Critical Infrastructure Protection Curriculum

Cyber Security for Industrial Control Systems

Training Services

**COURSE FORMAT**

This 1-day course utilizes an instructor-led structure that blends presentations with informative, relevant ICS-specific demonstrations utilizing real-world ICS software and related security components. Key topics are reinforced with examples using ICS components.

**PREREQUISITES**

The material is “advanced” in content, however the course duration limits the detail presented on any single topic. To receive the greatest value, attendees should have a basic knowledge of networking concepts, and an understanding of industrial control systems. Additional material is provided to assist attendees in any areas that require improvement.

**WHO SHOULD ATTEND**

This course is designed for anyone who is involved in industrial or manufacturing facilities including both management and technical staff. This includes engineering and facility managers; as well as control system engineers, system integrators, system vendors, OEM suppliers, technicians, security/IT auditors, and IT support personnel.

Engineering and facility managers gain valuable insight into the issues surrounding their critical automation systems. Engineers, system integrators, vendors, suppliers, technicians, auditors, and support personnel are provided with a well-rounded introduction into not only the problems facing industrial systems, but some of the steps necessary to adequately secure industrial systems.

**COURSE DESCRIPTION**

This intermediate-level course is designed to provide a well-rounded overview of the issues facing industrial environments and the solutions around securing the automation systems from current and emerging cyber threats. Students begin with an overview of risk management and the components that translate cyber risk into business risk. Each of these elements is discussed in relation to industrial systems, and how standards, guidelines and best practices are used to help reduce overall risk. Students are also introduced to methodologies used in the execution of actual system evaluations to assess current risk and identify areas of improvement.

**LEVERAGING EMERGING TECHNOLOGIES**

Instructor-led demonstrations focus on providing a real-world scenario combining not only ICS equipment, but also ICS-specific security technologies.

Some of the technologies covered in this intermediate course include:

- Enterprise Firewalls & Firewall Evaluation Tools
- Log Monitoring
- Security Incident & Event Management Solutions
- Vulnerability Scanners
- Compliance Auditing Tools
- Industrial Firewalls including Deep Packet Inspection for Industrial Protocols
- Application and Network Whitelisting
- Industrial Protocols
- Unidirectional Security Gateways
- Network Encryptors for Industrial Protocols
CRITICAL INFRASTRUCTURE PROTECTION CURRICULUM

Cyber Security for Securing Industrial Control Systems

Learning Objectives

WHY INDUSTRIAL CONTROL SYSTEMS ARE AT RISK FROM CYBER THREATS
- Challenges in Securing ICS Architectures
- Industrial Security Incidents
- Cyber Threats and Trends
- Misconceptions about Industrial Security

WHY INDUSTRIAL SECURITY IS DIFFERENT FROM INFORMATION SECURITY
- Common and Less Common Threat Vectors
- Understanding the Similarities & Differences
- Endpoints and Cyber Security
- Major Security Objectives
- Security Life Cycle Management

IS YOUR INDUSTRIAL NETWORK SECURE?
- Always a Game of “Catch Up”
- Exploitation and Open Source
- Top Cyber Concerns and Controls Used

UNDERSTANDING AND IDENTIFYING ICS VULNERABILITIES
- Assessment Results
- Understanding Types of Vulnerabilities
- Common ICS Vulnerabilities Classes
- How have things changed since Stuxnet?

RISK MANAGEMENT AND CYBER SECURITY
- Components of Risk
- Consequences of an ICS Compromise
- Functional Safety & Industrial Security
- Risk Assessment Methodologies

CONDUCTING AN ICS CYBER SECURITY ASSESSMENT
- Goals and Objectives
- Security and Vulnerability Assessments
- Assessment Methodologies
- Theoretical Assessments (CSET)
- Physical Assessments
- On-Line versus Off-Line Assessments
- Data Collection
- System Characterization
- White Box versus Black Box Techniques
- Network Assessment Tools & Techniques
- Firewall, Router & Switch Analysis
- Vulnerability Scanning & Prioritization
- Compliance Auditing

PREPARING FOR THE NEXT-GENERATION OF CYBER THREATS
- Recent Events Analysis
- Lessons Learned
- Are we doing enough?

OPTIONAL DEMONSTRATIONS
- Network Segmentation and IP Subnetting
- Network Communication & Enhanced Access Control
- Improving Credential Management using Active Directory
- Mapping and Monitoring Network Anomalies on Industrial Networks

SUPPLIMENTAL COURSE MATERIAL
(AVAILABLE VIA ON-LINE DOWNLOAD)
- Industry Standards & Best Practices
- Guidance Documents
- Case Studies
- Reference Library