Guardian™ Cybersecurity – Assessment Services

OT-focused cybersecurity assessment and consulting services from Emerson

- Identify cybersecurity gaps across your operational technology (OT) environment, including Guardian™ software, the DeltaV™ Automation Platform, AMS™ solutions, and other non-Emerson process control systems
- Align with Guardian™ Cybersecurity best practices and recognized industry standards
- Receive qualitative reports to support the planning and execution of priority cybersecurity solutions



Guardian™ Cybersecurity – Assessment Services are an integral part of Emerson's three-step approach to implementing and managing effective cybersecurity best practices.

Introduction

Effective cybersecurity solutions are not "set once and forget." Constantly evolving threats are launched at control systems from every direction. Understanding how to deploy a best-practice cybersecurity program cost-effectively can be a daunting task without specialized knowledge.

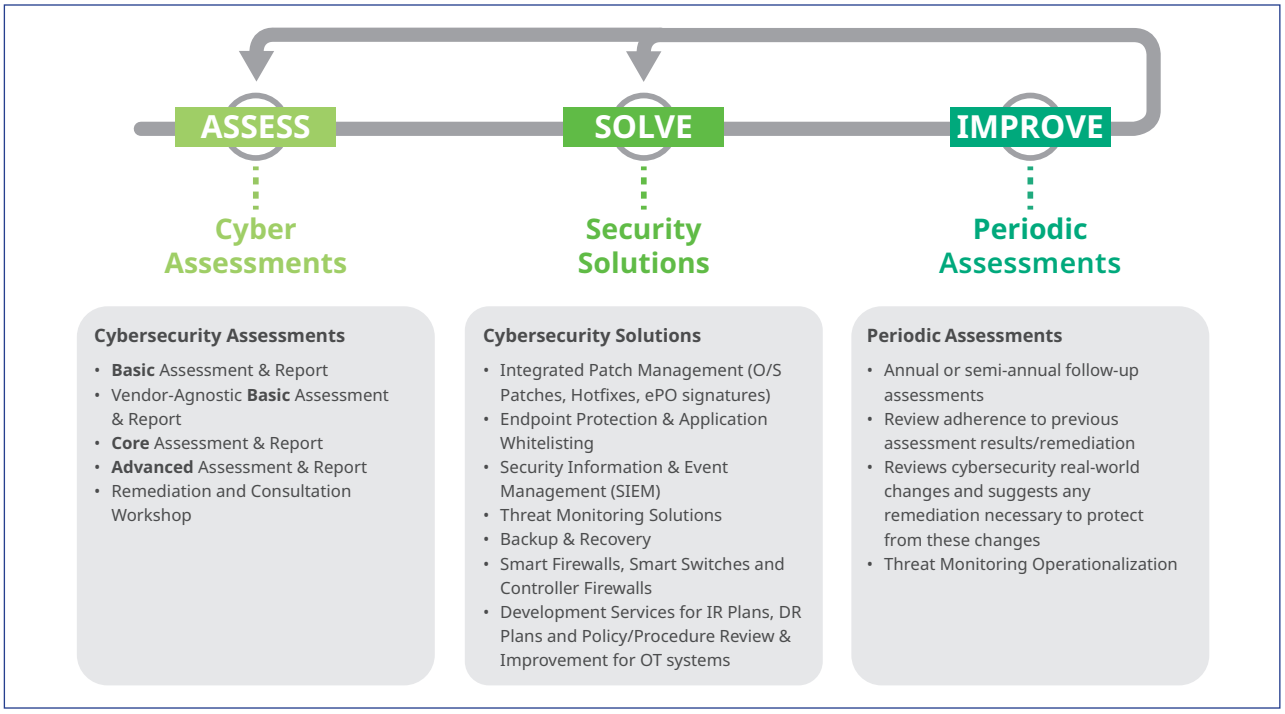
Guardian™ Cybersecurity – Assessment Services provides expert, OT-focused consultation to help organizations evaluate, prioritize, and improve their cybersecurity posture across OT environments, including Guardian™ software, the DeltaV™ Automation Platform, AMS™ solutions, and other non-Emerson process control systems.

