

Cybersecurity Professional

Duration: 5 Days

Language: en

Course Code: PI1-127

Objective

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

- Understand security fundamentals, risk assessments, controlling access, securing software development, and related concepts.
- Adequately prepare for the CISSP certification assessment, empowering participants with the understanding and assurance needed to excel in their certification pursuit.
- Be proficient in crafting robust security frameworks, handling security incidents, and recovering from breaches while adhering to legal and regulatory standards.
- Develop expertise in managing identity and access, ensuring secure verification and authorisation, and managing identities throughout their lifecycle.
- Acquire competencies in security operations, encompassing monitoring, responding to incidents, and ensuring compliance, alongside understanding secure methodologies for software development to build resilient applications.

Audience

This course is designed for anyone responsible for reducing organisational security risks. It would be most beneficial for:

- IT Specialists
- IT Managers
- Risk Managers
- Security Awareness Managers
- Business Owners
- Department Managers
- Operations Managers
- Systems Managers
- Developers

Training Methodology

This course uses a variety of adult learning styles to aid full understanding and comprehension. Participants will watch videos to highlight the importance of cybersecurity process implementation and understand, through real-world case studies, what could happen if cybersecurity is not taken seriously.
They will then undertake group activities and discussions to understand how robust their cybersecurity is within their organisation and develop plans to increase the security of their systems and data.

Summary

The job role of a cybersecurity professional is crucial in safeguarding an organisation's digital assets, infrastructure, and sensitive information from cyber threats. These professionals are tasked with identifying vulnerabilities, implementing protective measures, and responding to security incidents to mitigate risks effectively. With cyberattacks becoming increasingly frequent and sophisticated, cybersecurity professionals' role has become indispensable for organisations' future viability and success. They are pivotal in maintaining customer trust, protecting intellectual property, ensuring regulatory compliance, and preserving the organisation's reputation. As technology continues to advance and cyber threats evolve, the

demand for skilled cybersecurity professionals will only grow. Their role is essential for securing the future of any organisation in an increasingly digital world.

Course Content & Outline

Section 1: CISSP & Other Security Concepts

- Introduction to CISSP (Certified Information Systems Security Professional).
- Fundamentals of cybersecurity.
- Network security principles.
- Cryptography essentials.
- Access control mechanisms.
- Security architecture and design.
- Software development security.
- Security operations and incident response.
- Risk management concepts.
- Legal, regulatory, and ethical considerations in security.
- Security testing and assessment techniques.
- Emerging technologies in cybersecurity.
- Integration of security concepts into organisational practices.

Section 2: The Importance of Cybersecurity

- Understanding the significance of cybersecurity in modern society.
- Identifying cyber threats and their potential impacts.
- Exploring cybersecurity best practices for individuals and organisations.
- Recognising the role of cybersecurity in protecting personal and sensitive information.
- Examining the economic and reputational consequences of cyber attacks.
- Discussing legal and regulatory frameworks relevant to cybersecurity.
- Highlighting the importance of cybersecurity in safeguarding critical infrastructure.
- Addressing the challenges and opportunities in the cybersecurity landscape.
- Promoting cybersecurity awareness and education initiatives.
- Emphasising the need for proactive cybersecurity measures in an interconnected world.

Section 3: Asset Security Management

- Asset identification and classification methodologies.
- Risk assessment and management for assets.

- Implementing access controls to safeguard assets.
- Physical security measures for protecting assets.
- Data encryption and protection techniques.
- Asset lifecycle management strategies.
- Security awareness and training for asset management.
- Incident response and recovery procedures for asset security breaches.
- Compliance with asset security regulations and standards.

Section 4: Network Security & Communication Strategies

- Network access control mechanisms and strategies.
- Intrusion detection and prevention systems.
- Secure configuration and management of network devices.
- Virtual private network (VPN) technologies and implementation.
- Wireless network security considerations.
- Network security monitoring and incident response procedures.
- Security best practices for cloud-based networks.
- Role of encryption in securing network communications.

Section 5: Identity & Access Management (IAM)

- Role-based access control (RBAC) implementation.
- Single sign-on (SSO) solutions and federated identity management.
- Identity lifecycle management strategies.
- Multi-factor authentication (MFA) techniques.
- Identity governance and compliance considerations.
- Privileged access management (PAM) principles.
- Identity theft prevention measures.
- Emerging trends and challenges in IAM.

Section 6: Penetration Testing & Software Development

- Understanding software development lifecycle (SDLC).
- Integrating security into each phase of SDLC.
- Identifying vulnerabilities in software applications.
- Penetration testing tools and techniques.
- Conducting code reviews for security vulnerabilities.
- Secure coding best practices.
- Automated and manual penetration testing approaches.
- Reporting and remediation of security findings.
- Continuous integration and deployment security.
- DevSecOps principles and practices.

Section 7: Security Operations Best Practices

- Incident detection and response strategies.
- Security information and event management (SIEM) implementation.
- Security incident management processes.
- Threat intelligence gathering and analysis.
- Security orchestration, automation, and response (SOAR).
- Vulnerability management techniques.
- Log management and monitoring practices.
- Incident response planning and exercises.

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

Tags

Cybersecurity, Asset Security, CISSP

Related Articles



Importance of Cyber Security

YouTube Video

https://www.youtube.com/embed/I_fLHTwrcnE?si=-xl7TiYT3wNj4eOG