Global Instrumentation and Control

Network Architecture and Cyber Security: All-in-One Cyber Security Monitoring System

Background

Regulatory bodies and industry groups around the world now require nuclear utilities to introduce new hardware and software into the plant architecture to prevent cyber-attacks and to collect, monitor and analyze data for cyber vulnerabilities, threats and unwarranted activities. Westinghouse can assist with installing and configuring All-in-One cyber security monitoring systems which contain Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) devices from the industry's top vendors. Westinghouse is able to provide a scalable, comprehensive solution to secure Instrumentation and Control (I&C) systems.

All-in-One Cyber Security Monitoring System

An All-in-One cyber security monitoring solution from Westinghouse allows a customer to actively detect, analyze and monitor the network from an array of security attacks including viruses, worms, spyware, denial-of-service attacks, malware, as well as unknown or zero-day attacks. All-in-One monitoring solutions are designed to passively monitor an entire network infrastructure.

This system can monitor all devices internally while examining traffic on a network. By utilizing signature-based detection, anomaly-based protocol detection and stateful protocol analysis; customers are able to detect the latest threats entering a system. An All-in-One monitoring system consists of multiple devices including a user interface station, high-capacity storage solution, network routing devices with the core security functions contained within an Intrusion Detection System (IDS) and a Security Information and Event Management (SIEM) device.

Intrusion Detection System (IDS)

An IDS allows a Westinghouse customer to take control of the network with the ability to maintain multiple simultaneous intrusion detection systems and policies from a single appliance. An IDS can be deployed in-line with all network traffic or out of band. The IDS will take all traffic received and correlate events to network and session activity using built-in network flow collectors for exploit, vulnerability and anomaly-based detection.

Security Information and Event Management (SIEM)

A Security Information and Event Management (SIEM) device brings event, threat and risk data together to provide strong security intelligence, rapid incident response, seamless log management and extensible compliance reporting. A SIEM consolidates data, correlates, assesses and prioritizes security events for all logging capable software applications and appliances on a network.

This solution collects security event logs from I&C systems (critical digital assets) and stores the events in a central location. The SIEM provides the customer with automated alerting, information and event management, log management, network analysis functionality, while collecting data for analysis and correlation. This functionality allows a Westinghouse customer to greatly improve their monitoring capabilities, risk intelligence and threat prioritization of critical digital assets.

Westinghouse Content Support

Westinghouse offers on-site and remote support for IDS and SIEM solutions for single and multi-level security implementations. Westinghouse support includes custom nuclear content support, extended hardware and software support as well as on-site training services. Additional content includes configuration settings, monitoring, and reports such as:

- Custom control system alerts
- Proprietary system alerts
- Compliance-related alerting and viewing
- Compliance-related reporting
- Security zones (for multiple level deployments only)

Westinghouse

Westinghouse Troubleshooting and Tuning Support

Westinghouse can perform on-site configuration and tuning for SIEM & IDS products. Westinghouse troubleshooting and tuning support ensures that SIEM and IDS devices are deployed properly in an environment. Support covers initial installation, troubleshooting of current installations, as well as tuning. Tuning and configuration covers elements such as:

- Log correlation
- Rule creation & modification
- False Positive Tuning
- SIEM/IDS receiver(s) support
- Network connectivity
- Data sources
- Storage Nodes

