



Career
Conversion



Continuing
Professional
Development

Incident Response for IT Staff/ Operational Digital Forensics

Our **six day** GCHQ certified course will provide you with the necessary responsive skills and appropriate decision-making abilities to effectively investigate IT security incidents using cutting edge digital forensics tools, tactics and techniques. You will also become a malware hunter and defender for your organisation and be able to identify suspicious activity on a corporate system and from network traffic to discover and investigate high-end cyber threats.

Aim

Understand the types of tactics a threat actor uses to evade detection by developing advanced skills to locate malicious elements on a network and respond appropriately. Learn how to report a compromise, who to alert and how countermeasures may help defend against future threats.

Who Should Attend?

- IT professionals who operate as the IT support function in an organisation
- Professionals who need to understand how to effectively respond to a potential incident and quickly apply the necessary actions
- The course is also available as part of a workforce transformation program ensuring all IT staff are better defenders of their organisation's network.

Learning Objectives

- Develop skills using fully immersive, hands-on training and a variety of tools
- Effectively discover host or network breaches in order to triage potential attacks
- Understand how malware typically finds its way onto a system
- Understand variations of malware and cyber threats
- Gain knowledge of the fundamentals of Windows operating systems
- Gain knowledge of file systems and processes
- Interrogate the Windows Registry
- Perform volatile memory capture (RAM dumps)
- Perform forensic imaging
- Differentiate between law enforcement and corporate incident response
- Perform network traffic forensics
- Perform disk-based forensics
- Find and identify important artefacts
- Report findings.



Certified Training

