GE VERNOVA

FACTSHEET

GE Vernova's Cybersecurity Platform - OTArmor

PROFESSIONAL SERVICES

OVERVIEW

Organizations greatly benefit by starting with a benchmarking exercise to understand the current state of security readiness. **GE Vernova offers a control system agnostic cybersecurity risk assessment service** to support compliance with industry standards such as **ISA99/IEC 62443, NEI 08-09, NIST SP800-161, NIS-D** and **NERC-CIP** and will help elevate your cybersecurity awareness and identify potential vulnerabilities. After the assessment is conducted, the final report provided **enables the creation of an actionable road map of prioritized mitigations to improve your security posture.**

CYBERSECURITY ASSESSMENTS

GE Vernova's cybersecurity validation platform offers a large variety of security assessment services. Designed for the CEO, CISO, Plant Manager, or Compliance Manager to prioritize steps for mitigation and even to help obtain future budgets within a multi-year cybersecurity program.

- Useful for obtaining budget and prioritizing cybersecurity road map
- Understand current state of security readiness
- Compare your results versus industry expectations
- Identify weakness early to prevent exploitation
- Deliver prioritized, actionable mitigation steps tailored to your environment

TYPES OF ASSESSMENTS OFFERED:

- Vulnerability and risk assessment
- Asset inventory assessment
- Compliance framework assessment (IEC 62443, NERC, NEI, ISO27001, NIST, NIS-D)
- CIS top 18 controls
- Highly complex risk assessments or penetration tests
- Product security assessment (IIoT, controller, etc.)
- Network architecture assessment
- Threat assessment
- Assessment against customer specific framework

FEATURES OF CYBERSECURITY ASSESSMENT

Below is a list of some of the important items that are reviewed during the assessment:

- **Control system application:** Control system or PLC configuration review, network security configuration, control system integration methodologies, and technical support agreement status
- **HMI server hardware configuration:** Hardware warranty status, health, environmental conditions, and physical security
- **HMI operating system configuration:** Access control, account and password review, anti-virus configuration, patch management, logging, backup and recovery, server performance and

resource snapshot, installed applications, TCP/IP network integration and architecture, performance, availability, and health monitoring

- **Control system protection:** Password strength, control system integration methodology, TCP/IP network integration architecture, environmental conditions, and physical security
- **TCP/IP network infrastructure review:** Review firewall, router, and switch configuration, firmware updates, and management process, access control and authorization, system performance and availability management, physical security, and environmental conditions
- **Process review:** Change management, IT incident management, patch management, system access authorization, and implementation, lost/forgotten password, key management, and governance documentation

EXPERT SERVICES THAT STRENGTHEN SECURITY AND RESILIENCE

Hardware Maintenance Services

Your Challenges
Investing in routine HMI hardware maintenance is wise. It can help prevent issues and extend your systems' usability. However, with lean internal teams, it can be difficult to find staff with the time and expertise needed to perform this maintenance, and to ensure that they carry out this work on an ongoing, consistent basis.

Our Solution
On a one-time or recurring basis, we can provide comprehensive HMI maintenance. As part of our services, we handle a range of efforts:

- Thorough system internal component cleaning to remove any contaminants
- Complete system diagnostics and remediation of any detected issues
- Disk defragmentation to improve system performance
- System component inspection—including cooling fans, power supplies, keyboards, air filters, and more.
- Replacement of any faulty components, as needed

Business Challenges

- Once a day, the energy sector faces a cyber attack that hasn't been seen before.[1]
- 46% of all cyber attacks in the OT environment go undetected.[2]
- $4.45MM: Average total cost of a data breach.[3]

On-site Patch Deployment Services

Your Challenges
Cyber attacks are a constant threat for today's power generation plants. At any time, attackers may try to exploit software vulnerabilities to gain system access and achieve nefarious objectives. It is therefore critical to address vulnerabilities that rogue actors can exploit. This includes installing security patches.

For many power generation plants, staffs struggle to keep pace with daily demands, leaving precious little time to handle these critical, yet time-consuming patching efforts. Furthermore, these efforts not only take a lot of time, but they also require a lot of expertise. To manage patching effectively, staff need current security expertise on evolving threats and vulnerabilities. They also must know how to implement patches safely and efficiently, without jeopardizing functionality and ongoing operations. Given these requirements, critical patching efforts continue to be relegated to the back burner, meaning the open vulnerabilities backlog continues to grow.

Our Solution
GE Vernova's team can deliver complete, end-to-end patching services—including comprehensive project management. We will work with your on-site staff and resources to establish an HMI patching sequencing plan. As part of this plan, we'll develop a detailed schedule for modifications and sequencing; so that we can promote speed and efficiency, while avoiding any potential disruptions. Our team will identify which HMIs can be modified in parallel and those that must be worked on in isolation. We'll make sure that, while one HMI is modified, other resources will be in place so that critical plant operations continue to function.