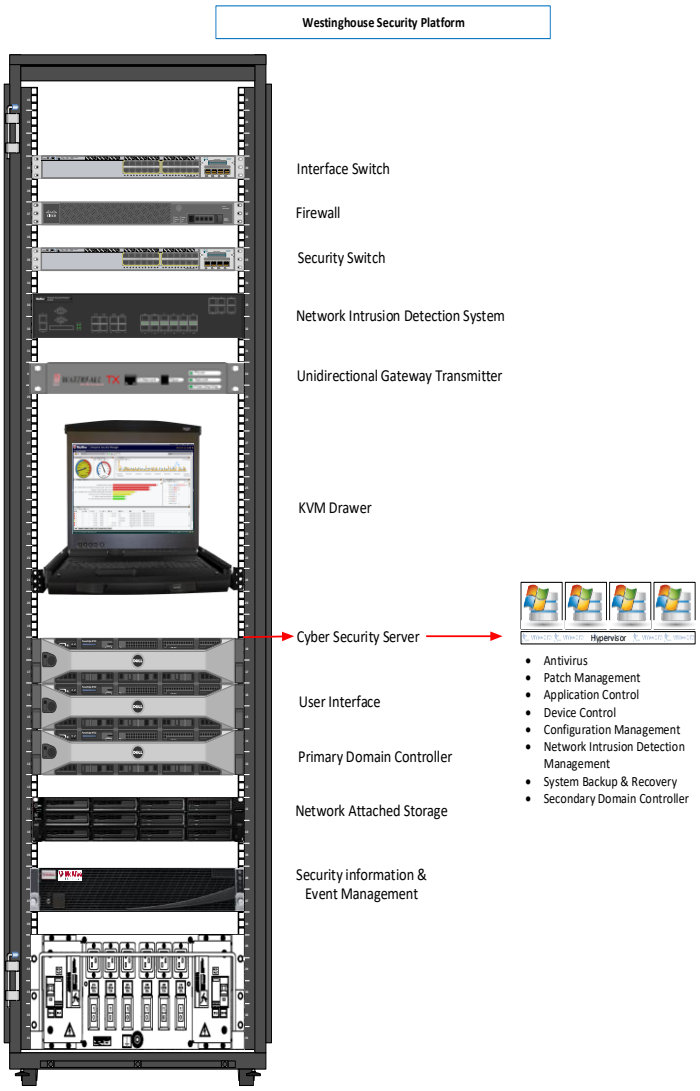
Westinghouse Partnership with McAfee

Westinghouse Electric Company LLC and McAfee, Inc., have entered into a partner agreement providing a comprehensive solution to the nuclear market. Westinghouse Cyber Security specializes in following list of McAfee® licensed products:

- McAfee Enterprise Security Manager (ESM)
- McAfee Advanced Correlation Engine (ACE)
- McAfee Application Data Monitor (ADM)
- McAfee Enterprise Log Manager (ELM)
- McAfee Event Receiver (REC)
- McAfee Network Security Platform (NSP)
- Gold Level Support and Maintenance
- Services and Training

Regulatory Requirements

Monitoring and event analysis ensures that the adequate regulatory controls are met in a challenging and ever-changing environment. SIEM and IDS products offered by Westinghouse allow customers to meet monitoring and log correlation requirements stemming from RG 5.71, NEI 08-09, ISO 27001, and IEC 62645, which are shown in the table, below. The solutions offered provide customers with event analysis, tracking, event correlation, incident monitoring, auditing capabilities and automated alerting required by compliance.



The standard cabinet layout of the Westinghouse Security Platform (WSP) delivering an all-in-one management and monitoring solution

Westinghouse Electric Company
1000 Westinghouse Drive
Cranberry Township, PA 16066

July 2019/ NA-0125

Westinghouse All-in-One Cyber Security Monitoring System Compliance Checklist

RG 5.71	NEI 08-09	ISO 27001	IEC 62645	Control
B.1.11	D1.11	A12.4	5.2.3.2.3 I	Supervision and Review - Access Control
B.1.15	D1.15	A13.1	5.2.3.3.1 5.2.3.2.3	Network Access Control
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.1.2	D1.2	A6.1, A12.4	5.2.3.2.3	Account Management
B.1.20	D1.20			Proprietary Protocol Visibility
B.1.21	D1.21	A15.1 A15.2	5.1.1 H 5.1.1 I	Third Party Products and Controls
B.1.4	D1.4	A11.2 A12.1 A13.1 A13.3	5.2.3.2.3	Information Flow Enforcement
B.1.7	D1.7	A6.1 A12.4	5.2.3.2.3	Unsuccessful Login Attempts
B.1.9	D1.9			Previous Logon Notification
B.2.10	D2.10	A12.4.1	5.2.3.2.7 C 5.2.3.2.3 N	Non-Repudiation
B.2.11	D2.11	A12.4 A12.3.1 A18.1.3	5.1.3.1	Audit Record Retention
B.2.12	D2.12	A12.4	5.2.3.2.3	Audit Generation
B.2.2	D2.2	A12.4 A18.1	5.2.3.2.3	Auditable Events
B.2.3	D2.3	A12.4	5.1.3.1, 5.2.3.2.3	Content of Audit Records
B.2.4	D2.4	A12.4		Audit Storage Capacity
B.2.5	D2.5	A12.4 A18.1.2	5.2.3.2.3 K	Response to Audit Processing Failures
B.2.6	D2.6	A12.4	5.2.3.2.3 H	Audit Review, Analysis, and Reporting
B.2.7	D2.7	A12.4	5.2.3.2.3	Audit Reduction and Report Generation
B.2.9	D2.9	A12.4	5.2.3.2.3 I	Protection of Audit Information
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.3.4	D3.4			Denial of Service Protection

Westinghouse All-in-One Cyber Security Monitoring System Compliance Checklist (Continued)

RG 5.71	NEI 08-09	ISO 27001	IEC 62645	Control
B.3.6	D3.6	A8.3.3, A10.1.1 A11.2.4 A13.1.1	5.2.3.2.3 F	Transmission Integrity
B.4.4	D4.4	A12.4.1 A12.4.3	5.2.3.2.3	Non-authenticated Human Machine Interaction (HMI) Security
B.4.5	D4.5	A9.2 A9.4	5.2.3.2.3 D 5.2.3.2.3 E	Device Identification and Authentication
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.5.4	D5.4	A11.1.2 A11.1.4	5.2.3.2.3 C 5.2.3.2.3 F 5.2.3.2.3 O	Hardware Configuration
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.11.9	E10.9	A8.1.1 A8.1.2	7.2.3.2	Component Inventory
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.3.8	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
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.7	E6		5.1.1 5.2.3.2.3	Defense-In-Depth
C.8.5	E7.5	A16.1.4	7.2.9.2	Incident Monitoring
C13	E12	A12.6.1	5.2.3.1.1 E	Evaluate and Manage Cyber Risk