

CyberSecurity 102

course outline

In this second course in our series on the core elements of information security, you'll explore different ways organisations protect their information and systems from malicious activity.

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 IT security concepts.

ABOUT THE COURSE

Continuing with the foundational elements of security begun in our CyberSecurity 101 course, in this second course, you'll explore different ways organisations protect their information and systems from malicious activity.

You'll start by learning best practices in intrusion prevention and move on to the fundamentals of penetration (pen) testing. From there, you'll examine how organisations manage and analyse the results of their pen-testing activities.

AIMS AND OBJECTIVES

In this second course in our series on the core elements of information security, you'll explore the various ways organisations protect their information and systems from threats and malicious activity.

PRE-REQUISITES

While there are no formal pre-requisites for this course, it is the logical follow-on from our CyberSecurity 101 course.

COURSE CONTENT

Module 1 - Intrusion Prevention - Best Practices

Module 2 - Pen Testing Fundamentals

Module 3 - Pen Testing Awareness - Results Management

CAREER PATH

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

COURSE DURATION

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



CPD POINTS: 15

CPD points awarded upon successful completion.

