

Advanced Cybersecurity Leadership

Duration: 5 Days

Language: en

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

Upon successful completion of this training course, delegates will be awarded a Holistique Training Certificate of Completion. For those who attend and complete the online training course, a Holistique Training e-Certificate will be provided.

Holistique Training Certificates are accredited by the British Assessment Council (BAC) and The CPD Certification Service (CPD), and are certified under ISO 9001, ISO 21001, and ISO 29993 standards.

CPD credits for this course are granted by our Certificates and will be reflected on the Holistique Training Certificate of Completion. In accordance with the standards of The CPD Certification Service, one CPD credit is awarded per hour of course attendance. A maximum of 50 CPD credits can be claimed for any single course we currently offer.

Categories

IT & Computer Application, Technology, Telecommunication

Tags

Cyber security, Cybersecurity

Related Articles



Top 10 Cybersecurity Courses and Training Programs

Master cybersecurity with top courses like CISSP, CEH, and CISM. Learn risk management, incident response, compliance, and digital asset protection