Cybersecurity Management Services

- Utilize a combination of people, technology and cybersecurity best practices designed to ensure the availability of your DeltaV system
- Help assess the current cybersecurity posture of your DeltaV system
- Remediate protection gaps to improve the overall cybersecurity protection of your DeltaV system

Introduction

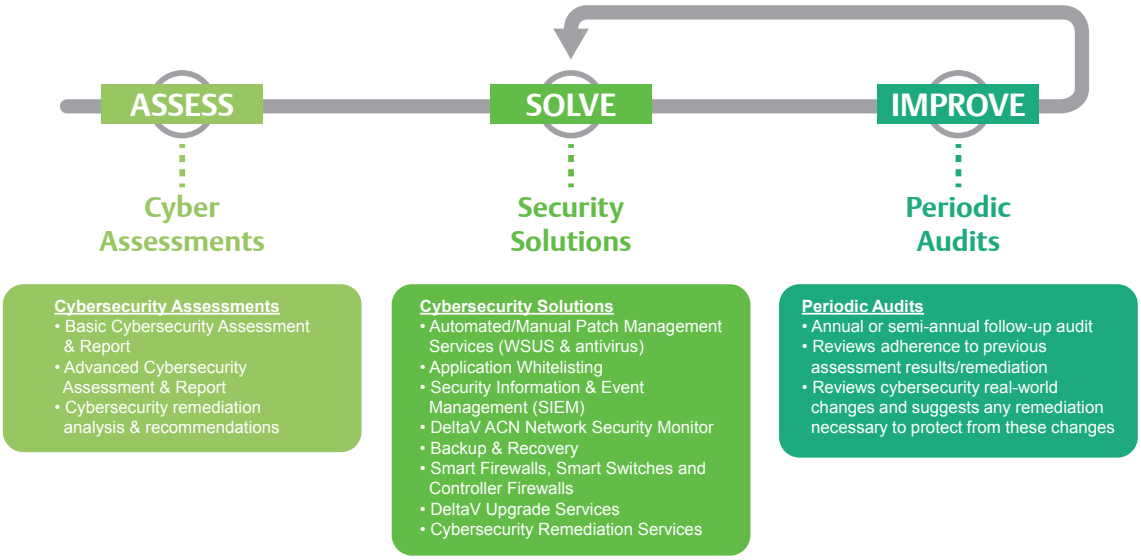
Emerson's Cybersecurity Management Services applies to Emerson DeltaV™ DCS and provides expert consultation and assistance with evaluation, testing, and implementation support for cybersecurity enrichment of process controls systems. Cybersecurity Management Service is another way Emerson Process Management is demonstrating our commitment to being the first-choice, best-value solution provider to our clients. Because every customer has their own network architecture, Emerson can provide cybersecurity consulting in a collaborative framework to determine the best overall deployment of cybersecurity products and services for that customer's specific needs and operating practices.

Benefits

Utilize a combination of people, technology and cybersecurity best practices designed to ensure the availability of your DeltaV system: Emerson's global network of cybersecurity experts can be leveraged to reduce your local workload. Our embedded DeltaV security features and other plug-and-play security products can provide additional layers of protection. And our evergreen DeltaV security best practices, aligned with global defense-in-depth standards, can be applied to your DeltaV System.

Help assess the current cybersecurity posture of your DeltaV system: A comprehensive cybersecurity assessment can often uncover security gaps in an existing process control system that, when remediated, can result in the avoidance of a cybersecurity attack or breech. Identification of potential exploit corridors or malware injection points prior to any infection will pay dividends versus the damage and clean-up needed to get a system back on-line post-infection.

EMERSON



Remediate protection gaps to improve the overall cybersecurity protection of your DeltaV system: Installation of preventative measures along with continued auditing of the system and associated policies and procedures will ensure that the investments made in cybersecurity protection solutions is maintained at its highest levels. Avoidance of a cybersecurity breech is paramount and the peace of mind knowing that utilizing the latest "best practice cybersecurity concepts" provides your system with the best chance of avoiding a cyber-attack.

Cybersecurity Management Solutions

Cybersecurity Consultation and Assessments are an integral part of Emerson's Cybersecurity Management Solutions portfolio. A comprehensive cybersecurity solution can consist of many different components; each one specific to reducing risks associated with various process control system entities. Cybersecurity Management is an integrated approach to finding the best cyber solutions to fit both your current process control system and existing plant security policies and procedures.

