€TRAINING

Process Control Cybersecurity

Process Control Cybersecurity

Introduction:

This training program provides comprehensive instruction on safeguarding industrial control systems from cyber threats. Through it, attendees are equipped with the knowledge and skills necessary to ensure the integrity, availability, and confidentiality of critical process control systems.

Program Objectives:

At the end of this program, participants will be able to:

- List what process control assets need to be protected.
- Understand the Current Industrial Security Environment.
- List and explain the main components of the process control security standard IEC 62443.
- Understand how to perform a risk assessment and apply cybersecurity counter-measures.
- Learn how to perform application diagnostics, troubleshooting, and incidence response.

Targeted Audience:

- Operations and Maintenance Personnel.
- Process Control Operators, Engineers.
- Process, Plant, and Project Managers.
- Process Engineers and Managers.
- Instrumentation Technicians and Engineers.
- System Integrators.
- IT/OT Engineers and Managers Industrial Facilities.
- IT/OT Corporate / Security Professionals.
- Plant Safety, Security, and Risk Management.
- Security Personnel in all categories.

Program Outlines:

Unit 1:

Introduction and Cybersecurity Fundamentals:

- Introduction to Process Control Cybersecurity.
- Understanding the Current Industrial Security Environment.
- How IT and OT Operational Technology in the Plant Floor are Different and How They are the Same.
- Overview of Process Control.
- Overview of Industrial Communication Systems and Networks.
- How Cyber-attacks Happen: Threats, Vulnerabilities, Attacks.
- Asset Identification and Impact Assessment.

Unit 2:

Introduction to the IACS Cybersecurity Lifecycle and ISA99 / IEC 62443:

- Identification & Assessment Phase.
- Design & Implementation Phase.
- Operations & Maintenance Phase.
- Limits of a Conventional IT Approach.
- The IEC 62443 Security Approach and Standards.
- Risk Analysis Risk Identification, Classification, and Assessment.
- CAL Cybersecurity Assurance Levels.
- Functional Requirements of IEC 62443.

Unit 3:

Addressing Security Risks: Process Control Security Counter-Measures:

- Antivirus, Anti-spyware.
- Firewalls, Traffic Analyzers.
- Encryption, Virtual Private Networks VPNs.
- Passwords - Authentication Systems.

- Access Control - Intrusion Detection / Prevention.
- Network Segmentation.

Unit 4:

Application Diagnostics and Troubleshooting and Management:

- Interpreting Device Alarms and Event Logs for early detection.
- Network Intrusion Detection Systems for identifying suspicious activities.
- Network Management Tools for monitoring and managing network infrastructure.
- Application Management and Whitelisting Tools for controlling application access.
- Antivirus and Endpoint Protection Tools for protecting endpoints from malware.
- Security Incident and Event Monitoring SIEM Tools for comprehensive monitoring and analysis.

Unit 5:

Advanced Practices in Process Control Cybersecurity:

- Understanding the Current Industrial Security Environment and Cybersecurity Fundamentals.
- Introduction to the IACS Cybersecurity Lifecycle and ISA99 / IEC 62443.
- Addressing Security Risks: Process Control Security Counter-Measures.
- Application Diagnostics and Troubleshooting.
- Developing and Following an IACS Management of Change Procedures.
- Developing and Following an IACS Patch & Antivirus Management and Cybersecurity Audit Procedures.