Global Instrumentation and Control

Network Architecture and Cyber Security: Vulnerability Scanning

Background

Nuclear power plants around the world are faced with stringent regulatory requirements established to ensure safety of the plant, constituents, and the areas serviced. Networks and digital assets have evolved to the point where cyber-attacks present a real world threat to safety and security. Regulatory requirements which address the establishment, implementation and maintenance of a cyber security program present integration challenges.

Westinghouse is committed to ensure safety and security regulations are met. Vulnerability discovery and assessment is a top priority in maintaining Instrumentation and Control (I&C) system safety and security. Vulnerability scanning uncovers threats and risks before an incident can occur. Westinghouse offers vulnerability scanning as a service to ensure safety without negatively impacting the I&C system during the vulnerability scanning and testing process.

Description

Vulnerability assessment is a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Westinghouse assists customers in meeting the remediation, monitoring, verification and cyber threat evaluation and management requirements found in RG 5.71, NEI 08-09, ISO 27001 and IEC 62645. A compliance mapping of these security regulatory requirements can be found below.

Vulnerability Scanning

- **Vulnerability discovery and verification**

  Westinghouse offers solutions for customers to identify high-risk vulnerabilities and the necessary information required to effectively secure systems through mitigation, patching, and reconfiguration. Westinghouse offers multi-tiered network modeling by importing topology information from network devices, automating the vulnerability validation process by continuously validating exploits with known threats, prioritizing real exposures, and documenting all possible attack paths. With these attack paths identified, security resources can focus on updating systems that add risk to critical digital assets.

- **Categorize Assets**

  Westinghouse identifies the importance and value of network assets through direct integration with common asset management, network configuration and vulnerability management tools. This classification allows organizations to grade assets based on data sensitivity, location, user and other important operational characteristics. Identifying each asset’s value, and its context within the business, greatly improves risk intelligence and threat prioritization.

Industry Scanning

The key focus of Westinghouse cyber security is to provide thorough, safe, and complete vulnerability assessments during an outage. Westinghouse has experience with major vulnerability scanning brands such as Tenable, Rapid7, McAfee, CORE, and others to meet a large variety of customer requirements. By safely discovering real-world threats in network systems, customers can determine the real threats that I&C systems are facing.

Benefits

- **Vulnerability Reporting**

  Vulnerability scan reports offer the ability to quickly identify, track, and posture a network's risk. Reporting also allows for tracking a systems risk profile over time to better gauge threat level progression. Westinghouse scan reports allow specific categorizations of all key digital systems ensuring adequate prioritization and monitoring is achieved.

- **No Harm to Systems**

  Westinghouse offers in-depth vulnerability scanning profiles that ensure maximum integration with network systems while not interfering with critical processes. These Westinghouse proprietary scans minimize risk by utilizing the appropriate scan configurations, techniques and network topology. All vulnerability testing is utilized to minimize the risk of impacting control systems while maximizing vulnerability discovery. The unique scanning profiles allow Westinghouse to handle the requirements and challenges that are unique to the nuclear industry without sacrificing quality.

- **Testing Environment**

  Westinghouse offers test beds and vendor-maintained test environments used for performing vulnerability scans. Westinghouse provides testing services either onsite or in the Westinghouse laboratory environment, thus minimizing risk to production systems and verifying compliance with NEI Appendix E controls.

- **Regulatory Requirements**

  Vulnerability scanning aids in meeting regulatory controls in a challenging and ever-changing environment. Westinghouse ensures the controls addressed by these vulnerability tests include:

Compliance Mapping

By implementing vulnerability scanning, the following controls may be addressed in whole or in part:

RG 5.71	NEI 08-09	ISO 27001	IEC 62645	Control Title
C.3.2	E3.2	A12.6.1	7.2.8.7, 5.1.3.1 B	Flaw Remediation
C3.4	E3.4	A12.2.1, A12.4.1	5.2.3.2.3 C, 5.2.3.2.3 K	Monitoring Tools and Techniques
C3.6	E3.6	A11.2.4, A12.1.3	5.2.3.2.3 C	Security Functionality Verification
C3.7	E3.7	A9.4.4, A9.4.5	5.2.3.2.3 N, 5.2.3.2.3 O, 5.2.3.2.7 D2	Software and Information Integrity
C11.3	E10.3			Baseline Configuration
C12.6	E11.6	A14.2.2, A14.2.3, A14.2.9, A14.3.1	6.6.1	Licensee Testing
C13	E12	A12.6.1	5.2.3.1.1 E	Evaluate and Manage Cyber Risk
C13.1		A12.6.1	5.1.2.3 K, 5.1.3.1, 5.2.3.2.2, 6.4.2.1	Threat and Vulnerability Management

Westinghouse Electric Company
1000 Westinghouse Drive
Cranberry Township, PA 16066

www.westinghousenuclear.com