OSINT – Advanced Skills for CISOs

The Risk and The Fix

CYBER

Designed for

- CISOs and senior technical teams.

Benefits of attending

- Understand how an attacker uses OSINT (open source intelligence) to obtain corporate data and personal details using nothing more than search engines and free, legal tools
- Equip teams with tools and techniques to perform investigations of targets in the preparation for a notional attack, essentially becoming the hacker to demonstrate just how easy those attacks often are due to the visibility of staff and corporate data online
- Create a cyberattack response plan - the blueprints of the towering inferno

Learning Objectives

- Cyber risk in the real-world
- Attackers and their methods
- Incident Response
- The attack
- Mitigation
- Compromised data and your organisation
- Resilience against social engineering and the insider threat
- A vehicle for both corporate and individual compromise
- Wi-Fi and tracking
- Reconnaissance and OSINT
- Technical and non-technical attacks
- Influence and persuasion
- Going beyond the tech
- Common, less common and emerging vulnerabilities

How you will learn

Education includes role-playing, case studies, discussion and team exercises. Individual personal review of skills development. Softcopy course take-aways.

Module 1: Introduction to Cyber Risk; Module 2: Attacks and attacker Methodology

Module 3: The Persistent Threat of Leaked Data; Module 4: Wi-Fi - the Corporate and Personal Risk; Module 5: Exercise; Module 6: The Devastation; Module 7: Mitigation

Programme Leader

Ciaran Richardson - is a former UK intelligence officer with a background in Counter Terror and military special operations. A special emphasis is given to the 'cyber-human' interface, tracking individuals through OSINT (open source intelligence) to identify and apply ethical social engineering tests and awareness training for a safe and secure workforce.

Overview

Focus on developing a sound understanding of just how easy and low-tech the efforts of an attacker can be and how to implement mitigation strategies. You will see demonstrations of the vulnerabilities in realistic targets. A key theme running through the course is that of workforce vulnerability – no matter how well defended the organisation's intellectual property is, the staff are the way in.

Hear real world examples of damaging attacks are dissected, with emphasis on correct implementation of cyber incident response.

Case studies and practical work are drawn from around the globe to educate you to understand how attackers set about compromising an organisation and to provide you with the most effective measures to mitigate an attack to bring a business back online at minimum expense.

Dates and Cities

13-15 May 2019	London
3-5 June 2019	Amsterdam
1-3 July 2019	Zurich
5-7 Aug 2019	London
2-4 Sept 2019	Dubai
7-9 Oct 2019	Johannesburg

This course can be run as an In-house or Bespoke Programme

Faisal Malik
+44 (0)20 7936 8987
fasial.malik@pulseconferences.com

Connecting minds, assuring the future:
Education that builds business resilience and professional skills
www.pulseeducate.com