Global Instrumentation and Control

Network Architecture and Cyber Security: Host-based Security Solutions

Background

Nuclear power plants around the world are faced with tough regulatory requirements established to ensure safety of the plant, constituents, and the general public. Digital plant components have evolved to the point where cyber-attacks present a real-world threat to safety and security.

Host-based security relies on agent software installed on each device to provide protection. The agent software monitors the local files, processes, and communication to block or alert on suspicious activity.

Description

Westinghouse is experienced in deploying security solutions on critical digital assets using host-based security agents while minimizing the impact to Instrumentation and Control (I&C) systems.

Westinghouse has performed cyber security assessments on many different kinds of critical digital assets in I&C systems, and is familiar with the requirements of the regulatory guides in relation to the threat vectors concerning existing I&C systems. Westinghouse tailors security solutions to meet each facility's operating environments and needs; experience gives Westinghouse insight into which solutions work best for an individual plant.

Westinghouse tests host-based solutions prior to purchase and installation to provide safe integration with existing control systems.

The Westinghouse solutions are based on the individual needs of the customer and include:

- **Antivirus Software**

  Custom antivirus configurations designed to be used in I&C environments.

- **Patch Management**

  Validate, deploy, and audit system patch levels. Simplifies system administration and maintenance through a centrally managed interface.

- **Application Control (Application White Listing)**

  Permit only baselined applications required for I&C functions. Westinghouse is experienced in creating custom configurations for a variety of environments.

- **File Integrity Monitoring**

  Verifies configurations of I&C Systems, ensuring critical files match configuration controlled baselines.

- **Device Control**

  The use of devices (such as removable media) is monitored and blocked according to site portable media requirements. Permissions to use devices can be restricted based on user or computer.

- **Backup and Restore**

  Hosts are backed up to a server so the machine can be restored in the event of a system failure, minimizing mean time to recovery (MTTR) for critical components.

Benefits

Host-based security can significantly reduce the risk of the most common cyber-attacks. Each host is protected from threats both internal and external to the network.

Westinghouse reduces the hardware footprint and potential future obsolescence issues by implementing virtual machines.

Westinghouse deployments do not obstruct the I&C system. Custom configurations are created based on operational experience with a variety of hosts and performance requirements.

Westinghouse

Compliance Mapping

By implementing host-based security, the following controls may be addressed in whole or in part:

RG 5.71	NEI 08-09	ISO 27001	IEC 62645	Control Title	Antivirus	Application Control	FIM	Device Control	Patch Management	Backup & Recovery
B.1.17	D1.17	A11.2, A12.1, A13.1	5.2.3.2.3	Wireless Access Restrictions				✓		
B.1.18	D1.18		6.6.1	Insecure and Rogue Connections		✓		✓		
B.1.19	D1.19	A.6.2.1	7.2.7.2	Access Control for Portable and Mobile Devices				✓		
B.3.3	D3.3	A6.1.2, A11.2.3, A12.1.4, A13.1.3	5.2.3.2.3	Shared Resources			✓			
B.3.14	D3.13	A12.5.1, A12.6.2, A14.2.4		Mobile Code	✓					
B.3.21	D3.20			Heterogeneity		✓				
B.5.1	D5.1		5.2.3.2.3 A3	Removal of Unnecessary Services and Programs		✓			✓	
B.5.2	D5.2		5.1.1 G, 5.2.3.2.3 K	Host Intrusion Detection System	✓	✓	✓			
B.5.3	D5.3	A9.4.4, A14.2.4	5.2.3.2.3 N, 5.2.3.2.3 O	Changes to File System and Operating System Permissions			✓			
B.5.5	D5.5	A12.5.1, A12.6.2, A14.2.4,	5.1.1 H, 5.1.1 I	Installing Operating Systems, Applications, and Third Party Software Updates					✓	
C.3.2	E3.2	A12.6.1	7.2.8.7, 5.1.3.1 B	Flaw Remediation					✓	
C.3.3	E3.3	A12.2.1	7.2.8.7	Malicious Code Protection	✓	✓		✓		
C.3.4	E3.4	A12.2.1, A12.4.1	5.2.3.2.3 C, 5.2.3.2.3 K	Monitoring Tools and Techniques	✓	✓	✓			
C.3.7	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		✓	✓		✓	
C.4.2	E4.2		7.2.3.1	Maintenance Tools				✓		
C.4.3	E4.3	A11.2.4, A14	7.2.3.3	Personnel Performing Maintenance and Testing Activities				✓		
C.9.6	E8.5	A12.2.1, A12.3.1, A17.2.1	7.2.10.3	CDA Backup						✓
C.9.7	E8.6	A17.2.1, A12.3.1, A17.1.2	5.2.3.2.3 P, 7.2.10.3	Recovery and Reconstitution						✓
C.11.3	E10.3			Baseline Configuration		✓	✓		✓	
C.11.4	E10.4	A12.1.2, A14.2.4	5.2.3.2.3 G, 6.9.1	Configuration Change Control			✓		✓	
C.11.6	E10.6	A12.1.2, A12.5.1	6.9.3, 7.2.3.3, 6.9.3	Access Restrictions for Change			✓			
C.11.7	E10.7		5.2.3.2.3	Configuration Settings		✓	✓			
C.11.8	E10.8		5.2.3.2.3 E	Least Functionality	✓	✓	✓			
C.11.9	E10.9	A8.1.1, A8.1.2	7.2.3.2	Component Inventory			✓	✓	✓	
C.12.5	E11.5	A14.2.1, A14.2.3, A14.2.4, A14.2.8, A14.2.9	7.2.8.3, 7.2.8.5, 7.2.8.10	Developer Security Testing	✓					
	E12	A12.6.1	5.2.3.1.1 E	Evaluate and Manage Cyber Risk	✓	✓				