Assured Service Provider

in association with National Cyber Security Centre

Training Course

APMG International

HUMAN RED TEAM

A DIVISION OF SYNOVUM CYBER SECURITY

ETHICAL SOCIAL ENGINEERING ADVANCED

Master the Skills of Defending Against Human-Centric Cyber Threats

In the world of cyber security, technology is only part of the battle. **Social Engineering**, the manipulation of individuals into revealing sensitive information or performing actions that compromise security, has become a key method for attackers to bypass even the most sophisticated technical defences.

Human vulnerabilities are often regarded as the weakest link in any security system, making social engineering one of the most important areas to address in modern cyber security strategies.

Why Social Engineering is a Critical Area of Cyber Security

- **Exploiting Human Weaknesses**: No matter how secure your organisation's firewalls or software might be, attackers know that **humans are often the easiest target**. By exploiting trust, fear, or curiosity, cybercriminals can manipulate employees into giving up sensitive data or access, completely bypassing complex technological barriers.
- **Growing Attack Vector**: **Phishing, vishing, pretexting, baiting**, and other forms of social engineering attacks have surged, affecting organisations of all sizes. These tactics are often the entry point for more complex technical attacks.
- **Difficult to Defend Against**: Unlike traditional cyber security threats that often rely on technical vulnerabilities, social engineering targets **human behaviour**. This makes it harder to detect, prevent, and mitigate without proper training and education.
- **High-Profile Breaches**: Some of the most devastating security breaches and attacks in recent years have been traced back to social engineering attacks, proving that even the most well-defended organisations are vulnerable when the human element is exploited.

Course Overview

This hands-on, practitioner-level course, assured by the UK's **National Cyber Security Centre** (NCSC), has been designed for industry professionals who want to understand, ethically simulate, and be able to defend against these attacks in order to strengthen their organisation's cyber security posture. Utilising industry and academic source materials, the course equips delegates with the knowledge and skills to conduct ethical social engineering activities and identify key areas of human risk within organisations.

Through comprehensive learning sessions, completion of practical/interactive exercises and review of real-world case studies, delegates will understand how threat actors exploit human psychology through the use of multiple social engineering techniques, and how to use these same techniques for ethical defence purposes.

Course Benefits

By attending this course, delegates will become key assets to their organisation, be equipped to mitigate the risks from social engineering attacks, and ensure that their organisation's security infrastructure accounts for the human factor.

Delegates will also be able to design and implement more robust employee training programmes, identify hidden people-based vulnerabilities, and strengthen their organisation's defence against cyber threats.

Predict, Prevent, Protect: Master Ethical Social Engineering

training@synovum.co.uk

www.synovum.co.uk

www.humanredteam.com

@syncybersec

@humanredteam

Key Learning Objectives

- **Understand Advanced Social Engineering Tactics**: Dive deep into the techniques used by attackers, including phishing, vishing, pretexting, baiting, and more.
- **Ethically Conduct Social Engineering Engagements**: Learn how to safely simulate attacks within your organisation to test vulnerabilities without compromising trust.
- **Identify and Mitigate Human Vulnerabilities**: Recognise common psychological triggers that attackers exploit and develop strategies to address these risks.
- **Develop a Comprehensive Human-Centric Security Strategy**: Integrate social engineering defences into your organisation's overall cyber security strategy, emphasising employee education and training.

Why Attend?

- **Protect Your Organisation**: Delegates will gain the skills to proactively defend their organisation against the growing threat of social engineering attacks.
- **Practical Expertise**: Hands-on exercises will prepare delegates to simulate real-world social engineering scenarios, helping their organisation identify weak points before attackers do.
- **Stay Ahead of Threats**: As social engineering tactics evolve, this course ensures delegates are up to date with the latest threats and defence techniques.
- **Earn a Practitioner-Level Certification**: Upon successful completion of the course and all assessment elements, delegates will be awarded the ***Certified Professional-Ethical Social Engineer*** (CP-ESE®) certification, demonstrating advanced levels of understanding and practical implementation of ethical social engineering practices.

Who Should Attend?

- **Security/IT Professionals** seeking advanced knowledge and skills in ethical social engineering.
- **Penetration Testers** looking to add ethical social engineering techniques to their toolbox.
- **IT Managers and Cyber Security Leaders** aiming to improve their organisation's human defence strategies.
- **Law Enforcement Professionals** wanting to advance their skills in practical influence/persuasion and elicitation tactics.
- **Academics** studying the field of human psychology in relation to cyber security.

Course Duration

- 5 Days (practical exercises will also be undertaken on the evenings of days 1-4).

Assessment

To gain the **internationally–recognised** APMG certification as a *Certified Professional - Ethical Social Engineer* (CP-ESE®), delegates will be required to pass all three assessment elements:

- 125-question (2.5 hours) multiple-choice exam.
- Non-verbal communication/micro expressions assessment.
- 1-hour viva voce assessment.

Successful candidates will receive a **APMG** certificate and separate **Credly** certification badge. Following receipt of their initial certification, candidates will be required to re-certify every two years to maintain their active CP-ESE® certification.

Delegate Pack

- Electronic version of the *Ethical Social Engineering-Advanced* delegate manual.
- Electronic version of the *Social Engineering Engagement Framework (SEEF)* manual.
- One-year access to online micro-expressions training tool/assessment.
- Exam & viva voce voucher.

Enhance your expertise in one of the most crucial areas of cyber security by attending this **NCSC Assured** training course.

Get in touch with us to find out more.

Predict, Prevent, Protect: Master Ethical Social Engineering

training@synovum.co.uk

www.synovum.co.uk

www.humanredteam.com

@syncybersec

@humanredteam