Certified Cyber Security Specialist

Why Attend

- This course will provide participants with in-depth knowledge and practical skills to plan, deliver and monitor IT/cyber security to internal and external clients encompassing a complete, conjoined set of disciplines in the areas of IT policies, Security-Operational-Run-Book, Security/Penetration Testing, Ethical Hacking and Black Hat Hacking.
- It will also cover WiFi security, Website security, human factors, cyber forensics, cyber security team management, Secure Operations Center (SOC) and Computer Security Incident Response Team (CSIRT) infrastructures.
- As part of the course, participants will conduct a risk assessment of two different deployments based on the ISO27001 to identify any direct, or indirect threats, security exposures, or potentials for vulnerabilities. Participants will also respond to an example security incident and identify the best practices which could be applied to secure their own organization, and associated assets. All participants will be given copies of Run Books to deal with cyber extortions, Distributed Denial of Service (DDoS/DoS) and forensic investigations.

Course Methodology

- The course will include practical sessions, videos as well as live examples [e.g. Virus] and demonstrations of white and black hat hacking tools. All participants will also be provided with the latest research papers and articles.
- As part of the course, participants will conduct a risk assessment of two different deployments based on the ISO27001 to identify any direct, or indirect threats, security exposures, or potentials for vulnerabilities. Participants will also respond to an example security incident and identify the best practices which could be applied to secure their own organization, and associated assets.

Course Objectives

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

- Apply information security standards to their organization and its critical assets
- Identify the threats presented by viruses, malware, active code, and Active Persistent Threats (APT) and consider the different mitigating options
- Formulate and manage effective cyber security teams, and apply the Computer Security Incident Response Team (CSIRT) framework, tools and capabilities to deliver cost effective and robust solutions to protect the organization
- Use Neuro Linguistic Programing (NLP) to deliver messages that will change the way employees work and think about security
- Examine the area of wireless security protocols, their security attributes, and their potential insecurities within the organization, and in public spaces
- Illustrate how penetration testing and ethical hacking enhance organizational security
- Evaluate and apply two of the most important aspects in the modern day of cyber-adversity: Open Source Intelligence (OSINT) and cyber threat intelligence

Target Audience

- IT professionals, security professionals, auditors, site administrators, general management and anyone tasked with managing and protecting the integrity of the network infrastructure. This also includes anyone already familiar and involved with IT/cyber/digital security and seeking to build on their fundamental principles of security.

Target Competencies

- Information security management
- Vulnerability assessment and management
- Applying cyber security solutions
- Developing IT policies and procedures
- Cyber forensics
- Ethical hacking and Black Hat hacking

Adapting to evolving standards

- Information security standards (e.g. PCI-DSS/ISO27001)
- Documented tools:
- ISO/IEC 27001
- PAS 555
- Control Objectives for Information and Related Technology (COBIT)
- Future standards
- ISO/IEC 2018
- EU privacy regulations

Principles of IT security

- Enterprise security
- External defenses
- Web filtering
- Intruder Prevention Systems (IPS)
- Intruder Detection Systems (IDS)
- Firewalls
- Secure code
- Software Development Lifecycles (SDL)
- Potential insecurities within developed applications
- WiFi security protocols and attributes
- Voice over IP (VoIP) security
- Governance Risk and Compliance (GRC)
- Security Incident Event Management (SEIM) applications
- Cloud security
- Third party security and compliance

Adopting cyber security measures

- Employee perception on security through Neuro Linguistic Programing (NLP)
- Security education and awareness: techniques, systems, and methodologies
- Penetration testing
- Ethical hacking
- Options to mitigate viruses, malware, active code threats and Active Persistent Threats (APT)
- The Computer Incident Response Team (CSIRT) frameworks, tools and capabilities
- Incident first response: proven methodologies, tools, and systems
- The science of applying robust digital forensics: applicable law, capabilities, and methodologies
- Supervisory Controls and Data Acquisition (SCADA); security requirements, processes and methodologies
- Abuse images: complying with local and international law

Building cyber security teams

- Creation and management of a Secure Operations Center (SOC)
- Development of the Corporate Security Organization Framework
- Formulation and deployment of a Computer Security Incident Response Team (CSIRT)
- Bespoke Security Incident and Event System (SIEM) for the operational deployment
- Risks associated with I/O Security (e.g. USBs, CDs, other forms of media)
- Risks of Active Code Injection, and mitigation techniques

Advanced cyber risks and tools

- Cyber crime and the darknet/darkweb: the world of the hackers/hacktivists
- The underground of cyber criminality
- Social engineering as a tool to test operational resilience
- Open Source Intelligence (OSINT)
- Cyber threat intelligence
- Open source and commercial security tools

Steganography - Techniques used to hide hacking tools and malware on networks

- Command line and tools used to identify and extract dangerous files and contain malware and hacking applications
- The 1-10-60 Rule to identify and contain dangerous hidden applications
- Alternate Data Streams (ADS) and the threats they can pose under an NTFS environment
- Leveraging ADS to hide undetectable malware within an operational network