DeltaV™ Cybersecurity Assessment Services

- Identify, remediate, and secure your DeltaV distributed control system from cybersecurity risks
- Align with Emerson's cybersecurity best practices and standards
- Receive qualitative reports for the planning and execution of cybersecurity remediation solutions

Emerson's DeltaV™ Cybersecurity Assessment Services are an integral part of Emerson's three-step approach to effective cybersecurity best practice implementation and management.

Introduction

Effective cybersecurity solutions are not a "set once and forget" solution. Constantly evolving threats are launched at control systems from every direction. Understanding how to deploy a best practice cybersecurity program in a cost- effective manner can be a daunting task without specialized knowledge. Emerson's Cybersecurity Assessment Services for DeltaV™ distributed control systems (DCS) provide expert consultation for cybersecurity hardening of a DeltaV DCS.

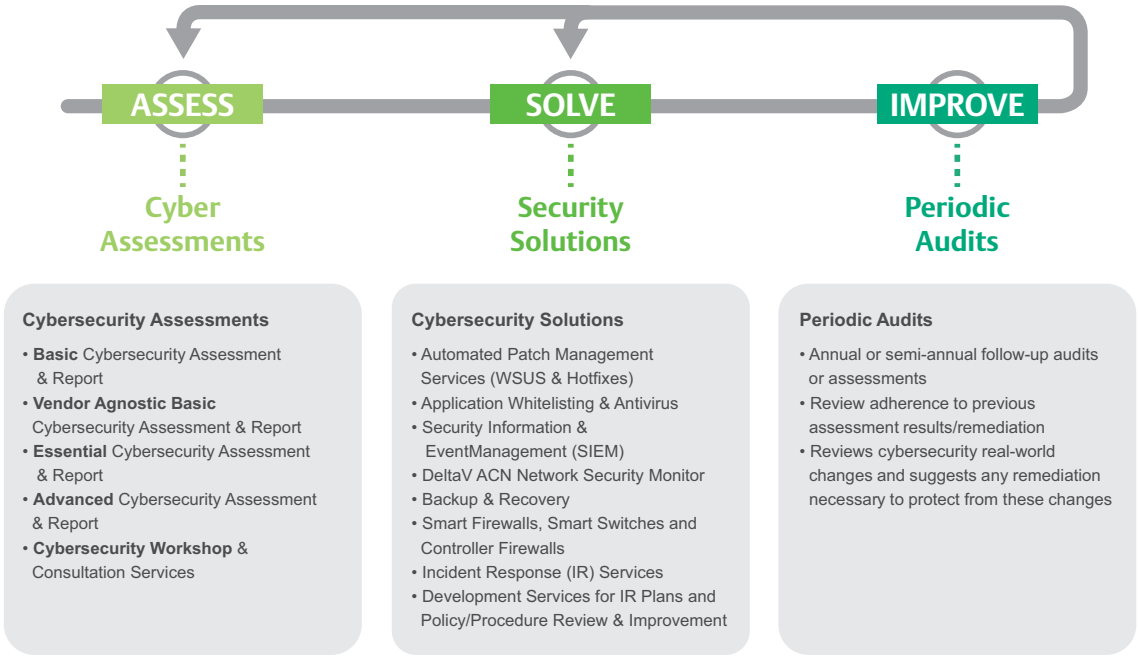
There are several versions of assessment solutions, allowing you to select an appropriate level of service, whether it is an initial look at system cybersecurity, a deep analysis at one or more specific areas, or implementing solutions for already identified risk issues.

Benefits

Identify, remediate, and secure your DeltaV DCS from cybersecurity risks: The consequences of a successful breach/attack can cause serious damage to your plant, reduce or shut down production, and even have safety and environmental implications. The results of an assessment will produce a report allowing you to better understand how secure your system is relative to best practices and provide guidance on how to make improvements.

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

EMERSON



Emerson uses a three-step process (above) for cybersecurity prevention to harden DeltaV system features, products (hardware/software), and services.

Receive qualitative reports for the planning and execution of cybersecurity remediation solutions: The most basic cybersecurity assessment will form the foundation to assess and remediate cybersecurity vulnerabilities within your process control system. When considering the business value of the Cybersecurity 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— are 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 down-time, 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 counter measures have been deployed, that final deployment may have missed key configuration of components and are still providing cyber-gaps in your protection scheme.

