Cyber Asset Protection Subscription for Power Generation

Overview

In a complex world of ever-changing technologies, GE realizes the importance of having an experienced partner to guide successful cyber security implementation. As a global leader of industrial controls, GE is well-equipped to help customers improve their security posture and support compliance efforts. Our products are built with security in mind and are easily integrated into broader plant-level systems and IT architectures.

GE's Cyber Asset Protection Subscription solution is a key part of a defense-in-depth system for turbine, plant, and generator controls environments. The subscription service includes operating system and application patches as well as anti-virus/intrusion detection signatures to cover updates for HMIs, servers, switches, and network intrusion detection devices. Monthly updates can be applied to individual HMIs or via the SecurityST* appliance for network-wide deployment.

The Cyber Asset Protection Subscription is part of GE's SecurityST Mark* VIe Solution and Commissioning Services, which is Achilles® Practice Certified – Bronze, indicating the solution has undergone strict cyber security best practices demonstrating to customers that systems are developed and implemented with security in mind. Cyber Asset Protection Subscription is designed to support the plant operation's compliance to cyber security standards and guidelines including NERC CIP, NEI 08-09 and IEC 62443-2-4.

Why patching is critical

Patching your systems is one of the best things you can do to protect your assets and assure the operating systems and programs running have updates to provide the latest security protection without risking your operation. Listed as two of the "First Five Quick Wins" by The SANS Institute, a well-respected authority on information security and cyber security training, patching of application and system software is critical to improving and maintaining a high security posture.

How it works

The Cyber Asset Protection subscription provides monthly updates for your HMI, Historians, switches, firewalls, OSM and RSG. Software updates include:

- Windows® Operating System
- GE Cimplicity (ICS-CERT-specific)
- Intrusion Detection signatures
- Anti-virus signatures
- Switch updates
- System 1*

The subscription service also provides a monthly report of patches that need to be installed and the areas of which are critical for attention.

Benefits

- Provides tested updates to keep your legacy critical infrastructure running
- Reduces downtime by providing validated patches which are tested in an environment to assure applicability and compatibility
- Keeps your risk profile updated and increases your security posture by protecting your critical assets from known vulnerabilities on a monthly basis
- Helps you meet regulatory requirements and avoid fines
- Improves safety and reliability by preventing loss of view
- Provides a dedicated service manager for cyber issues

The importance of validation

With validated patch management, the updates are validated in a lab that mimics the plant environment in order to identify any incompatibilities that may exist before the patch is applied. This allows operators to determine what alterations need to be made to ensure uptime and protection against cyber threats without having to create simulators themselves. Our testing is done in a secure lab environment using both physical hardware and software, which is the best method to guarantee industrial controls receive tailored patches and an applicability report on a monthly basis.

A trusted partner for compliance

As a vendor of industrial controls, GE embraces its responsibilities to assist critical infrastructure owners as they improve their security postures and support compliance efforts related to GE-provided equipment throughout the 10 to 20 year lifecycle of the control system itself. Together with Wurldtech Security Technologies, GE is able to offer security support that spans from initial system design to commissioning, all the way through ongoing support and maintenance.

NERC CIP Rev 5

Many U.S. electric utilities are now federally mandated to comply with NERC CIP requirements that dictate industrial security and remediation technology, including required compliance, by April 2016/2017. To be considered in adapting operations to these regulations is the difficulty of patching industrial controls and the frequent attacks on the equipment. In addition, customers need to address known ICS vulnerabilities without disrupting operations. Because of these factors, electric utilities require a solution that is easy to implement and provides visibility into the industrial network and compliance.

NEI 08-09

US Nuclear Power companies are federally mandated to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. As part of having a cyber plan, operators are required to address known ICS vulnerabilities and have solutions in place for operating system, application and third-party software updates, Host Intrusion Detection, and non-repudiation, among others.

IEC 62443-2-4

IEC 62443-2-4 is a published international standard, defining cyber security capabilities that Industrial Automation and Control System (IACS) service providers may implement and offer. The standard can help asset owners consistently procure and manage control systems security expertise. IEC 62443-2-4 was developed by IEC Technical Committee 65, in collaboration with the International Instrumentation Users Association (previously WIB) and ISA 99 committee members. GE hardens customer systems using a combination of technical and procedural measures that have been certified to meet IEC 62443-2-4 security standards. These standards specify a comprehensive set of security requirements for the installation and maintenance of IACS.

To read more about our capabilities on these three standards and regulations, visit our website, www.gemeasurement.com/machinery-control.

For more information please contact:
GE Oil & Gas
North America: 1-888-943-2272; 1-540-387-8726
Latin America (Brazil): +55-11-3958-0098
Europe (France): +33-2-72-249901
Asia/China (Singapore): +65-6622 1623
Africa/India/Middle East (U.A.E.): +971-2-699 7119

Email: ControlsConnect@ge.com
Customer Portal: ge-controlsconnect.com

1800 Nelson Road
Longmont, CO, USA 80501
https://www.gemeasurement.com

For further assistance or technical information, contact the nearest GE Sales or Service Office, or an authorized GE Sales Representative.

GEA30382D (06/2016)