CyberSentry™ Health Check

Identify fundamental security gaps in your Industrial Control System

ge.com/grid

Overview

Cyber security threats to the Power Grid and Industrial Control Systems (ICS) are on the rise. Nation states, malware, hackers, organized crime and insider attacks pose serious cyber security risks to the critical systems such as energy, industrial and oil & gas. With growing cyber security concerns, organizations are required to identify fundamental security gaps in their systems and mitigate most critical vulnerabilities as soon as possible.

GE's CyberSentry Health Check is specifically designed to meet the needs of organization's concerns about cyber security in Operational Technology (OT) and Automation & Control systems. The Health Check is a non-invasive assessment of an organization's overall cyber security posture. The Health Check helps substation/plant operators and managers to identify, prioritize and remedy ICS cyber security vulnerabilities by providing an accurate view of their control system's security posture. GE's cyber security consultants are domain experts when it comes to ICS cyber security. Since our cyber security consultants have years of experience in Operational Technology (OT), we are able to carry out our security assessments efficiently and accurately. After our security assessment, we work with P&C Engineers, SCADA engineers and IT security leaders to adapt cyber security best practices appropriately for the ICS environment.

Benefits

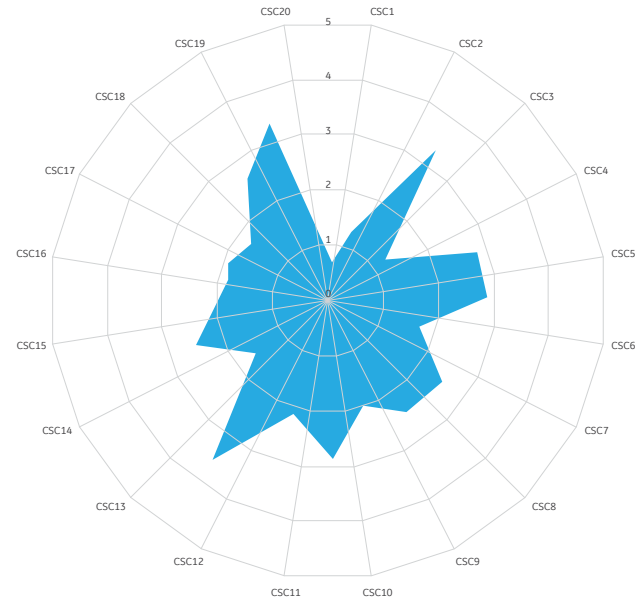
- Identify ICS security gaps and vulnerabilities
- Identify improvement opportunities in People, Process and Technology
- Solid foundation from which an organization can build a sustainable cyber security program
- Non-invasive assessment approach avoids the operational risk in ICS environment
- OT domain experts carrying out assessment efficiently and accurately
- Delivers recommendations to close security gaps quickly and improve security posture
- Standard and repeatable approach to ensure the consistency across systems and sites

Our Approach

GE's CyberSentry Health Check is a quick non-invasive assessment that collects data without impacting the control system's operation. Health Check starts with series of questions followed up with interviews of key personnel to gather information regarding security policies and procedures. Health check follows ICS 20 CyberSentry Security Controls (CSC) framework, which is specifically designed to measure the security posture in ICS environments. Collected data is entered in to CyberSentry Health Check Analyzer which calculates the site maturity rating and improvement opportunities for three key areas: People, Process and Technology.

CSC framework is designed by adopting industrial security standards & regulations such as NIST security framework, IEC 62443, NIS Directives, ICS-CERT and NERC-CIP. CSC framework addresses common threats that organizations are facing today.

The chart below shows mapping from CyberSentry Security Controls (CSC) in to NIST cyber security framework core functions and categories.



ICS Site Position

		NIST Cyber Security Framework				
	CyberSentry Security Controls (CSC)	**Identify (ID)**	**Protect (PR)**	**Detect (DE)**	**Respond (RS)**	**Recover (RC)**
CSC1	Cybersecurity Single Point of Accountability (SPoA)	GV				
CSC2	Training and Awareness		AT			
CSC3	ICS Cybersecurity Policy		IP			
CSC4	System Architecture		PT	AE		
CSC5	Network Security		PT	DP, CM		
CSC6	Inventory Management	AM				
CSC7	Protection Against Malicious and Mobile Code		PT	CM		
CSC8	Identity and Access Control		AC	CM		
CSC9	System Hardening		IP, DS			
CSC10	Media Handling		PT, DS			
CSC11	ICS Information Security		DS			
CSC12	Supply Chain and External Dependencies Management	SC				
CSC13	Assessments & Vulnerability Management	RA		CM	MI	
CSC14	Exception Handling	GV				
CSC15	Change Management		MA			RP
CSC16	Patch Management		PT			
CSC17	Incident Response and Management	RM		AE	AN, CO, RP	
CSC18	Backup and Recovery					RP, IM
CSC19	Business Continuity Plan	RA			AN, IM	RP, IM
CSC20	Physical and Environment Security			CM		

Identify	ID.AM	Asset Management
	ID.BE	Business Environment
	ID.GV	Governance
	ID.RA	Risk Assessment
	ID.RM	Risk Management Strategy
	ID.SC	Supply Chain Risk Management
Protect	PR.AC	Identity Management and Access Control
	PR.AT	Awareness Training
	PR.DS	Data Security
	PR.IP	Information Protection Processes and Procedures
	PR.MA	Maintenance
	PR.PT	Protective Technology

Detect	DE.AE	Anomalies and Events
	DE.CM	Security Continuous Monitoring
	DE.DP	Detection Processes
Response	RS.RP	Response Planning
	RS.CO	Communications
	RS.AN	Analysis
	RS.MI	Mitigation
	RS.IM	Improvements
Recover	RC.RP	Recovery Planning
	RC.IM	Improvements
	RC.CO	Communication

What you get

Health Check Report

Detailed technical report describing GE's observations, including any security gaps, architectural weaknesses, security policy inconsistencies with actionable and prioritized technical recommendations for each observation. Report provides the site maturity rating and summary of key improvement opportunities for three key areas: People, Process and Technology.

Presentation of Strategic & Technical Recommendations

A summary of GE's observations and actionable recommendations to the technical and management-level stakeholders.

Imagination at work

GEA-33138-(E)
English
190807