PACEUP
Your Oil & Gas Training Solutions

Cekap

ICS CYBER SECURITY AWARENESS

3 Days | Kuala Lumpur

Program Overview

The move to using open standards such as Ethernet, TCP/IP, and web technologies in supervisory control and data acquisition (SCADA) and process control networks has begun to expose these systems to the same cyberattacks that have wreaked so much havoc on corporate information systems. This course provides a detailed look at how the ANSI/ISA99 standards can be used to protect your critical control systems. It also explores the procedural and technical differences between the security for traditional IT environments and those solutions appropriate for SCADA or plant floor environments.

Who Should Attend?

All plant's employees who access ICS/SCADA/DCS systems and the managers.

Course Methodology

- From trainer lead presentations to online courses
- From quiz to escape games
- From custom made movies to posters & goodies

Key Modules

- Understanding the Current Industrial Security Environment
- How Cyberattacks Happen
- Creating A Security Program
- Risk Analysis
- Addressing Risk with Security Policy, Organization, and Awareness
- Addressing Risk with Selected Security Counter Measures
- Addressing Risk with Implementation Measures
- Monitoring and Improving the CSMS

Learning Objectives

Awareness training objective is to prepare your company's plant personnel to understand the importance of Cyber Security for Plant's systems, the latest threat landscape, and their role to mitigate today's cyber threat – thereby increasing the awareness of your frontline personnel to resist social engineering, phishing, as well as to help them identify and report possible cyber issues.

Learning Outcome

- Discuss the principles behind creating an effective long term program security
- Interpret the ISA/IEC 62443 industrial security framework and apply them to your operation
- Define the basics of risk and vulnerability analysis methodologies
- Describe the principles of security policy development
- Explain the concepts of defense in depth and zone/conduit models of security
- Analyze the current trends in industrial security incidents and methods hackers use to attack a system
- Define the principles behind the key risk mitigation techniques, including anti-virus and patch management, firewalls, and virtual private networks

For more information, visit us at:
www.paceup.com.my

In Collaboration with:

GLOBAL SECURITY NETWORK

HRDF MALAYSIA
CLAIMABLE

COURSE OUTLINE

UNDERSTANDING THE CURRENT INDUSTRIAL SECURITY ENVIRONMENT

- What is Electronic Security for Industrial Automation and Control Systems?
- How IT and the Plant Floor are Different and How They are the Same?

HOW CYBERATTACKS HAPPEN?

- Understanding the Threat Sources
- The Steps to Successful Cyberattacks

CREATING A SECURITY PROGRAM

- Critical Factors for Success
- Understanding the ANSI/ISA-62443-2-1 (ANSI/ISA-99.02.01-2009)
  Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program

RISK ANALYSIS

- Business Rationale
- Risk Identification, Classification, and Assessment

ADDRESSING RISK WITH SECURITY POLICY, ORGANIZATION, AND AWARENESS

- CSMS Scope
- Organizational Security
- Staff Training and Security Awareness

ADDRESSING RISK WITH SELECTED SECURITY COUNTER MEASURES

- Personnel Security
- Physical and Environmental Security
- Network Segmentation
- Access Control

ADDRESSING RISK WITH IMPLEMENTATION MEASURES

- Risk Management and Implementation
- System Development and Maintenance
- Information and Document Management

MONITORING AND IMPROVING THE CSMS

- Compliance and Review
- Improve and Maintain the CSMS

For more information, visit us at:
www.paceup.com.my

In Collaboration with:

GLOBAL SECURITY NETWORK

HRDF MALAYSIA CLAIMABLE