Telecommunications and Network Security

ME188

Course Overview:

Embark on a focused exploration of telecommunications and network security tailored for seasoned professionals. In today's digitally interconnected enterprises, ensuring secure communication and data integrity is paramount. This course empowers participants to address complex security threats, implement robust protection controls, and manage evolving risks to maintain organizational resilience in telecommunications systems.

Course Objective:

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

-Explain fundamental network security concepts in a corporate context

-Identify common network threats and assess their organizational impact

-Implement appropriate network protection controls and strategies

-Apply security principles to real-world telecom infrastructures

-Enhance incident response capabilities within their network environments

Course Outline:

Module 1: Security Principles

-Confidentiality, integrity, and availability

-Security governance and risk management

-Network security frameworks

Module 2: Security Operations

-Incident response process

-Logging and monitoring techniques

-Change and configuration management

Module 3: Common Network Threats and Attacks

-Malware, phishing, and DDoS attacks

-Insider threats and social engineering

-Threat vectors in telecom systems

Module 4: Network Protection Controls

-Firewalls and intrusion prevention systems

-Network access control

-VPNs and secure communication channels

Module 5: Telecommunications Security Architecture

-Voice and data convergence risks

-Protocols (VoIP, SIP, etc.) vulnerabilities

-Segmenting and securing telecom networks

Module 6: Secure Network Design

-Designing for security and resilience

-Defense in depth strategies

-Redundancy and failover planning

Module 7: Access Control and Identity Management

-Authentication and authorization models

-Role-based access control

-Identity lifecycle management

Module 8: Compliance and Legal Considerations

-Regulatory standards (e.g., GDPR, ISO/IEC 27001)

Training Language:

EN

Training Methodology:

The course combines various teaching methods, including instructor-led presentations, group discussions, case study analyses, and assessments through quizzes and a final exam to engage participants and ensure they understand and retain the material.

Venue | Date | Fees

Jubail | 06-07-2025 | 6,900 SAR

-Industry-specific compliance (e.g., telecom regulations)

-Legal implications of data breaches

Module 9: Case Studies in Telecom Security

-Analysis of past telecom breaches

-Lessons learned and best practices

-Response and recovery measures

Module 10: Course Review and Assessment

-Recap of key concepts

-Final knowledge assessment

-Action planning for workplace application

Who Should Attend:

-Telecom Managers

-IT Security Officers

-Network Administrators

-Cybersecurity Analysts