Digital Forensics and Cyber Investigations

Why Attend

- The requirement for operational Incident Response, and Digital Forensic disciplines and procedures, has been forced to evolve in the last decade – driven by the increase of unprecedented cyber breaches, and associated cyber-crimes. Data breaches and intrusions have also evolved to more complex engagements, presenting the need for a robust in-house Digital Forensics/First Responder capability.
- This course enables participants to engage with, and to investigate, both internal and external digital crimes and infractions. Applying robust processes and procedures which encompass the Digital Forensic acquisition of images, from media and artifacts to computers and mobile technologies. Aligned with tough proven processes to secure evidential materials, participants have the opportunity to apply best practices to assure associated evidential integrity and value is maintained intact.
- From a background of "in-the-field" law enforcement, associated with the key concepts of legal practices, this course will provide hands-on pragmatic experiences, underpinned by the academic and legal structures which form the basis of Forensic Science.
- Including the key requirements of the Secure Operational Centre (SOC) and its interfaces with the Computer Security Incident Response Team (CSIRT), this course will provide participants with the skills they require to respond to a digital investigation with the assurance of completing it correctly.

Course Methodology

- The course includes practical sessions, videos as well as live demonstrations and live coding. A hands-on use of all tools is encouraged throughout the course as all participants engage in the real-time investigation of a test case.

Course Objectives

By the end of the course, participants will be able to:

- Apply a Digital Forensics methodology in an operational environment
- Set a strategy for a Digital Forensics response framework
- Conduct investigations into social media, malware, viruses, and ransomware
- Manage a Digital Scene-of-Crime and its Digital evidence and artifacts
- Investigate mobile technologies, and other media which may hold evidential materials and artifacts
- Apply the techniques to extract images from systems artifacts

Target Audience

- This course is designed for IT professionals, Fraud Investigators, Auditors, CSIRT and SOC Analysts, working in companies that are targets for cyber and digital attacks. It is also highly beneficial for police and military personnel, probation officers and other security personnel who deal with cyber investigations.

Target Competencies

- Performing incident response
- Understanding digital forensics
- Conducting digital crime investigation
- Applying forensic science

Digital forensics – background and legal practices

- Introduction to the science of forensics
- Terms and definitions
- Chain of digital crime
- The background of digital crime
- Case histories of real-life cases
- Digital forensics - law
- Digital forensics - legislation
- Standards of digital forensics
- Fundamentals of digital forensics
- The risks faced by organizations

The digital forensics response framework

- The first responder digital forensics toolkit
- Scene of digital crime management
- The Secure Operations Centre (SOC)
- The CSIRT (Computer Security Incident Response Team)
- Roles and responsibilities
- Implementing a framework
- Case management

Collecting and processing digital evidence

- Domain Name System (DNS)
- Extended security infrastructures
- Investigating mobile technologies
- Acquisition of digital evidence and artifacts
- Handling of digital evidence and artifacts
- Processing of digital evidence and artifacts
- Case management protocols
- Wireless protocols
- Supporting technologies
- Reporting practices

Investigations of internal and external digital crimes

- OSINT (Open Source Intelligence)
- Its place in the digital forensic investigation
- Defining internal crimes
- Defining external crimes
- Child exploitation and investigations
- Malicious applications
- Ransomware
- Anti-forensics capabilities
- Digital forensics and terrorism