TIGERSCHEME™

Providing excellence in penetration testing

FORENSICS

1 day assessment

Tiger Scheme and their approved Training Partners provide a range of training courses and certifications relating to forensic investigation. These are at both the intermediate (Qualified) level and the Senior level.

Please note that the Senior assessment is a challenging exercise, demanding industry-leading abilities. Candidates should have a number of years of hands-on experience, with significant practical experience in this field.

Forensics Investigator

The Forensics Investigator qualification covers many broad areas: legal, management, ethics, compliance; technical expertise; and effective delivery of results. The assessment itself consists of a one-hour multiple choice examination, a three hour written paper, a six hour practical assessment and an interview with an examiner. The practical element is based on a rig which as far as possible mimics the environment that an investigator would face on a real world assignment.

Forensic Readiness

This is an intermediate level qualification based upon the more advanced Forensic Investigator qualification, reflecting also the requirements of the emerging ISO27037 standard. Candidates will be expected to demonstrate the skills necessary to preserve and seize computer based evidence.

Incident Handler

Successful candidates will possess and have the ability to demonstrate a range of skills associated with the role of First Responder, including imaging mainstream desktop and laptop devices, as well as being able to specify the actions needed to recover digital evidence from more complex equipment such as RAID arrays, mobile devices etc.. The assessment includes a requirement to demonstrate the ability to obtain an image from a test rig.

Malware Analyst

This is a specialist qualification which builds upon Senior level skills. Candidates will be expected to analyse network traffic information, identify and locate a targeted piece of malware and reverse engineer it, to the point where its purpose, functionality and possible source can be identified. This assessment is a very demanding one, requiring experience in the field, a solid grounding in a number of aspects of malware analysis, and a sound grasp of underlying operating systems.

Candidates will also be expected to demonstrate an appropriate level of knowledge and expertise in the following key technical areas:

- The ability to capture and decode IPv4 and IPv6 network traffic so as to identify the activity of malicious software and reconstruction of documents and files sent across the network
- The ability to identify various infection strategies and payloads
- The ability to identify various techniques that an adversary might reasonably use to avoid detection
- The ability to identify and reverse engineer a payload (e.g. packers)
- The ability capture and analyse live memory and process information
- The ability to perform the classification and identification of in-memory infection

Forensics details continued on reverse >

TIGERSCHEME™

For more information visit **www.TigerScheme.org**

Providing excellence in penetration testing

TigerScheme™

Providing excellence in penetration testing

1 day and 2 day assessment

FORENSICS

Forensics details continued:

These must be supported by a working knowledge, demonstrated through the application of best practice, in the following supporting areas:

- Awareness of requirement for authority documents to have been signed by all relevant parties including any third party hosting company or service providers
- Awareness of the agreements on any status update process throughout the forensic investigation
- Awareness of the agreements with regard to delivery of the draft and final reports
- Awareness of the risks associated with malicious software investigations and the impact that they can have on customer systems; these may include unintentional disruption to network devices and links through bandwidth consumption.

Tiger Scheme is a not-for profit organisation working in co-operation with The University of South Wales (formerly the University of Glamorgan) to provide an independent, University recognised assessment of the technical, legal and ethical capabilities of penetration testers within the UK. Buyers of penetration testing are vocal of the shortage of certified skill in the UK, and the negative impact this has on project timescales and costs. Tiger Scheme bridges this gap between buyers and suppliers of assessment services. Whilst many UK based certification concentrate purely on commercial service providers, Tiger Scheme offers certification to both professional penetration testers and IT professionals working within internal IT teams. This allows organisations to have leading edge expertise within their own teams, offering greater flexibility and cost effectiveness.