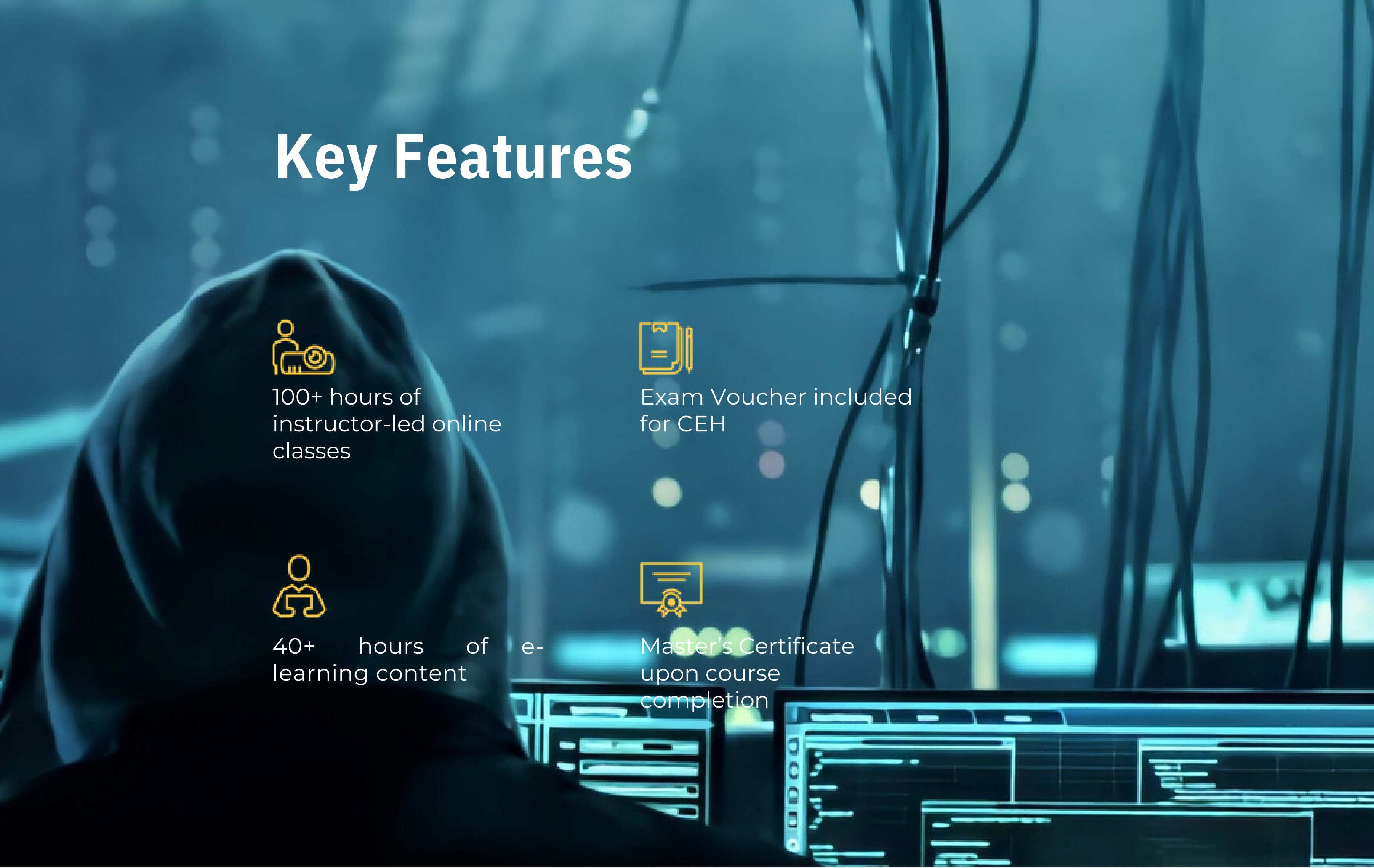
CK Solutions

CYBER SECURITY COURSE

About the Course

The Cyber Security Master’s Program will equip you with the full range of skills needed to become an expert in this rapidly growing domain. You will learn comprehensive approaches to protecting your infrastructure, including securing data and information, running risk analysis and mitigation, architecting cloud- based security, achieving compliance and much more with this best-in-class program.



