PECB BEYOND RECOGNITION

PECB Certified Cybersecurity Essentials

Start building your career in Cybersecurity by gaining an essential knowledge on Cybersecurity, including how to anticipate threats, protect systems and networks.

Why should you attend?

This training course has been designed to prepare anyone to become a cybersecurity professional. The content of this training course represents the essentials of Cybersecurity, and it is designed in the way that the capabilities learned by following this training course will be used to protect organizations and the society as a whole from areas of emerging threats. Throughout this training, you will gain a comprehensive knowledge on Cybersecurity based on the best practices, the relationship between Cybersecurity and other types of IT Securities, the identification of processes that are the most vulnerable to cyber-attacks, and so on. Participants will gain an insight into the fundamental Cybersecurity principles, Risk Management, Security Architecture and Controls, Incident Management, Cryptography and Operations Security, etc.

In addition to the training, participants will have access to exams in order to receive an internationally recognized certification that will validate their Cybersecurity skills and prepare them to successfully enter or advance in the labor market.

Who should attend?

This course is aimed at all the individuals who want to guide their future professional career in the area of Cybersecurity. It is not important whether you are a student, manager, engineer, IT administrator, systems administrator etc., this is a training course for everyone who wants to expand his or her professional knowledge in this area.

Course agenda

Duration: 10 days

Day 1 | Introduction to Information Security

- Section 01: Course objectives and structure
- Section 02: Fundamental concepts in cybersecurity
- Section 03: Fundamental principles and concepts
- Section 04: Threats and malware
- Section 05: Cybersecurity components
- Section 06: Information security policies
- Section 07: Organization of information security
- Section 08: Information security for supplier relationships

Day 2 | Information Security Risk Management

- Section 09: Information security risk management based on ISO/IEC 27005
- Section 10: EBIOS risk assessment methodology
- Section 11: MEHARI risk assessment methodology
- Section 12: OCTAVE risk assessment methodology

Day 3 | Day 3: Asset Security, Identity and Access Management

- Section 13: Human resources security
- Section 14: Asset management
- Section 15: Identity and access management

Day 4 | Cryptography and Operations Security

- Section 16: Cryptography
- Section 17: Operations security
- Section 18: Logging and monitoring

Day 5 | Day 5: Physical Security & Mid-Course Exam

- Section 19: Physical security
- Section 20: Equipment security

Day 6 | Communications and Network Security

- Section 21: Network architecture
- Section 22: Network controls
- Section 23: Security of network and wireless services
- Section 24: Segregation in networks
- Section 25: Information transfer

Day 7 | Incident Management and Business Continuity

- Section 26: Business continuity
- Section 27: Incident management
- Section 28: Incident response and forensics

Day 8 | Data Protection and Security

- Section 29: The legal aspect of cybersecurity
- Section 30: Protection of personal data
- Section 31: Privacy by design
- Section 32: Personal data protection controls

Day 9 | Cloud Security

- Section 33: Fundamental concepts and definitions of cloud security
- Section 34: Cloud computing risks
- Section 35: Key security aspects in cloud environment
- Section 36: Cloud computing controls

Day 10 | Software Development Security and Acquisition & Certification Exam

- Section 37: Fundamental concepts of software development security
- Section 38: Software development lifecycle
- Section 39: Software application attacks and controls
- Section 40: Closing the training

Learning objectives

- Understand and acquire comprehensive knowledge on the main concepts of cybersecurity and the relationship between cybersecurity and other types of IT securities
- Explain the goal and content of different standards and other best practices related to cybersecurity and information security
- Master concepts and fundamental cybersecurity principles, risk management, network security, incident management, cloud security, software development security, etc.
- Obtain the expertise required in order to be able to build a career in cybersecurity

Examination

Duration: 3 hours

The "PECB Certified Cybersecurity Essentials" exam meets all the requirements of the PECB Examination and Certification Program (ECP). The exam covers the following competency domains:

Domain 1	Fundamental principles and concepts of information security
Domain 2	Information security risk management
Domain 3	Asset security & identity and access management
Domain 4	Cryptography & operations security
Domain 5	Physical security
Domain 6	Communications and network security
Domain 7	Incident management & business continuity
Domain 8	Data protection and security
Domain 9	Cloud security
Domain 10	Software development security and acquisition

For more information about exam details, please visit Examination Rules and Policies.

Certification

After successfully completing the exam, you can apply for the credential shown on the table below.
You will receive a certificate once you comply with all the requirements related to the selected credential.

For more information about PECB Cybersecurity Essentials certification and the PECB certification process, please refer to the Certification Rules and Policies.

Credential	Exam	Professional experience	Cybersecurity experience	Other requirements
PECB Certified Cybersecurity Essentials	PECB Certified Cybersecurity Essentials exam	None	None	Signing the PECB Code of Ethics

General information

- Certification fees are included on the exam price
- Training material containing over 1000 pages of information and practical examples will be distributed to participants
- A participation certificate of 62 CPD (Continuing Professional Development) credits will be issued
- In case of exam failure, you can retake the exam within 12 months for free