27001/27002
- ISA/IEC 62443
- NIST800-53r5
- NIST800-82

VULNERABILITY ASSESSMENT

- Automated Software Verification
- Manual Software Verification
- Check patch management and missing levels
- Verify configuration to assess security
- Review for hardening
- Active/Automated scans for non-critical systems
- Passive/Manual scan for critical systems

CRITICAL CONTROLS VERIFICATION

- Standard Critical Controls
- Center for Internet Security (CIS) Controls

ANALYSIS DEPTH
Identifies Advanced cybersecurity gaps

You know your facility.
Enhance your Security with Honeywell.

buildings.honeywell.com

CUSTOMER TYPE

VERTICALS

Critical Facilities

- Airports
- Banking/Financial Services
- Data Centers
- Government
- Healthcare
- Pharmaceuticals

BUILDING COMPLEXITY
High

INFRASTRUCTURE READINESS
Complex based on the type of facility and also based on the infrastructure.
Greater than 60 nodes

EXAMPLES

Typical Site Layout: International Airport

30 Buildings	**4** Data Centers
50 Applications	**40** Servers
5 Control Rooms	**30** Workstations

DELIVERABLES

- Detailed Report
- In-depth Analysis and customized recommendation
- Briefing and Presentation on Findings
- Workshop conducted by cybersecurity engineers
- Roadmap of Mitigation
- Post engagement consultation

THE FUTURE IS WHAT WE MAKE IT

Honeywell Building Solutions
1985 Douglas, Drive North
Golden Valley, MN 55422-3992
Tel: 1-800-345-6770
www.Honeywell.com