Services

The following assessment services are available from Emerson:

- Basic Cybersecurity Assessment Service
- Essential Cybersecurity Assessment Service
- Advanced Cybersecurity Assessment Service
- Cybersecurity Remediation and Consultation Service

Each service is individually described in the following sections and most are available for both DeltaV and non-DeltaV process control systems.

Basic Cybersecurity Assessment Service

The effort to determine what is required to proactively prevent an attack most logically starts with a Basic Cybersecurity Asse ssmentatyoursitefromyourlocalEmerson-certified DeltaV DCS service representative. The Basic Cybersecurity Assessment Service will provide high level insight into the present security posture of your DeltaV DCS, as well as identify areas in need of improvement. As site specific needs affect the network architecture, Emerson utilizes local DeltaV DCS service representatives to perform the basic assessment in conjunction with site personnel.

Your local service representative will lead you through a series of questions/discussions aimed at determining the current state of cybersecurity readiness for your DeltaV DCS. These questions are generally grouped into seven major categories:

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

Emerson's initial Basic Cybersecurity Assessment Service covers a wide range of cybersecurity related issues including:

- Review of the DeltaV DCS network segmentation
- Review of existing cybersecurity policies and procedure in place
- Review of existing portable device policies (USB sticks, Portable CDs, etc.)
- Review of 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 the data gathering has been completed, 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 a 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 Cybersecurity Assessment

The Vendor Agnostic Basic Cybersecurity Assessment and Report was created in response to direct customer requests. After the presentation of a Basic Cybersecurity Assessment, customers desired the same assessment to be done on other control systems at their site. Regardless if Emerson is asked to deploy remediations on other control systems, Emerson can certainly assess the current cybersecurity solution on a competitive system. This demonstrates Emerson's understanding of cybersecurity principles, regardless of the system deployed.

Currently, Emerson is determining what components are necessary to support vendor agnostic services for customers, with respect to contracts, to handle the cybersecurity of all control systems at a site – a growing request from customers. These services would allow Emerson Performance Services (or possibly local service organizations) to provide the site guidance for cybersecurity monitoring and/or improvements to DeltaV and other control systems. An update to these services is a work in process.

Essential Cybersecurity Assessment Service

The Essential Cybersecurity Assessment Service will provide deeper-level insight into your DeltaV DCS cybersecurity posture. This assessment is generally an onsite 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 pre-determined needs for assessing, or enable our experts to perform a comprehensive and thorough cybersecurity assessment. Emerson's Performance Services can deliver exactly what you need.

Once the required assessment services are agreed upon, a pre-site conference call, followed by an onsite visit, is required to fully explore all aspects of the selected assessment areas. Commonly explored elements of this assessment option include:

- Review of the DeltaV DCS network segmentation
- Review of existing cybersecurity policies and procedure in place
- Review of existing portable device policies (USB sticks, Portable CDs, etc.)
- Review of 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

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

Advanced Cybersecurity Assessment Service

Any Advanced Cybersecurity Assessment will provide an even deeper-level insight into your DeltaV DCS 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 Cybersecurity Assessment results as a guide to dig deeper into specific areas. We allow you to select your own pre-determined needs for assessing or enable our experts to perform a comprehensive and thorough cybersecurity assessment.

The Advanced Cybersecurity Assessment adds a series of additional options that are even more dynamic that those included in the Essential Cybersecurity Assessment that would include (but not limited to):

- Deeper Network Security Analysis
  - Network Equipment Analysis
  - Protocol Analysis
  - Advanced Network Diagnostics
- Workstation Hardening Review
- Risk scoring based off of customer requested Best
- Practice 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

Cybersecurity Consultative Workshop Service

If you have already determined what is needed to improve your cybersecurity protection for your DeltaV DCS but require Emerson assistance in the remediation process, the Cybersecurity Remediation and Consultation Workshop Service 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.

Cybersecurity experts will provide additional insight into cybersecurity improvements on your DeltaV systems and are 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 on-line conferencing services.

Ordering Information

Description	Model Number
Basic Cybersecurity Assessment Service	Please Contact Your Local Emerson Sales Office
Essential Cybersecurity Assessment Service	
Advanced Cybersecurity Assessment Service	
Cybersecurity Consultative Workshop Service	

This product and/or service is expected to provide an additional layer of protection to your DeltaV 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**.

Contact Us
www.emerson.com/contactus

EMERSON