



مجموعة جامعة
الجميع الذكية
للتعليم القابضة



CompTIA Security+

Introductory Lecture

SY0-701

Course Outlines

By
Dr. Khaled ELMenshawy

www.midocean.ae

Lecture
Intro

LEARNING OUTCOMES

- In this course, students will implement, monitor, and troubleshoot infrastructure, application, information, and operational security.
- Identify attacks and vulnerabilities to mitigate them before they infiltrate IS.
- Establishes the core knowledge required of any cybersecurity role.
- Students will prepare for the CompTIA Security+ certification examination (SY0-701).



Dr. Khaled ELMenshawy

- *Staff member of department of Cybersecurity Department - Faculty of Informatics-Midocean University.*
- *Head of Networks Technology Department of faculty of Information Systems and Computer Science-October 6 University –Egypt*
- *Manager of Quality Assurance Unit.*
- *Manager of Huawei ICT Academy.*
- *Manager of CISCO Networking Academy.*



Attacks, Threats, and Vulnerabilities

- Compare and contrast different methods of social engineering techniques.
- Learn about potential indicators to determine the type of attack.
- Explain different threat actors, intelligence sources, and Vectors.
- Explain the security-related concerns associated with different types of vulnerabilities.
- Summarize techniques used in security assessments.
- Explain the strategies that are used in penetration testing.

Architecture and Design

- Importance of security concepts in an organization environment.
- Summarize authentication and authorization design concepts and the basics of cryptographic concepts.
- Explain the security implications of physical security.

Implementation

- Implement secure protocols, host or application security solutions, and secure network designs.
- Comprehend how to install and configure wireless security settings and how to apply cybersecurity solutions to the cloud
- Implement authentication and authorization solutions and identity and account management controls
- Understand implementing public key infrastructure (PKI).

Operations and Incident Response

- Use the appropriate tool for assessing the organizational Security.
- Learn about the importance of policies, processes, and procedures for incident response.
- How to implement mitigation techniques or controls to secure an environment.
- Explain key aspects of digital forensics.

Risk Management

- Compare and contrast different types of controls.
- Explain the necessity of standards or frameworks, applicable regulations that impact the organizational security posture.
- Summarize risk management processes and concepts.
- Explain privacy and sensitive data concepts about Security.

