PARTNERS IN KNOWLEDGE UK LTD

Suite No. 129
295 Chiswick High Road
LONDON W4 4HH

Cyber Security Specialist

PIK458-1025 LON-1

PARTNERS IN KNOWLEDGE UK LTD
Suite No. 129
295 Chiswick High Road
LONDON W4 4HH

Place:	London (UK)	**Venue:**			
Start Date:	19-10-2025	**End Date:**	23-10-2025	**PPP:**	£4950

Cyber Security Specialist

PIK458-1025 LON-1

If you can't train them, you can't blame them!

Short Description:

This course will provide participants with in-depth knowledge and practical skills to plan, deliver and monitor IT/cybersecurity 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, cybersecurity team management, Secure Operations Center (SOC), and Computer Security Incident Response Team (CSIRT) infrastructures.

Course Overview:

Course Objectives:

At the end of this course the participants will be able to:

- 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.
- 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 cybersecurity teams, and apply the Computer Security Incident Response Team *(CSIRT)* framework, tools, and capabilities to deliver cost-effective and robust solutions to protect the organisation.

PARTNERS IN KNOWLEDGE UK LTD
Suite No. 129
295 Chiswick High Road
LONDON W4 4HH

Targeted Audience:

- IT professionals.
- Security professionals.
- Auditors.
- Site administrators.
- General management.
- Anyone tasked with managing and protecting the integrity of the network infrastructure.
- Anyone already familiar and involved with IT/cyber/digital security and seeking to build on their fundamental principles of security.

Program Outline:

Day 1: Adapting to evolving standards

1. Information security standards (e.g. PCI-DSS/ISO27001).
2. Documented tools *(ISO/IEC 27001, PAS 555, Control Objectives for Information and Related Technology COBIT).*
3. Future standards *(ISO/IEC 2018, EU privacy regulations, Local and international government stipulations implicating access to private data).*

Day 2: Principles of IT security

1. Enterprise security *(External defenses, Web filtering, Intruder Prevention Systems (IPS), Intruder Detection Systems (IDS), Firewalls).*

1. Software Development Lifecycles *(SDL).*
2. Potential insecurities within developed applications.
3. WiFi security protocols and attributes.
4. Voice over IP *(VoIP)* security.
5. Governance Risk and Compliance *(GRC).*
6. Security Incident Event Management *(SEIM)* applications.
7. Cloud security.
8. Third-party security and compliance.

Day 3: Adopting cybersecurity measures

1. Employee perception of security through Neuro-Linguistic Programming *(NLP).*

2. Security education and awareness: techniques, systems, and methodologies.
3. Penetration testing.
4. Ethical hacking.
5. Options to mitigate viruses, malware, active code threats and Active Persistent Threats *(APT)*.
6. The Computer Incident Response Team *(CSIRT)* frameworks, tools, and capabilities.
7. Incident first response: proven methodologies, tools, and systems.
8. The science of applying robust digital forensics: applicable law, capabilities, and methodologies.

Day 4: Building cybersecurity teams

1. Supervisory Controls and Data Acquisition *(SCADA);* security requirements, processes, and methodologies.
2. Abuse images: complying with local and international law.
3. Creation and management of a Secure Operations Center *(SOC)*.
4. Development of the Corporate Security Organization Framework.
5. Formulation and deployment of a Computer Security Incident Response Team *(CSIRT)*.
6. Bespoke Security Incident and Event System *(SIEM)* for the operational deployment.
7. Risks associated with I/O Security *(e.g. USBs, CDs, other forms of media)*.
8. Risks of Active Code Injection, and mitigation techniques.

Day 5: Advanced cyber risks and tools

1. Cybercrime and the darknet/dark web: the world of the hackers/hacktivists.
2. The underground of cyber criminality.
3. Social engineering as a tool to test operational resilience.
4. Open Source Intelligence *(OSINT)*.
5. Cyber threat intelligence.
6. Open source and commercial security tools.
7. The operational use of encryption.
8. Virtual private networks.