Continuing Professional Development

SOC Incident Responder

Our **ten day** GCHQ certified Security Operations Centre (SOC) Incident Responder course puts you at the forefront of monitoring and then effectively reacting to potential security incidents. The course provides experienced cyber security professionals with deep understanding of: attacker tactics, digital forensics (disk, memory and network), malware analysis and interfacing directly with respective parties and stakeholders to perform first line incident response.

Aim

Acquire and expand the necessary technical skills and knowledge to function as an effective and specialist incident responder working within a fully operational SOC.

Who Should Attend?

- Trainees who have had previous experience in a SOC, who are now considered senior and require incident responder specialist training to appropriately and safely react to client requirements.

Prerequisites

It is preferable that trainees have experience and fundamental knowledge of Windows and Linux operating systems. If this is not the case – an evening, a half day or a full day can be bolted onto the course for adequate preparation.

Learning Objectives

- Understand the functional requirements needed when responding to an incident
- Understand the roles in an organisation and the language of reporting that may be needed
- Determine the terminology required when liaising with clients regarding collation of data
- Prepare a generic incident response jump kit
- Strategically prepare a plan of action when identifying the scope of work
- Perform effective and efficient digital forensics to quickly acquire data
- Understand the legal requirements that should be adhered to when acquiring data that may later be required for law enforcement or court proceedings
- Explain to clients the role of the SOC incident responder and actions taken during an incident
- Ensure any potentially malicious software that may be present is contained securely and safely.

GCHQ Certified Training

Cascades 1 | 1190 Park Avenue | Aztec West | Bristol | BS32 4FP | UK
Tel: +44 (0) 207 887 2699 Email: clientservices@pgitl.com Visit: www.pgitl.com