GE VERNOVA

FACTSHEET

GE Vernova's Cybersecurity Solution- OTArmor

CYBERSECURITY ASSESSMENT

OVERVIEW

Aiming to ensure you have a full understanding of how your critical assets may be vulnerable to cybersecurity threats is a best practice that must be adhered to, especially for those operating in industries mandated by security compliance standards such as NERC/FERC/CIP or WIB. GE Vernova is your partner in helping you secure your operational technology network and assets.

Our cybersecurity assessment is specifically engineered to help you better understand and address your weaknesses as well as help meet your compliance objectives.

According to the Department of Energy, implementing just the Top 5 CIS Security Controls can reduce the risk of a **cyber attack by 85%!**

BENEFITS

- Cost-effective and scalable to help meet your unique cybersecurity needs
- Control system agnostic approach allows us to assess third party systems
- Leverage our Operation Technology (OT)-specific cybersecurity expertise while you focus on your core business
- Based on industry best practices of the Center for Internet Security (CIS) Top 20 Controls
- Can support compliance with several industry standards such as ISA99/IEC 62443 and NERC-CIP
- Elevate your cybersecurity awareness and identify potential vulnerabilities
- Actionable roadmap of prioritized mitigations to improve your security posture

$4B

aproximate organizational loss after WannaCry attack, due to significant business interruption (no data loss or physical destruction).[1]

163

reported electrical incidents to US electric grid caused by cyber and physical attacks.[2]

$1M

maximum potential penalty per day for a NERC CIP violation.[3]

OUR APPROACH

We start by collecting data on your control system to identify, inventory, and categorize every asset that will be included in the scope of the assessment. Next, we review system configurations, log files, malware defenses, network configurations, data recovery capabilities, access control, and supporting security processes. Finally, we provide a detailed report that quantifies your current cybersecurity maturity rating and provides a prioritized roadmap of recommended mitigations.

WHY GE VERNOVA CYBERSECURITY ASSESSMENT?

For years we've been providing OT cybersecurity solutions for Industrial Control Systems and have full understanding of your availability and security needs related to critical infrastructure. Our cybersecurity experts are knowledgeable on CIS Top 20 Controls and industry standards such as ISA99/IEC 62443, NERC CIP, NIST, and WIB. We can provide your team with the needed support for standards compliance and assist you in better understanding and addressing your vulnerabilities. Our scalable assessment allows you to establish a successful cybersecurity strategy while effectively managing your limited resources.

83%

of the 2170 Industrial Control System (ICS) related vulnerabilities in 2022 reside deep within the ICS network.[4]

45

targeted cybersecurity incidents in energy industry since 2017, 85% could have been prevented with security controls.[5]

605

ransomware attacks in 2022 in industrial organizations, 87% increase YoY.[6]

FEATURES

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

- Control system application: Control system 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
- Mark/EX/LSI protection system: 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

Sources

[1] Security Magazine article, May 2022, https://www.securitymagazine.com/articles/97610-five-years-after-the-wannacry-ransomware-attack#:~:text=Several%20organizations%20were%20affected%20by,approximately%20%244%20billion%20in%20damages.

[2] Axios article on attacks on US power grid, Mar 2023, https://www.axios.com/2023/03/08/power-grid-physical-security-attacks-alarm

[3] North American Electric Reliability Corporation, NERC Guidelines, Jul 2014: https://www.nerc.com/pa/Stand/Resources/Documents/Appendix_4B_of_the_Rules_of_Procedure_Sanction_Guidelines.pdf

[4,6] Dragos 2022 Year in Review Executive Summary, https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Exec-Summary-2022.pdf?hsLang=en#:~:text=Dragos%20investigated%202170%20vulnerabilities%20in,35%25%20more%20ransomware%20groups%20impacting

[5] Power & Beyond article, Mar 2023 https://www.power-and-beyond.com/energy-sector-more-cyber-attacks-in-2022-than-ever-before-a-a53dfeb9e1a85d8a0710a010c7a7e7d3/https://www.power-and-beyond.com/energy-sector-more-cyber-attacks-in-2022-than-ever-before-a-a53dfeb9e1a85d8a0710a010c7a7e7d3/

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.

GEA35308 (11/2023)