In building the schedule, we'll account for dependencies. For example, we'll factor in timeframes needed to gain permissions required to work on different HMIs, so we can reduce the time spent waiting for resources to become available. Our team will also identify the personnel needed to assist us—for example, engineers who must give us system access or validate functionality. We'll then align plans and schedules with resource availability. Throughout the project, GE Vernova's team will review progress with site personnel, and make plan modifications if needed.

Sources

[1] S&P Global, "Feature: Energy industry faces unprecedented cyber threats almost daily," July 19, 2018, www.spglobal.com/platts/en/market-insights/latest-news/electric-power/071918-feature-energy-industry-faces-unprecedented-cyber-threats-almost-daily.

[2] Ponemon Institute LLC, "The State of Cybersecurity in the Oil & Gas Industry: United States," February 2017, www.crc-ics.net/documents/CRC-ICS-2017_Pokemon%20Report-Cyber_Readiness_US_Oil Gas_2017.pdf.

[3] Ponemon Institute, sponsored by IBM Security, "2019 Cost of a Data Breach Report," July 2019, www.ibm.com/security/data-breach.

Following is an overview of how patch installation is managed:

- Before making any changes, we will reboot the HMI and verify that the system functions correctly after reboot. If so, we will then back up the HMI.
- Before installation begins, we'll create patch collections, verify all patch signatures, and validate patch collection integrity.
- Next, we will install security patches.
- After changes are made, we'll work with site engineers to test patched systems and validate that they are functioning properly.
- If the HMI does not function correctly, we can revert to the original backup. If the system is functioning properly, we will make a new backup of the updated system.

At the end of the installation, we will give your staff documentation specifying which changes were made to the HMI. If any planned changes weren't executed, our documentation will detail the reasons for exclusion. Finally, we can provide any necessary training to help staff continue to safely operate systems after the engagement.

Hardening Services

Your Challenges

For any number of reasons, HMIs may be unnecessarily exposed to unauthorized access. Misconfigurations, unapproved credentials, access methods, and even the system's age can play a role in HMI vulnerability. However, in many organizations, addressing these vulnerabilities is challenging. Constantly juggling competing priorities and demands, internal staff struggle to find the time needed to do proactive diagnosis and remediation. Thus, vulnerabilities are often left unaddressed.

Our Solution

GE Vernova's experts can comprehensively examine your HMIs and carry out a thorough hardening to strengthen system security. Our system hardening approaches are based on the Security Technical Implementation Guide (STIG) and GE Vernova's standards. We'll manage the entire project. Our team will work with your internal staff to establish and document a plan, specifying all the tasks and activities we'll be carrying out over the engagement. Our team can provide comprehensive hardening services and approaches, offering coverage of the following areas:

- **Applications.** We will work with your staff to identify which applications are approved and remove any unapproved applications.
- **Media ports.** We'll lock down unused media ports—such as USB ports—using port blockers and other software or configuration techniques.
- **Settings.** Our team will change settings that unnecessarily leave a system exposed to various malware attacks. For example, if a compromised DVD is inserted into a system with auto-play enabled, the machine may be exposed to a malicious code injection. By disabling auto-play, we can help protect systems against this threat. We can also eliminate a potential attack vector by disabling IPv6 services. (GE control systems only use IPv4; so, there is no need to enable IPv6 services.) Our team can also implement any recommendations specified in our Cyber Security Technical Information Letters.
- **Passwords and access controls.** GE Vernova's teams can institute a range of changes to help safeguard system access. For example, we'll disable automatic login, so user authentication is required for each session. We'll set BIOS passwords to help prevent unauthorized BIOS configuration changes. Our team will also work with your staff to identify and disable any unapproved accounts and network shares. We can also join the HMI with an optional Active Directory domain, which GE Vernova can furnish. Through this effort, we can help establish and enforce access policies. We can help apply password expiration and complexity policies. Additionally, we can identify well-known, commonly used privileged accounts, and either disable or rename them. For example, instead of using easily guessed account names like "admin", we will assign unique, site-specific account names.
- **Antivirus.** Our team can install antivirus software, along with the most recent antivirus signatures. Through our services, we can also do a full antivirus scan to detect and remove any viruses.

Benefits

By working with GE Vernova's professional services team, your organization can realize many benefits:

- **Boost staff efficiency.** By offloading ongoing efforts like maintenance, patching, and hardening, we can help your staff free up time to focus on their other responsibilities and priorities.
- **Extend HMI investments.** By doing proactive, preventive maintenance, your organization can avoid issues and prolong usage of your existing HMIs.
- **Mitigate risk.** By more consistently and comprehensively employing patches, our services can help your organization mitigate exposure to cyberattacks.
- **Avoid disruption and downtime.** Our expert engineers can work with your teams to establish plans that help critical plant operations remain functional while services are delivered. Through our proactive maintenance services, your organization can take steps to avoid system issues and the cost and disruption associated with urgent repairs.

