Global Instrumentation and Control

Network Architecture and Cyber Security: Westinghouse Security Platform (WSP)

Background

Every day, the number and sophistication level of cyber threats for systems is growing. Industrial control systems have been a prime target for threat actors in recent years. As a result, Westinghouse has created the Westinghouse Security Platform (WSP). The WSP consists of a suite of cyber security hardware and software monitoring products that integrate with a plant system, to provide centralized cyber security functionality and administer safeguards against cyber-attacks. The WSP has the tools available to secure control systems and comply with cyber security regulations.

Description

The WSP is an All-in-One centralized security monitoring solution, comprised of physical and virtual system components. The WSP can be deployed as an integrated cyber security solution with the control system, or in a standalone configuration to comply with customer requirements.

The WSP utilizes a suite of cyber security products configured and validated for use with Critical Digital Assets (CDA) in an Instrumentation and Control (I&C) environment. Westinghouse also uses the WSP for legacy systems adapting newer technology to secure CDAs. The WSP can be adapted to hardening configurations based on custom settings of systems and licensee requirements.

The WSP is the security platform that provides system integrity assurance, protection from an array of security threats including malware and zero-days, and monitoring of the network infrastructure for malicious activity.

WSP Capabilities

The WSP fulfils the resolution of regulatory compliance demands for control systems. The security products that are implemented address the security controls, but are not limited to, the following:

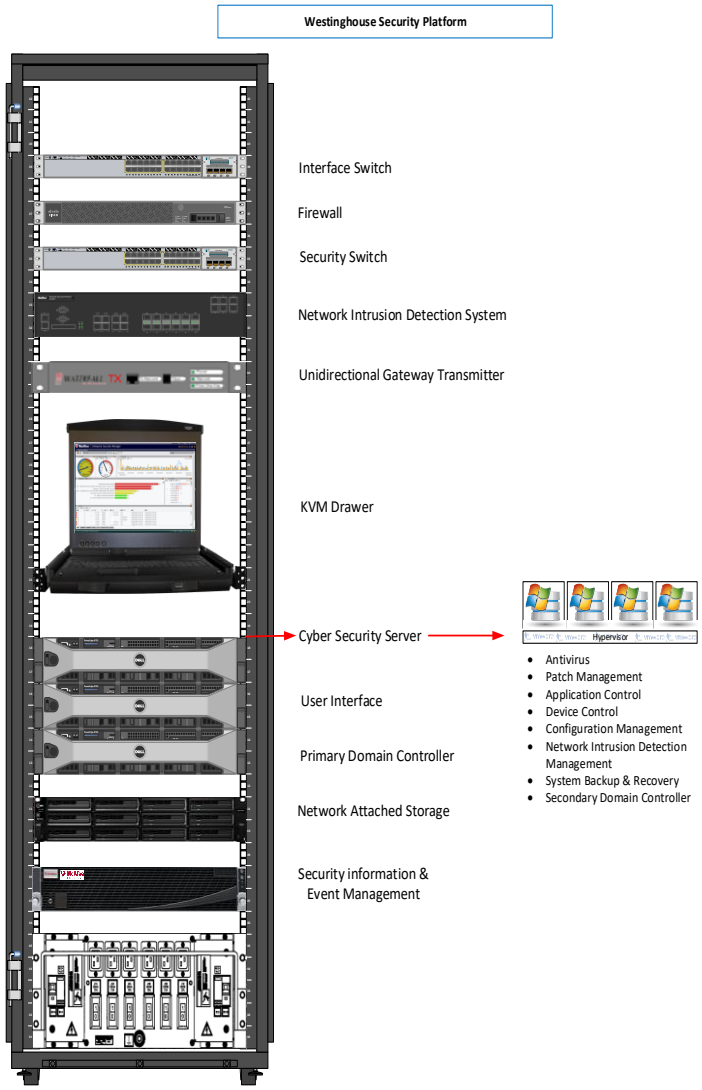
WSP Capabilities
Audit and Accountability
Heterogeneity
Removal of Unnecessary Services and Programs
Host Intrusion Detection System
Changes to File System and Operating System Permissions
Hardware Configuration
Installing Operating Systems, Applications, and Third Party Software Updates
System and Information Integrity
Flaw Remediation
Malicious Code Protection
Monitoring Tools and Techniques
Software and Information Integrity
CDA Backups
Recovery and Reconstitution
Baseline Configuration
Configuration Change Control
Access Restrictions for Change
Configuration Settings
Least Functionality
Component Inventory
Centralized Security Management
Enterprise Threat Detection
Data Loss Prevention

Westinghouse

Benefits

With Westinghouse, there is a comprehensive solution for solving security vulnerabilities and the expertise to implement the safeguards. Westinghouse provides detailed configurations for all products to in accordance with customer requirements. Solutions are centrally managed or standalone. These solutions include:

- **Security Information and Event Management (SIEM)** – Collects, stores and correlates system and security asset event logs. The Westinghouse SIEM product includes incident handling and replicates logs across a data diode.
- **Application Control** – Prevents unauthorized applications from running on the system, such as malware and zero-day threats.
- **Antivirus Software** – Quarantines system files if they match signatures of known malware as well as non-signature software that can detect malicious code.
- **Patch Management** – Manages and installs operating system and some application patches from a central server mitigating known vulnerabilities.
- **Backup and Recovery** – Backs up each client host to a storage server and provides the ability to restore. This is critical for I & C systems that need to be restored on a moment's notice.
- **Network and Attached Storage** – Provides high-performance storage to share and protect critical data and backups. Provides support for regulatory reporting of logs.
- **Vulnerability Scanning** – Offered as a service, scans system assets for insecure configurations. This will report any products that require patches to maintain compliance and security.
- **Device Control** – Monitors the use of devices such as removable media. Restricts access to devices based on user, computer or device type.
- **Network Intrusion Detection System (NIDS)** – Monitors and analyzes system network traffic for indications of malicious activity.
- **File Integrity Monitoring (FIM) / Configuration Management**– Monitors certain system files, folders and configuration settings for changes. Provides notification of changes that occur to demonstrate if the CDA was modified.
- **System Hardening** – Configuring systems and network components to a known secure benchmark to safeguard against vulnerabilities.
- **Cyber Security Server** – Component that houses the Virtual Machines (VM) of the software cyber security components. Reduces the foot print of the WSP which provides flexibility for deployment.
- **User Interface Server** – Component of the WSP that interfaces with physical and virtual components. This option provides a central location of access.
- **Domain Controller** – Both physical and virtual for centralized domain management making the WSP easy to manage.
- **Unidirectional Gateway, Interface Switch, Security Switch, and Firewall** – Networking components of the WSP architecture to provide segmentation and mitigate system intrusion.



Westinghouse Electric Company
1000 Westinghouse Drive
Cranberry Township, PA 16066

July 2019/ NA-0144