

Global Instrumentation and Control

Network Architecture and Cyber Security: BEACON Hardening

Background

The Best-Estimate Analyzer for Core Operations-Nuclear (BEACON™) System is a state-of-the-art product providing crucial reactor measurements for required safety margins. BEACON is Westinghouse's advanced core monitoring system which helps ensure safe reactor operations and has successfully been in operation since 1990. It is currently being used by over 50 nuclear power plants in eight countries around the world. The BEACON system has well over 400 reactor years of operational experience.

BEACON is classified as a critical digital asset and must be compliant with industry regulatory requirements. Westinghouse has worked with various regulatory frameworks in the past and has mapped out the controls that may be addressed in whole or in part by BEACON hardening. These include the Regulatory Guide (RG) 5.71, the Nuclear Energy Institute (NEI) 08-09, the International Organization for Standardization (ISO) 27000 series, and International Electrotechnical Commission (IEC) 62645.

Description

Westinghouse cyber security experts are experienced with BEACON Hardening and work so that many of the applicable control requirements outlined in the regulatory guides are met.

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

- **SUSE Linux Enterprise Server (SLES)**
BEACON Hardening is available for SUSE SLES versions 11 SP3 and above.
- **Center for Internet Security (CIS) Benchmarks**
Westinghouse utilizes CIS Benchmarks, a global standard and recognized best practices for securing IT systems, for system configuration.

- **Integration**

BEACON Hardening is completed in conjunction with Westinghouse BEACON operating system release.

Benefits

Westinghouse's cyber security team has experience securing plant control systems, as well as internal operating environments, including the Westinghouse Secure Development and Operating Environment.

BEACON hardening is performed according to CIS benchmarks to meet the regulatory requirements for licensees. Westinghouse has performed hardening procedures on BEACON systems currently installed at multiple plants.

Deliverables

Westinghouse will deliver a hardened SLES operating system, verification testing and report, and on-site support during Site Acceptance Testing (SAT).

Compliance Mapping

By implementing BEACON Hardening, the following controls may be addressed in whole or in part:

RG 5.71	NEI 08-09	ISO 27001	IEC 62645	Control
B.1.2	D1.2	A6.1, A12.4	5.2.3.2.3	Account Management
B.1.3	D1.3		5.2.3.2.3	Access Enforcement
B.1.5	D1.5		5.2.3.2.3	Separation of Functions
B.1.6	D1.6		5.2.3.2.3	Least Privilege
B.1.7	D1.7	A6.1, A12.4	5.2.3.2.3	Unsuccessful Login Attempts
B.1.8	D1.8			System Use Notification
B.1.10	D1.10			Session Lock
B.1.16	D1.16		5.2.3.2.3 A3	"Open/Insecure" Protocol Restrictions
B.1.19	D1.19	A.6.2.1	7.2.7.2	Access Control for Portable and Mobile Devices
B.2.2	D2.2	A12.4, A18.1	5.2.3.2.3	Auditable Events
B.3.2	D3.2		5.2.3.2.3, 5.1.1 C, 5.1.1 E 5.1.1F, 5.1.1G	Application Partitioning/Security Function Isolation
B.3.4	D3.4			Denial of Service Protection
B.4.2	D4.2		5.2.3.2.3 L, 5.2.3.2.3 D, 5.2.3.2.3 E	User Identification and Authentication
B.4.3	D4.3		7.2.1.2	Password Requirements
B5.1	D5.1		5.2.3.2.3 A3	Removal of Unnecessary Services and Programs
B5.3	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
C.7	E6.1		5.1.1, 5.2.3.2.3	Defense-in-Depth
C.3.8	E3.8	A9.4.1, A9.4.2	5.2.3.2.3 B1, 6.4.1.3 6.6.1	Information Input Restrictions
C.3.9	E3.9	A12.4.1	6.6.1	Error Handling
C11.7	E10.7		5.2.3.2.3	Configuration Settings
C11.8	E10.8		5.2.3.2.3 E	Least Functionality