Learning Topic: Security Management

Course Name: 3. Advanced Security System.

Reference Code :SAF 321

Description:
Physical and Cyber threats to operational environments are on the rise, but the unique nature of those environments requires different approaches to secure them. Many organizations are finding that existing security controls are inadequate to protect critical infrastructure. To catch up to the rapidly expanding threat landscape, companies recognize a need for new skills, and are seeking better awareness and specific training security professionals.

This course provides the advanced and best practice approach in industrial security needed to covers practical concepts to ensure that security professional are well equipped to successfully fill their role, including leadership strategies, vulnerability analysis, security culture, and more.

Course Objective:

At the end of the training, successful delegates will:
- Be able to understand the fundamental issues of the Security System in industrial setting
- Develop strategies for Security Vulnerability Analysis (SVA)
- Gain a broader understanding of the principles of asset protection in the interest of the employees and visitors
- Be able to develop a comprehensive and effective departmental security plan.
- Be able to assess and deal with Insider Security Threats

Program Methodology:

This program consists of modules containing lecture content, skill assessments, participative discussions, video presentations and delegate exercises in order to create high impact training. The program is designed to be dynamic and highly interactive as well as educational. The primary focus is to provide delegates with concepts and methods which they can put to immediate use in the workplace.

Who Should attend?
Primarily aimed at personal in the field security supervisory who have accountability and responsibility for the security activity within their company, and who are seeking high level and professionalism in the field. It will also benefit executives and managers who require an insight into security professionalism

United Arab Emirates

Emirates Towers, Level 41 Sheikh Zayed Road Dubai-UAE. P.O Box 3103

Kingdom of Saudi Arabia

Khobar Gate Tower King Fahad Street , Khobar 31952

Kingdom of Saudi Arabia

101 Business Tower, 8th Floor Al Jubail 35513, Bldg# 9278 ,KSA

Course Outline:

1. **Core of Security in Industry**
   - Assessing your needs
   - Security Policy: Development and Implementation
   - Security Management
   - Protecting your system: Physical Security
   - Protecting your system: Information Security
   - Protecting your system: Software Security
   - Protecting your system: User Access Security
   - Protecting your system: Network (Internet) Security
   - Training: A necessary investment in staff
   - Relevant video
     - Video elaboration and analysis (group workshop)

2. **Security Vulnerability Assessment – SVA**
   - What does security vulnerability assessment (SVA) involve?
   - Security-sensitive areas.
   - SVA risk variables
   - Asset attractiveness
   - Threat
   - Potential security infiltrations
   - Security & vulnerability assessment methodology
   - Security vulnerability screening
   - Countermeasures analysis
   - Relevant video
     - Video elaboration and analysis (group workshop)

3. **Physical Security: Managing the Intruder**
   - Shifting security paradigms
   - An integrated view of security
   - Motive, opportunity, and means
   - Physical security controls
   - Deterrence and delay
   - Visitor control
   - Detect and detain
   - Monitoring, surveillance, and alarms
   - Non-visual detection solutions
   - Response Relevant video
     - Video elaboration and analysis (group workshop)

United Arab Emirates

Emirates Towers, Level 41 Sheikh Zayed Road
Dubai-UAE. P.O Box 3103

Kingdom of Saudi Arabia

Khobar Gate Tower
King Fahad Street , Khobar 31952

Kingdom of Saudi Arabia

101 Business Tower, 8th Floor
Al Jubail 35513, Bldg# 9278 ,KSA

4. **Mitigating Insider Threats**
   - Know and protect your critical assets
   - Develop a formalized insider threat program
   - Monitor and respond to suspicious or disruptive behavior
   - Structure management and tasks to minimize insider stress and mistakes.
   - Establish a baseline of normal behavior for both networks and employees.
   - Incorporate malicious and unintentional insider threat awareness
   - Vendor Risk Management
   - Relevant video
     - Video elaboration and analysis (group workshop)

5. **Security Management System and Plan**
   - Management policy. commitment and responsibilities
   - Threat Assessment and Analysis
   - Education and Training
   - Program Exercises and Drills
   - Threat Mitigation, Control and Response
   - Incident Review and Analysis
   - Specific Response Protocols
   - Communications
   - Relevant video
     - Video elaboration and analysis (group workshop)

Course Duration	Date	Venue	Course Fee
5 Days			

Time: 08:00 AM -03:00 PM   **Numbers of hours: 30** Hours