Assessment Services offers three service levels along with a Remediation and Consultation Workshop. You can choose from an initial system cybersecurity review to a detailed analysis of specific cybersecurity dimensions, or support for applying solutions to existing cybersecurity gaps.

Benefits

Identify, prioritize, and reduce cybersecurity risk across your OT environment: A successful breach or attack can cause serious damage to your plant and reduce or shut down production. The assessment produces a report that helps you to better understand how secure your system is relative to best practices and provide guidance on how to make improvements.

Align with Guardian™ Cybersecurity best practices and standards: Unaddressed OT system hardening efforts, lack of effective user access policies and/or procedures, incomplete or deferred software antivirus and security updates, and inadequate cybersecurity training for personnel are all preventable cybersecurity vulnerabilities that have an impact on system performance.



Guardian™ Cybersecurity applies a structured, three-step approach (above)–Assess, Solve, Improve–to help industrial organizations systematically strengthen their cybersecurity posture across people, processes, and technology.

Securely receive qualitative reports for the planning and execution of cybersecurity remediation solutions: The most basic cybersecurity assessment will form the foundation for assessing and remediating cybersecurity vulnerabilities within your process control system. When considering the business value of the Assessment Service, the benefit of evaluating and remediating vulnerabilities that could lead to a cybersecurity breach — versus the downtime costs associated with the discovery and removal of the breach — is realized in several key areas:

- **Cost of Lost Revenue** — Value of the total revenue lost during the cyber incident evaluation and repair period.
- **Direct Cost to Return to Operation** — Cost of unscheduled downtime, material, labor, overtime, off-spec product and the start-up time required to begin operation.

A site-specific cybersecurity consultative workshop can often immediately pinpoint gaps in the cybersecurity protection deployed: Focused cybersecurity discussions specific to your process control system often reveal important missing cyber-protection coverage that, when corrected, can help prevent system downtime due to missing cyber solutions.

Additionally, in this one-on-one consultative environment, discussions can reveal that even though countermeasures have been deployed, the final deployment may have missed key component configurations and is still creating cyber-gaps in your protection scheme.

Assessment Services

The following Guardian™ Cybersecurity Assessment Services are available from Emerson:

- Basic Cybersecurity Assessment
- Core Cybersecurity Assessment
- Advanced Cybersecurity Assessment
- Remediation and Consultation Workshop

Basic Cybersecurity Assessment Service

The effort to determine what is required to proactively prevent an attack most logically starts with a basic cybersecurity assessment at your site from your local Emerson-certified service representative. This assessment will provide high-level insight into the present security posture of your OT environment. As site-specific needs affect the network architecture, Emerson uses local service representatives to conduct the initial assessment in conjunction with site personnel.

Your local service representative will lead you through a series of questions and discussions to determine the current state of cybersecurity readiness for your OT system. **These questions are aligned with IEC 62443 requirements and are grouped into six major categories:**

- User Account Management
- Patching and Security Management
- Physical Security and Perimeter Protection Management
- Security Monitoring and Risk Assessment
- Data Management
- Network Security

Basic Assessment covers a wide range of OT cybersecurity dimensions, including:

- Review of the network segmentation
- Review of existing OT cybersecurity policies and procedures in place
- Review of existing OT portable device policies (USB sticks, Portable CDs, etc.)
- Review of the level of workstation and server hardening efforts currently in place (USB ports, personnel access policies, etc.)
- Review of user access policies and procedures, including passwords and unused accounts
- Determination of O/S security update policies, procedures, training, and enforcement
- Review of current patch management practices and procedures
- Review of network physical security and perimeter protection best practices
- Review of data backup plans and data management procedures

The assessment data gathering/questionnaire process can typically be completed within one day. Once data gathering is complete, an assessment report is generated and the findings are reviewed with your site personnel.

Since knowledge transfer is critical on this subject matter, Emerson works in collaboration with your site personnel and local Emerson service resources to determine the best overall deployment of cybersecurity improvements specific to your current deployment situation.

Vendor-Agnostic Basic Assessment

A Vendor-Agnostic Basic Assessment and Report can be created at the customer's request. The Basic Assessment is based on recognized security guidelines and standards that apply to most industrial control systems, field devices, safety and protection systems, and industrial networks and controllers on the market, and it provides no system-specific guidance.