As indicated in the flowchart illustration above, Cybersecurity Management Services can utilize both services and products in the assessment of vulnerabilities on the control system as well as the application of services and products used in the cybersecurity protection of those systems. It is a three step process:

- **Assess** - On-site consultation and/or a comprehensive base-line vulnerability assessment.
- **Solve** - The application of security products and/or other remediation services.
- **Improve** - Finally, in order to protect the customer investment and keep current with changes in the cyber-attack scenarios, continuous auditing will maintain the high standards installed and prompt customers to make changes to protect the system from new threats.

Cybersecurity Management solutions cover:

- Alarm Maintenance & Operation
- Application Whitelisting
- Automated and Local Manual Patch Management
- Basic and Advanced Cybersecurity Assessments

- Cybersecurity Consultation Services
- Disaster Recovery / Backup & Recovery
- Network Security Monitor
- On-site Spare Parts Management
- Security Information & Event Management (SIEM)
- Smart Firewalls
- Smart Switches and Controller Firewalls
- System Health Monitoring

Reduction of risks associated with the use of these solution components reduces the time spent on controllable issues and allows focus on other important day-to-day issues.

Cybersecurity Service Architecture

The following bullets provide a general description for each of the above steps.

- **Cybersecurity Consultation and/or Vulnerability Assessment Services (Assess)**
  - **Basic Cybersecurity Assessment and Report:** An interview-based vulnerability assessment and report intended to provide an initial high-level, first-pass cyber assessment of a given site or system. The results of this assessment exercise would be to provide insight to general remediation opportunities and provide direction into which particular cybersecurity segment(s) needs immediate attention. This report can also be used to determine which sectors require a more thorough review and remediation first.
  - **Advanced Cybersecurity Vulnerability Assessment and Report:** Complete comprehensive baseline DeltaV cybersecurity vulnerability assessment and report to identify control system security vulnerabilities and recommend mitigating actions to help achieve the site's control system cyber security integrity requirements. This service element includes pre-assessment expert cybersecurity consultation service, either on-site or via conference call, reviewing existing policies/procedures, control system drawings, best practices and network architecture review. Then, an on-site visit is required to fully explore all aspects of the current installed cybersecurity processes, policies, procedures and enforcement activities.
  - **Cybersecurity Remediation Analysis and Consultation Service:** These consultative services can provide insight and remediation help where determinations on direction and next steps have already been determined locally. These experts can provide additional insight into cybersecurity improvements on DeltaV DCS.
- **Security Solutions Portfolio (Solve)**
  - Post assessment findings will utilize selections from the Security Solutions Portfolio to remediate findings:
    - Application Whitelisting
    - Backup & Recovery / Disaster Recovery
    - Controller Firewalls
    - DeltaV Upgrade Service
    - Guardian Support
    - Manual/Automated Patch Management
    - Network Security Monitor
    - Remediation Services
    - Security Information & Event Management (SIEM)
    - Smart Firewalls
    - Smart Switches
    - System Heath Monitoring (SHM)
- **Cybersecurity Follow-up Assessment Services (Improve)**
  - Annual, semi-annual or quarterly cybersecurity audits that help to preserve the customer's installed cybersecurity best practices and standards investment and keep current with emerging cyber-attack strategies.
  - Reviews adherence to previous assessment results/remediation.
  - Reviews cyber security real-world changes and suggests any remediation necessary to protect from these changes.

Ordering Information

Description	Model Number
Basic Cybersecurity Assessment Service	Please Contact Your Local Emerson Sales Office
Advanced Cybersecurity Assessment Service	Please Contact Your Local Emerson Sales Office
Cybersecurity Follow-up Assessment Service	Please Contact Your Local Emerson Sales Office
Expert Cybersecurity Consultation Services	Please Contact Your Local Emerson Sales Office

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 Management Services address your cybersecurity needs, contact your local Emerson sales office or representative, or visit **www.emerson.com/cybersecurity**.

Emerson
North America, Latin America:
+1 800 833 8314 or
+1 512 832 3774

Asia Pacific:
65 6777 8211

Europe, Middle East:
+41 41 768 6111

www.emerson.com/cybersecurity

EMERSON