CISSP - CISSP - Certified Information Systems Security Professional

CISSP - CISSP - Cyber Security

Durata:	Lingue:	Certificazione:
5 Giorni	**Italiano**	**-**

Descrizione del corso

This course aims to supply delegates with a theory-based approach to learning the Information Systems security process and how to apply this process practically to real-life scenarios. The course is based around teaching the eight fundamental domains of Information Security, which provide delegates with all the information they require to obtain a broad understanding of Information Security and pass the CISSP exam. The CISSP certification is globally recognised as the best Information Systems Security certification for Security Professionals. Our trainers use a theory-based training strategy, allowing for a clear explanation of CISSP terminology and methodology. Delegates can easily gain a comprehensive knowledge of the Information Security process by attending this course. The content of this course is largely centred on the eight fundamental domains of Information Security, which encompass everything delegates need to know about the topic. Despite being wholly theory-based, the CISSP certification emphasises the necessità of practically applying what is learned and effectively trains delegates to do this. Hence, by the end of the course, delegates will have acquired the knowledge and skills required to be able to design, develop, apply, and manage a security program to prevent malicious cyber-attacks. Thus, these individuals become greatly desirable for employers and can greatly improve their employabilità prospects. Certified Information Systems Security Professionals are crucial additions to the team as they can prevent the occurrence of a number of potentially harmful attacks to a business's systems. Corso erogato in collaborazione con ISC2 Italy chapter

Programma

Security and Risk Management:

•Confidentiality, Integrity, and availability Concepts

ITCore Group

Via Balestra, 12
6900 Lugano (CH)
+41.091.9760019
www.itcoregroup.com

Via Lanino, 36
21047 Saronno (VA)
+39.02.84108669
www.itcoregroup.com

•Security Governance Principles
•Compliance
•Legal and Regulatory Issues
•Professional Ethics
•Security Policies, Standards, Procedures, and Guidelines

Asset Security:
•Information and Asset Classification
•Ownership
•Protect Privacy
•Appropriate Retention
•Data Security Controls
•Handling Requirements

Security Architecture and Engineering:
•Engineering Processes using Secure Design Principles
•Security Models Fundamental Concepts
•Security Evaluation Models
•Security capabilityes of Information Systems
•Security Architectures, Designs, and Solution Elements Vulnerabilitàes
•Web-based Systems Vulnerabilities
•Mobile Systems Vulnerabilities
•Embedded Devices and Cyber-Physical Systems Vulnerabilitàes
•Cryptography
•Site and Facility Design Secure Principles
•Physical Security

Communication and Network Security:
•Secure Network Architecture Design
•Secure Network Components
•Secure Communication Channels
•Network Attacks

Identity and Access Management (IAM):
•Physical and Logical Assets Control
•Identification and Authentication of People and Devices
•identity as a Service
•Third-party identity Services

•Access Control Attacks
•identity and Access Provisioning Lifecycle

Security Assessment and Testing:
•Assessment and Test Strategies
•Security Process Data
•Security Control Testing
•Test Outputs
•Security Architectures Vulnerabilitàes

Security Operations:
•Investigations Support and Requirements
•Logging and Monitoring Activities
•Provisioning of Resources
•Foundational Security Operations Concepts
•Resource Protection Techniques
•Incident Management
•Preventative Measures
•Patch and Vulnerabilità Management
•Change Management Processes
•Recovery Strategies
•Disaster Recovery Processes and Plans
•Business Continuity Planning and Exercises
•Physical Security
•Personnel Safety Concerns

Software Development Security:
•Security in the Software Development Lifecycle
•Development Environment Security Controls
•Software Security Effectiveness
•Acquired Software Security Impact