OTHER PROFESSIONAL AND CONSULTANCY SERVICES

Some of the other professional and consultancy services GE Vernova offers are listed below:

COMPLIANCE STANDARDS

Organizations greatly benefit by starting with a Below are some of the common cybersecurity compliance

Professional/ Consultancy Service	Description
Cybersecurity Profiling	Current state analysis of organization's cybersecurity maturity level, followed by reporting based on responses from a detailed questionnaire
Industrial Wireless Network Services	Assessment on existing networks, pinholes, unmanaged plant Wi-Fi, weak performance areas, outdated equipment and unauthorized access to plant Wi-Fi
Cybersecurity/Compliance audits	Report on current compliance level to a specific standard or regulation and gap analysis
Incident Response Planning	Definition of roles, processes, communication, and constraints. Context based classification of incidents to provide meaningful alerts, root cause analysis, post incidence support, reporting
Incident Response: Onsite services	Resident Engineer services
Forensics & Analysis services	Digital Forensics readiness and engagement
Tabletop exercises (TTX)	Interactive simulation of business's response to a cybersecurity incident
Virtual CISO	Creation, improvement and maintenance of Cybersecurity Management System (QMS)
Prioritized Security Roadmap	Developing a multi-year roadmap based on types of assets and risk prioritization
Advanced security consulting	For example architecture review
Policy & procedure development	Building the governance model and procedures (network security governance)
Industrial Cybersecurity Training	Training on OT cybersecurity awareness, product installation, maintenance and technical support
Threat Intelligence	Insights on OT application/network vulnerabilities from experts, in-house vulnerability database and external vulnerability announcements
Installation Services	Installation and technical support (onsite and remote) of sensors, appliances and security management console

Note: Some services may not be available in all countries (or locations). Please check with your local GE Vernova representative on availability of service in your area (or location).

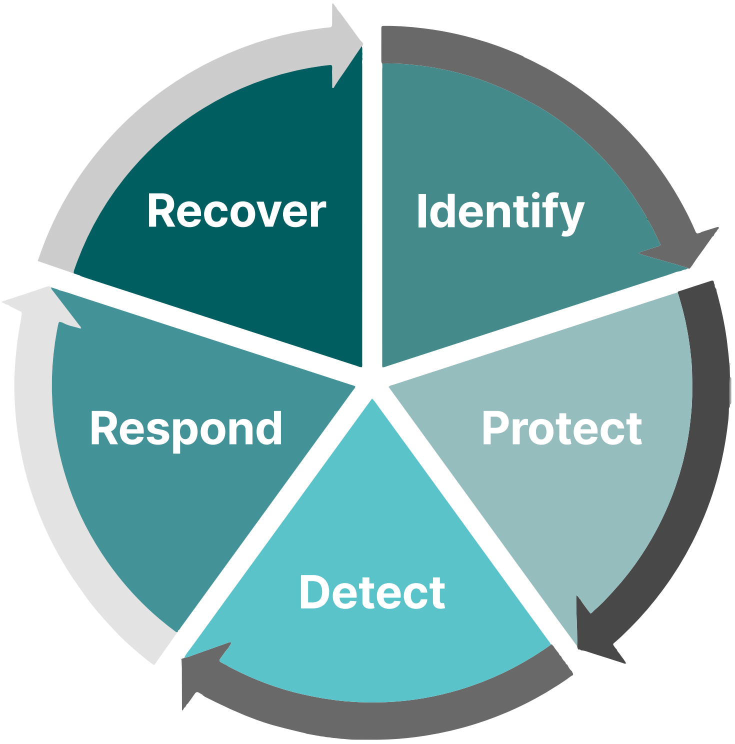
standards that GE Vernova provides professional and consultancy services for.

IEC 62443 - A published international standard, defining cybersecurity 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 was developed by IEC technical committee 65, in collaboration with the International Instrumentation Users Association (previously WIB) and ISA 99 committee members. GE Vernova hardens customer systems using a combination of technical and procedural measures (including patch management) that have been certified to meet IEC 62443 security standards. These standards specify a comprehensive set of security requirements for the installation and maintenance of IACS.

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 cybersecurity plan, operators are required to address known ICS security vulnerabilities and have solutions in place for operating system, application, and third-party software updates, Host Intrusion Detection (HID), and non-repudiation, among others.

NERC CIP - Many US electric utilities are now federally mandated to comply with NERC CIP requirements that dictate industrial security and remediation technology, including required compliance. 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 security 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.

NIST SP800-161 - NIST is the National Institute of Standards and Technology at the US Department of Commerce. The NIST Cybersecurity Framework helps organizations to better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The NIST framework is based on the following 5 core elements:



GE VERNOVA

gevernova.com

Information contained in this document is indicative. No representation or warranty is given or should be relied on. Information provided is subject to change without notice.