Key Features

- 100+ hours of instructor-led online classes
- Exam Voucher included for CEH
- 40+ hours of e-learning content
- Master's Certificate upon course completion

About Cks solutions

Cks is the world's #1 online bootcamp provider that enables learners through rigorous and highly specialized training. We focus on emerging technologies and processes that are transforming
the digital world, at a fraction of the cost and time as traditional approaches.

Program Outcomes

- Install, configure and deploy public key infrastructure and network components while assessing and troubleshooting issues to support organizational security
- Master advanced hacking concepts to manage information security efficiently
- Design security architecture and framework for a secure IT operation
- Frame cloud data storage architectures and security strategies, and utilize them to analyze risks
- Protect data movement, perform disaster recovery, access CSP security and manage client databases
- Implement technical strategies, tools, and techniques to secure data and information for your organization
- Adhere to ethical security behaviour for risk analysis and mitigation
- Understand security in cloud computing architecture in depth
- Comprehend legal requirements, privacy issues and audit process methodologies within the cloud environment
- Focus on IT compliance and the integrity of enterprise systems to establish a more secure enterprise IT framework

Introduction to Cyber Security

Cks Solutions Introduction to Cyber Security course for beginners is designed to give you a foundational look at today's cybersecurity landscape and provide you with the tools to evaluate and manage security protocols in information processing systems.

Key Learning Objectives

- ✓ Gain a comprehensive overview of cyber security principles and concepts
- ✓ Learn the challenges of designing a security program
- ✓ Develop and manage an information security program, perform business impact analysis, and carry out disaster recovery testing

Course Curriculum

- ✓ Lesson 1 - Course Introduction
- ✓ Lesson 2 -Cyber Security Fundamentals
- ✓ Lesson 3 -Enterprise Architecture and Components
- ✓ Lesson 4 -Information System Governance and Risk Assessment
- ✓ Lesson 5 - Incident Management

CompTIA Security+ (SY0-601)

The CompTIA Security+ course will enable learners to gain knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; operate with an awareness of applicable policies, laws, and regulations. Upon successfully validating their skills by passing the certification exam learners will be able to perform these tasks to support the principles of confidentiality, integrity, and availability. CompTIA Security+ meets the ISO 17024 standard and is approved by the U.S.

Key Learning Objectives

- ✓ Comprehend risk identification and mitigation
- ✓ Provide operational, information, application and infrastructure level security
- ✓ Secure the network to maintain the availability, integrity and confidentiality of critical information
- ✓ Operate within a set of rules, policies and regulations wherever applicable

- ✓ Lesson 1 - Lesson 01 - Learn about networking, firewalls, LAN security, IDS, NAC, IPSec
- ✓ Lesson 02 - Understand the principles of security, risk management, data classification, disaster recovery, and forensics
- ✓ Lesson 03 - Comprehend cyber attacks, DNS security, social engineering fundamentals, buffer overflows, security testing tools usage, honeypots, vulnerability and pen testing

- ✓ Lesson 04 - Learn how to handle bugs, secure storage platforms and the power grid, how to hack IOT
- ✓ Lesson 05 - Get familiar with access controls, Kerberos, identity federation, and id governance
- ✓ Lesson 06 - Encryption, advanced cryptography, crypto algorithm, PKI, etc are covered in this lesson

CEH (v12)- Certified Ethical Hacker

The Cks Solutions CEH v12 Certified Ethical Hacker training (earlier CEH v11) and certification course provide hands-on classroom training to help you master the same techniques that hackers use to penetrate network systems and leverage them ethically to protect your own infrastructure. The extensive course focuses on 20 of the most popular security domains to provide a practical approach to essential security systems.

Key Learning Objectives

After completing this course you will be able to:

Ace the CEH practical exam

Learn to assess computer system security by using penetration testing techniques

Scan, test and hack secure systems and applications, and gain hands-on experience with sniffing, phishing and exploitation tactics

Course Curriculum

Module 01: Introduction to Ethical Hacking - Overview of information security, threats, attack vectors, ethical hacking concepts, information security controls, penetration testing concepts, and information security laws and standards are covered in this module

Module 02: Footprinting and Reconnaissance - These modules cover concepts and types of footprinting, footprinting through search engines, web services, and social networking sites, footprinting tools, countermeasures, and footprinting pen testing

- MSocdaunlnei n0g3 :N etworks - Learn about network scanning concepts, tools and techniques, network diagrams, and scanning pen testing

