Certified Security Principles

Description:

Security Principles are your first line of defense, but often the last box checked! The IT world never stands still! Therefore, neither can IT security. It does not matter if we are talking about the implementation of IoT devices or cloud services, security is important. According to a recent study, the top source of security incidents within a company are the current employees!

The Certifed Security Principles, C)SP, course is going to prepare you for security across the entire environment including understanding risk management, identity and access control, network and data security. This is just a short list of everything that we cover within this course, which will include new technologies like IoT and cloud services. This course is intended to prepare you to become a benefit to any company that is attempting to improve its security posture!

The C)SP is a Foundational Part of Several Career Paths

We suggest that you master the concepts in the C)SP before moving into 300 level in the Management, Response and Recovery, or Auditing Career Paths. This course will introduce you to many of the key concepts you will need to succeed in the other courses.

Key Course Information

Live Class Duration: 5 Days
CEUs: 40
Language: English
Class Formats Available:

Instructor Led

Self-Study

Live Virtual Training

Suggested Prerequisites:

- 12 Months of experience with server administration
  Or
- Mile2 C)SA1, C)SA2, C)HT, C)OST and C)NP
  Or
- Equivalent Knowledge

Modules/Lessons

Module 1 - Intro to IT Security
Module 2 - Risk Management
Module 3 - Understanding of Cryptography
Module 4 - Understanding Identity and Access Management
Module 5 - Managing Data Security
Module 6 - Managing Network Security
Module 7 - Managing Server/Host Security
Module 8 -Application Security for Non-Developers
Module 9 – Understanding Mobile Device Security
Module 10 – Managing Day to Day Security
Module 11 – Understanding Compliance and Auditing

Who Should Attend

- IT Professionals
- Server Administrators
- Virtualization and Cloud Administrators

Accreditations

www.mile2.ca 403 Bank St Ottawa, ON K2P 1Y6 613-416-8898

Upon Completion

Upon completion, the Certified Security Principles candidate will not only be able to competently take the C)SP exam but will also understand the principle security knowledge to keep companies' IP and IT infrastructure safe.

Exam Information

The Certified Security Principles exam is taken online through Mile2's Learning Management System and is accessible on you Mile2.com account.

A minimum grade of 80% is required for certification.

Re-Certification Requirements

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

1) Pass the most current version of the exam for your respective existing certification
2) Earn and submit 20 CEUs per year in your Mile2 account.

Course FAQ's

Question: Do I have to purchase a course to buy a certification exam?

Answer: No

Question: Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at www.mile2.com.

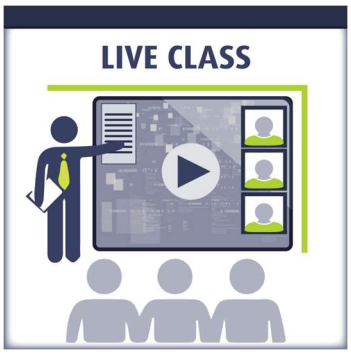
Question: Are all courses available as self-study courses?

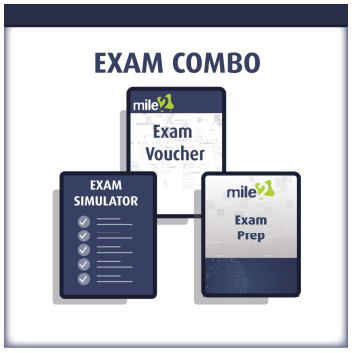
Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

Course and Certification Learning Options





www.mile2.ca 403 Bank St Ottawa, ON K2P 1Y6 613-416-8898

Detailed Outline:

Course Introduction

Module 1 – Introduction to IT Security

a. Understanding Security
b. Responsibilities
c. Building a Security Program
d. CIA Triad
e. Governance, Risk, Compliance
f. State of Security Today

Module 2 – Risk Management

a. Risk Management
b. Risk Assessment
c. Types of Risk, Threats and Vulnerabilities
d. Mitigating Attacks
e. Discovering Vulnerabilities and Threats
f. Responding to Risk

Module 3 – Understanding of Cryptography

a. Understanding Cryptography
b. Symmetric Encryption
c. Asymmetric Encryption
d. Hashing
e. PKI
f. Cryptography in Use

Module 4 – Understanding Identity and Access Management

a. Identity Management
b. Authentication Techniques
c. Single Sign-on
d. Access Control Monitoring

www.mile2.ca 403 Bank St Ottawa, ON K2P 1Y6 613-416-8898

Module 5 – Managing Data Security

a. Virtualization Principles
b. Key Components Mapped to Cloud Layer
c. Key Security Concerns
d. Other Technologies Used in the Cloud
e. The Layers
f. Relevant CCM Controls

Module 6 – Data Security

a. Different Types of Storage
b. Encryption Options
c. Data Management

Module 7 – Managing Server/Host Security

a. The Operating Systems
b. Hardening the OS
c. Physical security
d. Virtualization and Cloud Technologies

Module 8 – Application Security for Non-Developers

a. Application Security Principle
b. Software Development Life Cycle
c. OWASP Top 10
d. Hardening Web Applications
e. Patch/Update/Configuration Management

Module 9 – Understanding Mobile Device Security (IoT)

a. What Devices are we talking about?
b. What is the risk?
c. Hardening Mobile/IoT Devices
d. Corporate Management

Module 10 – Managing Day to Day Security

a. Company Responsibilities
b. Product Management
c. Business Continuity Basics

www.mile2.ca 403 Bank St Ottawa, ON K2P 1Y6 613-416-8898

d. Incident Response
e. Why Train?

Module 11 – Understating Compliance and Auditing

a. Benefits of Compliance
b. Assurance Frameworks
c. What is Auditing