Core Cybersecurity Assessment

The core assessment will provide deep-level insights into your OT cybersecurity posture. This assessment is generally an on-site activity involving detailed data gathering and assessment. It is fully customizable, allowing you to use your already completed Basic Cybersecurity Assessment results as a guide to dig deeper into specific areas, select your own predetermined needs for assessing, or enable our experts to perform a comprehensive and thorough cybersecurity assessment.

Once the required assessment services are agreed upon, a pre-site conference call, followed by an on-site visit, is required to fully explore all aspects of the selected assessment areas.

Upon completion of the Core Cybersecurity Assessment, you will receive a report covering the findings and possible remediation.

Commonly explored elements of this assessment option include:

- Review of the OT network segmentation
- Review of existing cybersecurity policies and procedures in place
- Review of existing portable device policies (USB sticks, Portable CDs, etc.)
- Review of the level of workstation and server hardening efforts currently in place (USB ports, personnel access policies, etc.)
- Review of user access policies and procedures, including passwords and unused accounts
- Determination of O/S security update policies, procedures, training, and enforcement
- Review of current patch management practices and procedures
- Review of network physical security and perimeter protection best practices
- Review of data backup plans and data management procedures

Advanced Cybersecurity Assessment

The Advanced Cybersecurity Assessment provides even deeper insight into your OT cybersecurity posture. This assessment is generally an on-site activity, involving detailed data gathering elements allowing for a more specific analytic assessment of your cybersecurity protection schemes. These assessments are fully customizable, allowing you to use your already completed Basic Assessment results as a guide to dig deeper into specific areas. We allow you to select your own predetermined needs for assessing or enable our experts to perform a comprehensive and thorough cybersecurity assessment.

The Advanced Assessment adds a series of additional options that are even more dynamic than those included in the Basic Assessment.

Advanced Assessment covers an additional range of OT cybersecurity dimensions, including:

- Deeper network security analysis
  - Network equipment analysis
  - Protocol analysis
  - Advanced network diagnostics
- Workstation hardening review
- Risk scoring based on customer requests, best practices or published industry standards
- Extended data management review
  - Identify critical data/systems
  - Disaster recovery planning review
  - Cybersecurity incident response planning review
- Active Directory trust review

Remediation and Consultation Workshop

If you have already determined what is needed to improve your cybersecurity protection for your OT environment but require Emerson assistance in the remediation process, the Remediation and Consultation Workshop is available to support your remediation efforts. This consultative service can provide insight and remediation help where determinations on direction and next steps have already been made locally.

Guardian™ Cybersecurity experts will provide additional insight into cybersecurity improvements on your OT systems and will be dispatched to your site to work directly with you to improve your cybersecurity protection coverage. This workshop service is available either on-site or via online conferencing services.

Ordering Information

Description	Model Number
Basic Cybersecurity Assessment	Please Contact Your Local Emerson Sales Office
Core Cybersecurity Assessment	
Advanced Cybersecurity Assessment	
Remediation and Consultation Workshop	

This product and/or service is expected to provide an additional layer of protection to your control system to help avoid certain types of undesired actions. This product and/or service represents only one portion of an overall DeltaV system security solution. Emerson does not warrant that the product and/or service or the use of the product and/or service protects the DeltaV system from cyber-attacks, intrusion attempts, unauthorized access, or other malicious activity ("Cyber Attacks"). Emerson shall not be liable for damages, non- performance, or delay caused by Cyber Attack. Users are solely and completely responsible for their control system security, practices and processes, and for the proper configuration and use of the security products.

To learn how comprehensive Cybersecurity Assessment Services address your cybersecurity needs, contact your local Emerson sales office or representative, or visit **www.emerson.com/cybersecurity.**

©2026, Emerson. All rights reserved.

The Emerson logo is a trademark and service mark of Emerson Electric Co. The Guardian logo is a mark of one of the Emerson family of companies. All other marks are the property of their respective owners.

The contents of this publication are presented for informational purposes only, and while diligent efforts were made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the designs or specifications of our products at any time without notice.

Contact Us
www.emerson.com/contactus

GUARDIAN™

EMERSON™