Global Horizon
TRAINING CENTER

Training Course:
Process Control Cybersecurity

29 September - 3 October 2024
Sharm El-Sheikh (Egypt)
Sheraton Sharm Hotel

Training Course:
Process Control Cybersecurity

Training Course code: IT234647 From: 29 September - 3 October 2024 Venue: Sharm El-Sheikh (Egypt) - Sheraton Sharm Hotel Training Course Fees: 3850 Euro

Introduction

This Process Control Cybersecurity training seminar will address the most important issues related to the protection of assets in a process control environment. Unlike traditional IT information technology systems, process control assets include IACS Industrial Automation and Control Systems which need to be protected.

Recently, three out of four organizations in the oil and natural gas industry in the Middle East have experienced a security compromise that resulted in the loss of confidential data or Operational Technology OT disruption. This is according to a recent study by Siemens and the Ponemon Institute. Another finding in the report is that - organizations believe that roughly one in every two cyberattacks against the OT environment actually goes undetected. The report also notes that the oil and gas industry is the target of as much as one-half of all cyberattacks in the Middle East and given its importance for the region's economies, the risks faced by the industry are all the more pressing. OT, which encompasses systems that monitor and control physical devices and industrial processes, is increasingly interconnected with IT networks. In spite of all its benefits, this IT/OT convergence is opening up new avenues for attacks.

Course Objectives of Process Control Cybersecurity

At the end of this course the 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 of Process Control Cybersecurity

- 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
- Any individual that needs to address issues in the ever-expanding and complex field of cybersecurity in the industrial environment

Course Outlines of Process Control Cybersecurity

Day 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

Day 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

Day 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

Day 4

Application Diagnostics and Troubleshooting

- Interpreting Device Alarms and Event Logs
- Early Indicators
- Network Intrusion Detection Systems
- Network Management Tools
- Interpreting OS and Application Alarms and Event Logs
- Application Management and Whitelisting Tools
- Antivirus and Endpoint Protection Tools
- Security Incident and Event Monitoring SIEM Tools

Day 5

IACS Cybersecurity Operating Procedures & Tools and Incident Response

- Developing and Following an IACS Management of Change Procedures
- IACS Configuration Management Tools
- Developing and Following an IACS Patch & Antivirus Management and Cybersecurity Audit Procedures
- Patch Management Tools
- Antivirus and Whitelisting Tools
- Auditing Tools
- Developing and Following an IACS Incident Response Plan
- Incident Investigation and System Recovery

Registration form on the Training Course: Process Control Cybersecurity

Training Course code: IT234647 From: 29 September - 3 October 2024 Venue: Sharm El-Sheikh (Egypt) - Sheraton Sharm Hotel Training Course Fees: 3850 Euro

Complete & Mail or fax to Global Horizon Training Center (GHTC) at the address given below

Delegate Information

Full Name (Mr / Ms / Dr / Eng): .....
Position: .....
Telephone / Mobile: .....
Personal E-Mail: .....
Official E-Mail: .....

Company Information

Company Name: .....
Address: .....
City / Country: .....

Person Responsible for Training and Development

Full Name (Mr / Ms / Dr / Eng): .....
Position: .....
Telephone / Mobile: .....
Personal E-Mail: .....
Official E-Mail: .....

Payment Method

- ☐ Please find enclosed a cheque made payable to Global Horizon
- ☐ Please invoice me
- ☐ Please invoice my company

Easy Ways To Register

Telephone: +201095004484 to provisionally reserve your place.	Fax your completed registration form to: +20233379764	E-mail to us : info@gh4t.com or training@gh4t.com	Complete & return the booking form with cheque to:Global Horizon 3 Oudai street, Aldouki, Giza, Giza Governorate, Egypt.