Security Professional: The latest Information System Security issues, concerns, and countermeasures

BTS Training & Consultancy

1st floor, Incubator Building, Masdar City, Abu Dhabi, UAE

00971-2-6452630

00971-50-6652671

info@btsconsultant.com

www.btsconsultant.com

Table of Contents:

Introduction:

This programme presents the latest Information System Security issues, concerns, and countermeasures. It comprehensively covers all the required subjects for an IT security specialist.

- Security Management Practices
- Security Architecture and Models
- Access Control Systems & Methodology
- Application Development Security
- Operations Security
- Physical Security
- Cryptography
- Telecommunications, Network, & Internet Security
- Business Continuity Planning

Who Should Attend?

This programme is intended for IT professionals, engineers, technicians and technical managers who need an intensive, thorough exposure to the principles and issues that define network security.

- People newly appointed to a security-oriented position that need to develop a functional knowledge foundation covering the many aspects of the subject
- Junior to intermediate IT and networking personnel who need an effective grounding in the scope and principles of the subject
- Individuals with responsibility in other areas of security (such as physical security) and who need to broaden their knowledge of the business with an appreciation of network and IT security

Methodology

This interactive Training will be highly interactive, with opportunities to advance your opinions and ideas and will include;

- Lectures
- Workshop & Work Presentation
- Case Studies and Practical Exercise
- Videos and General Discussions

Certificate

BTS attendance certificate will be issued to all attendees completing minimum of 80% of the total course duration.

Objectives

Participants attending this programme will:

- Evaluate where systems and networks are most vulnerable, and develop an understanding of the way in which vulnerabilities can be identified and analyzed during audit and appropriate countermeasures deployed
- Identify various types of malicious software that present a threat to safe, convenient use of tools like email and the World Wide Web - including viruses, Trojan Horse programs, worms and logic bombs
- Describe the various aspects and features of the highly complex and mathematical topic of encryption at a level of technical detail suitable to IT professionals and managers
- Develop an appreciation of trends (in both the threats and countermeasures to threats) that are evident in the industry, and put them into perspective

Outline

DAY 1:

Security Architecture and Models

- The Security Architecture and Models includes the concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment,

networks, applications and those controls used to enforce various levels of availability, integrity, and confidentiality

Access Control Systems and Methodology

- Access controls are a collection of mechanisms that work together to create a security architecture to protect the assets of the information system

DAY 2:

Application Development Security

- This topic addresses the important security concepts that apply to application software development. It outlines the environment where software is designed and developed and explains the critical role software plays in providing information system security

Operations Security

- Operations Security is used to identify the controls over hardware, media, and the operators and administrators with access privileges to any of these resources. Audit and monitoring are the mechanisms, tools, and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process

DAY 3:

Physical Security

- Physical security provides protection techniques for the entire facility, from the outside perimeter to the inside office space, including all of the information system resources

Cryptography

- Cryptography addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity

DAY 4 and 5:

Telecommunications, Network, and Internet Security

- Network Structures
- Transmission methods
- Transport formats
- Security measures used to provide availability, integrity, and confidentiality
- Authentication for transmissions over private and public communications networks and media

Business Continuity Planning

- The Business Continuity Plan (BCP) addresses the preservation and recovery of business operations in the event of outages