AbarSolutions
Petroleum Consultancy

Training Course :

Cyber Security for Industrial Control Systems

Training Course For One Week In

Turkey, Istanbul, Taksim Gonen Hotel

Which Be Held As Under Details :

Tel. : 00965 22610021 - 99600277 , Fax : 00965 22630021
Email : info@abarsolutions.com , W.Site : www.abarsolutions.com

Abar Solutions Petroleum Consultancy Invite Your Employee To Participate With Us In Special Training Course As Under Details:

Course Name	Cyber Security for Industrial Control Systems					
Code	Period	Language	Start	End	Location	Fees KD
IT 15	5 Days	English	17/09/2018	21/09/2018	Turkey, Istanbul, Taksim Gonen Hotel	1195
			15/10/2018	19/10/2018		
			19/11/2018	23/11/2018		
			10/12/2018	14/12/2018		
The Fees Includes: Lecturer, Training Material, Training Room With One Coffee Break Daily, Certificate Of Attendance In Last Day Training Course						

Course Description

The threat of Cyber Attacks is widespread and global, which affects individuals, commercial organisations and nation states alike. The ability to safeguard your organisation and technology from attacks, and more importantly understand how to identify, analyse, respond and investigate cyber-attacks as a security breach is paramount. The ability for an Information Security Breach resulting in the circumvention of operational technology controls can have disastrous effects, as we have seen with global documented case such as Ukraine Power Station attack in December 2015. Attacks are growing in number and sophistication. The networked control systems are often integrated and reliant with specialist strategic partners underpins your organisational risk and competitive ability. Furthermore, to effectively detect and deter any cyber attack, you need to understand the nature, motive and ways of perceived cyber threat actors. In doing so and utilising appropriate countermeasures, best practice and management techniques will mitigate the risk of cyber attack and enhance protection to your assets. Board of directors, corporate officers and chief engineers are starting to understand the implication of Cyber breaches within their commercial organisation and their potential effect to their personal liability. Therefore, Cyber Security is now promoted and listed as one of the top three Risks an organisation has to manage. This training course will feature:

- An understanding of Cyber Security issues
- Approaches to Cyber Security within an Operational Technology environment.
- An introduction to Cyber Security Frameworks
- Current Best Practice for Cyber Security Response Methods
- Approaching Cyber Security Response Plans

What are the Goals?

By the end of this training course, the participants will be able to:

- Understand Information Security, and how this is deployed in an Operational Technology Environment
- Understand a range of Cyber threats and assess a security posture within an Operational Technology environment.
- Appreciate the leading International Standards and Governance models for Cyber Security and current best practice.
- Understand the approaches for Crisis and Incident Management for Cyber Security Breaches

Course Content & Outlines

Day One: What is Cyber Security?

- Overview of Cyber Security and Organised Crime
- Key Elements of Cyber Crime and Terrorist Targeted Attacks
- Technology, Policing, and Investigation of Electronic Crime
- Ethical Hacking and Cyber Crime
- Civil and Criminal Considerations
- Case Study

Day Two: Assessing Your Cyber Security Posture

- Cyber Security and Risk Assessment
- Information Security and Standards
- ISO7799 -Information Security Management - Code of Practice
- ISA99 - International Standards for Automation Cyber Security Standard
- Reducing Your Security Risk and Increasing Your Security Capabilities

Day Three: Cyber Security and Industrial Control Systems Management

- Information Security and Operational Technology
- Quantifying Security Risks in Commercial Context
- Establishing Cyber Security Remedial Plan
- Selecting Security Controls and Best Practice
- Commercial Considerations for Enhancing Security

Day Four: Cyber Security Controls

- Detection, Prevention and Offensive Responses.
- Securing and Assessing OPERATIONAL TECHNOLOGY Environments (OTE)
- OTE ID and Authentication Control &User Management
- OTE System Integrity & Data Confidentiality
- OTE Restricted Data Flow
- Leading Case Study

Day Five: Building a Cyber Response Plan

- Defining a Cyber Response Strategy
- How to Present a Business Case Document for Cyber Resources
- Composing Cyber Response Plan
- Cyber Response Team Compilation and Service Vendor Support
- Cyber Preparedness and Corporate Governance

With Best Regards From Abar Solutions Petroleum Consultancy

Tel. : (965) 22610021 , (965) 99600277
Fax : (965) 22630021
Email : info@abarsolutions.com , abar-solutions@hotmail.com
Wsite : www.abarsolutions.com