Getting Started with Information Security

course outline

Information security is becoming increasingly crucial for all types of organisations. In this course, you'll explore key information-security concepts.

IS THIS COURSE FOR YOU?

This course is designed as an introductory-level information security course for anyone looking to develop an understanding of essential information security concepts.

ABOUT THE COURSE

In this course, you will learn the key concepts of different security topologies and the key role they play in network security. You will explore DevOps practices, such as continuous security and security monitoring, the benefits of using DevOps, and best practices of DevOps security. You will discover the importance of implementing security governance in an organisation.

You will examine the strengths and weaknesses of a honeypot and how it is placed in networks. (A honeypot system is configured to detect, deflect, or counteract any unauthorised attempt to gain access to information.) You will explore why pen testing is needed to ensure secure environments and investigate tools used for pen testing. And you will learn about key Advanced Persistent Threat (APT) concepts, such as defense and best practices.

You will also examine key features of network access control (NAC), the importance of NAC in a network, various NAC elements, authentication, and its implementation. You will explore key concepts related to subnetting, virtual machines (VMs), containers, and DNS security. And you will explore the common protocols in use and discover the security issues of the transmission control protocol / Internet protocol (TCP/IP) model and security protocols.

AIMS AND OBJECTIVES

This course is designed to further your introduction to core information security concepts.

PRE-REQUISITES

There are no pre-requisites for this course.

COURSE CONTENT

Module 1 - Hardened Security Topologies

Module 2 - Continual Infrastructure Testing

Module 3 - Security Governance

Module 4 - Honeypots

Module 5 - Pen Testing

Module 6 - APT Defenses

Module 7 - NACs & Gateways

Module 8 - Subnetting & DNS for Security Architects

Module 9 - Securing Networking Protocols

CAREER PATH

This course will be helpful to anyone looking to develop a foundational understanding of key information security concepts.

COURSE DURATION

20 hours. This will vary from individual to individual based on prior knowledge and ability.

Accredited cpd Centre

CPD POINTS: 20

CPD points awarded upon successful completion.

PITMAN TRAINING

Building careers for 180 years.

SPECIALISED TRAINING SINCE 1837