WHITEPAPER:
CYBERSECURITY

Enhancing Industrial Cybersecurity with FlexEdge®, Powered by Crimson®, Aligned with ISA/IEC 62443 Standards

Executive Summary

Cybersecurity is a growing concern in industrial environments, where alignment with ISA/IEC 62443 standards is critical. This whitepaper explores how Red Lion's FlexEdge®, powered by Crimson® 3.2, helps organizations meet these standards through key countermeasures, including logical access controls, data flow management, data integrity, policy enforcement, and system hardening.

FlexEdge, with its robust Crimson 3.2 software, offers tailored security features for industrial applications, such as secure login, role-based access, and remote authentication, aligning with logical access control requirements. It includes advanced data flow controls like VLANs and firewalls to manage network segmentation and secure data transmission. Data integrity is maintained through encryption and VPN support, safeguarding information from unauthorized access and modification.

Controls engineers can align with IT policies like password expiration, ensuring consistent security practices across the network. Additionally, FlexEdge allows administrators to disable unused ports and services, reducing potential vulnerabilities. By leveraging these features, organizations can align their industrial applications with ISA/IEC 62443, enhancing their cybersecurity posture against evolving threats.

Introduction of ISA/IEC 62443

ISA/IEC 62443 is a series of standards that secure Industrial Automation and Control Systems (IACS) throughout their lifecycle, from design to decommissioning. What sets ISA/IEC 62443 apart is its adaptation of IT cybersecurity practices to industrial environments.

KEY CONCEPTS INCLUDE:

Principle of Least Access: Restricting user and device permissions to the minimum necessary, reducing potential damage from breaches.

Defense in Depth: Implementing multiple layers of security controls, such as firewalls, encryption, and access controls, to protect critical assets even if one layer is compromised.

Zones and Conduits: Segmenting the network into secure zones with conduits controlling data flow between them, protecting sensitive data and limiting the spread of potential breaches.

Red Lion's FlexEdge supports these concepts, providing the necessary tools to implement a robust, ISA/IEC 62443-aligned cybersecurity posture.

Aligning Red Lion FlexEdge with ISA/ IEC 62443 Countermeasure Breakdown

LOGICAL ACCESS CONTROLS

Overview: Logical access controls ensure only authorized users have the necessary permissions to interact with specific systems, following the principle of least access.

FlexEdge's Role: FlexEdge provides secure login, role-based access control, and remote authentication (RADIUS). It enables administrators to define user roles and access levels, helping enforce granular policies.

Key Features: Customizable password policies, role-based permissions, integration with IT authentication protocols.

Benefit: Limits access to authorized functions, reducing the risk of unauthorized access.

DATA FLOW CONTROLS

Overview: Data flow controls manage the transmission of information within and between network segments, reducing unauthorized access, data leakage, and compromise.

FlexEdge's Role: Crimson® 3.2 empowers administrators to use VLANs and firewalls for segmenting network traffic and controlling data flow. This ensures that sensitive data remains within designated zones and is transmitted securely.

Key Features: VLAN support, integrated firewall, configurable traffic rules.

Benefit: Protects the network from unauthorized data flow, limiting exposure to threats and maintaining data integrity.

DATA INTEGRITY CONTROLS

Overview: Data integrity controls protect data from unauthorized alterations or corruption during transmission, ensuring its trustworthiness.

FlexEdge's Role: FlexEdge supports encryption (e.g., SSL/TLS) and VPN configurations to secure data communication. The platform also offers data integrity checks and whitelisting to prevent tampering.

Key Features: Built-in SSL/TLS support, VPN capabilities, data whitelisting.

Benefit: Ensures data remains confidential and unaltered, safeguarding against tampering and unauthorized disclosure.

POLICY/PROCEDURE ENFORCEMENT

Overview: Enforcing IT policies and procedures, like password expiration and access restrictions, helps maintain a consistent cybersecurity framework across the network.

FlexEdge's Role: Crimson® 3.2 enables the implementation of IT policies, including password policies and access control. It supports syslog for centralized audit logging, allowing for policy compliance monitoring.

Key Features: Password policy settings, user-defined access rules, syslog for audit trails.

Benefit: Facilitates consistent security practices and aids compliance with cybersecurity standards.

SYSTEM HARDENING

Overview: System hardening involves reducing the attack surface by disabling unnecessary services, closing unused ports, and applying security patches.

FlexEdge's Role: FlexEdge allows administrators to disable unused ports and services through Crimson® 3.2. This flexibility reduces the system's vulnerability to potential threats.

Key Features: Customizable security settings, port management, support for regular updates.

Benefit: Minimizes vulnerabilities, enhancing the network's overall security posture.

By addressing these counter measures, Red Lion's FlexEdge, powered by Crimson® 3.2, supports a comprehensive, layered defense strategy aligned with ISA/IEC 62443. This empowers organizations to protect their industrial assets and maintain the integrity and confidentiality of their operations.

Work with HMS.
The number one choice for Industrial ICT - Information and Communication Technology.

www.hms-networks.com