



# "كيف تصبح خبيراً في قيادة أمن المعلومات المتقدمة: الدورة الاحترافية في السيبرانية"

**Duration:** 5 Days

**Language:** ar

**Course Code:** PI1 - 132

## Objective

:Upon completion of this course, participants will be able to

- Develop a deep understanding of cybersecurity principles and best practices.
  - Master risk management and mitigation strategies.
  - Navigate the complexities of legal and regulatory compliance.
  - Design and implement comprehensive security programs.
  - Enhance incident response and recovery capabilities.
  - Prepare for the CISSP certification exam.

## Audience

:This course is intended for

- Senior IT and cybersecurity professionals.
- Chief Information Security Officers (CISOs).
  - IT security consultants and managers.
  - Network security engineers.
- Information assurance analysts.

## Training Methodology

This course uses a variety of adult learning styles to aid full understanding and comprehension. Including

- Interactive lectures and discussions.
- Real-world case studies and examples.
- Group projects and collaborative exercises.
- Hands-on training with cybersecurity tools and frameworks.

## Summary

This comprehensive course equips participants with the expertise to lead and manage cybersecurity initiatives within organisations. Emphasising strategic and operational aspects, the course covers risk management, legal and regulatory compliance, and incident response. Through interactive sessions, case studies, and practical exercises, participants will develop the skills to design robust security frameworks, ensure data protection, and respond effectively to cyber threats.

## Course Content & Outline

### **Section 1: Introduction to Cybersecurity and Leadership**

- Overview of the cybersecurity landscape
- Leadership roles in cybersecurity
- Case studies on cybersecurity breaches and responses

### **Section 2: Risk Management and Governance**

- Principles of risk management

- Developing and implementing security policies •
- Legal, regulatory, and compliance frameworks •

### **Section 3: Security Architecture and Engineering**

- Designing secure systems and networks •
- Security models and frameworks •
- Secure software development practices •

### **Section 4: Identity and Access Management**

- Authentication and authorisation methods •
- Identity lifecycle management •
- Implementing access control measures •

### **Section 5: Security Operations and Incident Management**

- Monitoring and detecting security incidents •
- Incident response planning and execution •
- Business continuity and disaster recovery •

### **Section 6: Exam Preparation and Review**

- Review of key CISSP domains •
- Mock exams and practice questions •
- Exam strategies and tips •

## **Certificate Description**

عند إتمام هذه الدورة التدريبية بنجاح، سيحصل المشاركون على شهادة إتمام التدريب من Holistique Training. وبالنسبة للذين يحضرون ويكملون الدورة التدريبية عبر الإنترنت، سيتم تزويدهم بشهادة إلكترونية (e-Certificate) من Holistique Training.

وخدمة اعتماد التطوير المهني (BAC) معتمدة من المجلس البريطاني للتقييم Holistique Training شهادات

ISO 29993. ISO 9001 أو ISO 21001 كما أنها معتمدة وفق معايير (CPD) المستمر.

لهذه الدورة من خلال شهادتنا، وستظهر هذه النقاط على شهادة إتمام (CPD) يتم منح نقاط التطوير المهني المستمر واحدة عن كل ساعة CPD يتم منح نقطة، ووفقاً لمعايير خدمة اعتماد Holistique Training. التدريب من لأي دورة واحدة نقدمها حالياً CPD حضور في الدورة. ويمكن المطالبة بحد أقصى قدره 50 نقطة.

## Categories

تطبيقات تكنولوجيا المعلومات والكمبيوتر، التكنولوجيا، الاتصالات

## Related Articles



### Top 10 Cybersecurity Courses And Training Programs

In today's digital era, mastering cybersecurity is vital. Courses like CISSP, CEH, and CISM cover security fundamentals, risk management, access control, and software security. They prepare professionals for certifications, incident handling, identity management, compliance, and resilient application development, ensuring robust protection of digital assets.