- Module 04: Enumeration - Enumeration concepts, types, techniques, and pen testing are covered in this module

- Module 05: Vulnerability Analysis - Overview of vulnerability assessment concepts, solutions, scoring systems, tools, and reports are explained in this module

- Module 06: System Hacking - Learn how to crack passwords, hide files, cover tracks, any many more

- Module 07: Malware Threats - This module gets you familiar with malware concepts, trojan concepts, malware analysis, countermeasures, malware penetration testing

- Module 08: Sniffing - Sniffing concepts, tools, and techniques are explained in this module

- MSoodcuialle E 0n9g: ineering - Comprehend social engineering concepts, techniques, countermeasures, and pen testing

- Module 10: Denial-of-service - Dos/DDoS concepts, techniques, tools, case studies, and penetration testing are covered in this module

- Module 11: Session Hijacking - Know what is session hijacking and its types, tools, countermeasures, and session hijacking penetration testing

- Module 12: Evading IDS, Firewalls, and Honeypots - Learn about firewalls and honeypots and how to detect and evade them

- Module 13: Hacking Web Servers - This module focuses on web server concepts, attacks, methodologies, tools, countermeasures, and penetration testing

- ✓ Module 14: Hacking Web Applications - Web app concepts, tools, methodologies, countermeasures, and penetration testing are covered in this module

- ✓ Module 15: SQL Injection - Get familiar with SQL Injection concepts, types, tools, methodologies, countermeasures, and penetration testing

- ✓ Module 16: Hacking Wireless Networks - Wireless concepts, threats, methodologies are covered in this module

- ✓ Module 17: Hacking Mobile Platforms - Learn how to hack android IOS, Mobile spyware, device management, security tools, and many more in this module

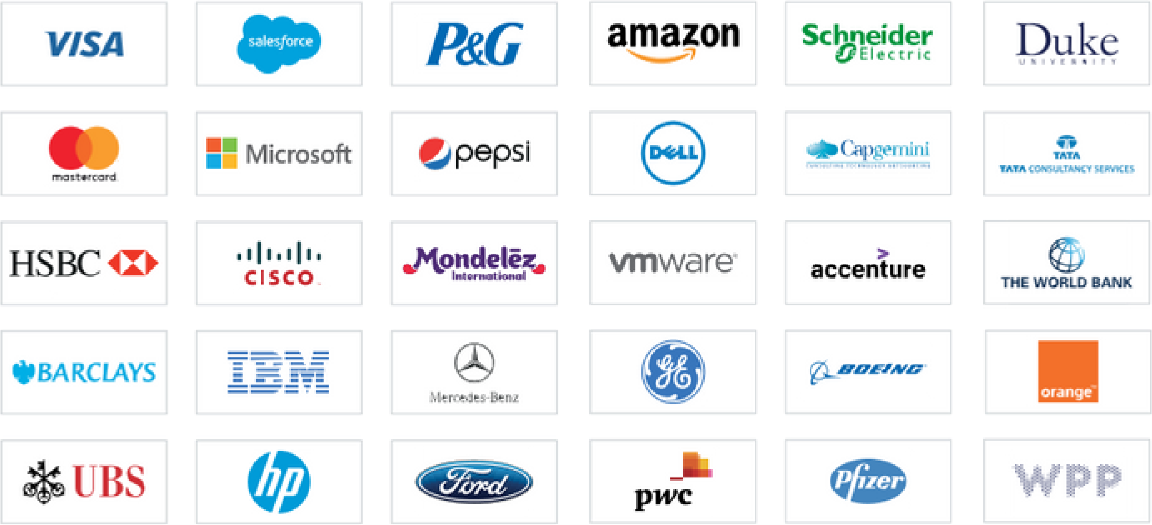
- ✓ Module 18: IoT Hacking - This module covers IoT Hacking concepts, attacks, methodologies, tools, countermeasures, and penetration testing

- ✓ Module 19: Cloud Computing - Concepts, attacks, methodologies, tools, countermeasures, and penetration testing of cloud computing are covered in this module

- ✓ Module 20: Cryptography - This module will teach you about cryptography concepts, encryption algorithms, tools, PKI, types of encryption, cryptanalysis, and countermeasures

Corporate Training

Top clients we work with:



100 % PLACEMENT PROGRAMME

CK
Solutions

124 road London England Ec 1v2nx
Mobile no. +12133 010384
Email :support@ckssolutions.co.uk