iSecure Consulting

CSI: Cyber Security Institute

Training Catalogue

SPECIALIZED CYBER SECURITY COURSES	
	Executive Cyber-Security Bootcamp
	Cyber-Security Essentials
	Cyber Surveillance
	Cyber Assurance & Management (Diploma Certificate)
	Cybercrime Investigation Training
	Lawful Interception Training
	National Cyber-Security Surveillance Training
	Wireshark Certified Network Analyst
FACULTY AND RESOURCES	
	Faculty Officers
	Resources

Course	**Executive CyberSecurity Bootcamp**
Synopsis	Information security is not only a technical issue, but a business and governance challenge that involves adequate risk management, reporting and accountability. Effective security requires the active involvement of executives to assess emerging threats and the organization's response to them.
Curriculum	Information Assurance Ecosystem; The Cybercrime Act 2015 and Critical Infrastructure: consequences of non-compliance; Correlation between Risk, Threat and Vulnerability: what is Risk Appetite?; Insider Threats Vs Internal Controls: Management and profile; Return On Security Investment (ROSI); Role-playing - Thinking like a hacker
Target Audience	Board of Directors, Executive Management, Business Owners, C-level officers, Critical Infrastructure (CI) owners, National Security Personnel, ISP Security Personnel. CISO, Insurance managers, brokers, safety practitioners, auditors, project managers, accountants, solicitors and consultants
Expected Outcome	Candidates will be able to (a) Understanding the cyber landscape and accurately demystify cybersecurity jargons; (b) correctly interpret the National Cybercrime Act and identify countermeasures; (c) Perform due care and due diligence within the 10 Domains of cybersecurity governance; (d) Develop Cybersecutiy Policy
Duration/ Loc	3 Days | UK | Kenya

Course	**CyberSecurity Essentials**
Synopsis	How do organizations deal with the risks if they do not understand the threats landscape, risks and vulnerabilities, motivations and mechanics behind the threats? This training is designed to highlight the current global/national (government) cyber initiatives for various sizes of enterprises including those who perhaps cannot afford the ISO 27002 Certification.
Curriculum	Risk Management, Threats, Risk and Vulnerability, Information Assurance Ecosystem, Standards and Framework ISO 27001, COBIT and ISF, Insider Threats, Cyber Controls - Policy, Business Continuity and Disaster Recovery, Hands-on practical - Policy Development, Risk Assessment.
Target Audience	Senior Executives, Critical Infrastructure (CI) owners, National Security Personnel, ISP Security Personnel.
Expected Outcome	Candidates will be able to (a) Understanding the cyber landscape and identify cyber risks, threats and vulnerabilities. (b) Identify and classify Cyber Incidences, (c) Develop cyber risk management program, (d) Understand Risk Assessment, augment their current risk management program and develop IS Policy
Duration/ Loc	2 Days | UK | Nigeria | Kenya

Course	Cyber Surveillance
Synopsis	This is a highly technical course designed specifically for providers of frontline cyber protection at corporate and National level. The objective is to build capacity of delegates to Protect, Defend, React and Recover. Delegates will unravel how perpetrators compromise a system, what they stole, and who is involved. The curriculum covers the most critical skills needed to mount efficient and effective real-time incident response investigations.
Curriculum	Introduction to Information Assurance, ISMS Framework and Legislations, Protocols and Network Basics (+ Wifi), Packet Analysis (Python, Wireshark, etc), Network Traffic Analysis, Reassembly and Reconstruction, Lawful Interception, Case Scenarios.
Target Audience	Network/Systems Administrators, Law Enforcement Agents, National Security Personnel, ISP Security Personnel, IT Security Professionals, Systems Auditors, Investigators, Systems/Security Manager, Forensics Investigators, and Expert Witnesses.
Expected Outcome	Candidates will be able to (a) Implement Advanced Packets Analysis techniques (b) Investigate internet crimes and capture packets before they leave network for evidential purpose (c) Understand ethical and legal issues pertaining to network packet capturing.
Duration/Loc	3 Days | UK | Nigeria | Kenya

Course	Cyber-Assurance & Management - Certificate
Objectives	Our flagship training course targeted at individuals who are planning to make a career in (or switch career to) cyber security field. It is a scheduled Ten-week intensive and highly focused program covering 12 Domains and a project work. During the course, participants will use various open-source tools such as Python and Linux built on Raspberry Pi.
Synopsis	Governance, Risk-management and Compliance (GRC), Penetration Testing, Root Linux, Violent Python, Wireshark and other Open-source tools, Risk Assessment, Business Continuity, Encryption Network and Physical Security, Network Access Control and a Project.
Target Audience	Private individuals with basic education qualification or equivalent work experience.
Expected Outcome	Ability to identify cyber threats and vulnerabilities, Ability to understand Risk Assessment and develop IS Policy.
Duration/Loc	20 Weeks | Nigeria

Course	**Cybercrime Investigation Training**
Synopsis	Developed in collaboration with our Technical Partners and a National Police University, the training is exclusively designed to build the capacity of Law Enforcement Agents who are directly responsible for cyber-related investigation. The training is in two parts: A 1-week local training (theory based) and 1-week overseas trip for practical hands-on experience.
Curriculum	Cyber Crime with VoIP and Telecom, Cyber Crime with Internet Services, Legal Processes with Cyber Crime Investigation, Methodology of Data Analysis for Cyber Crime Investigation, Weakness of Common IT Systems, Workshop on Drills
Target Audience	Middle and Senior management LEA staff, National Security Personnel
Expected Outcome	Delegates will develop cutting-edge cybercrime investigation skill using the latest technologies and protocols and gain in-depth knowledge on how to identify security vulnerabilities and subsequently identify tools used by attackers.
Duration/ Loc	3 Days | Taiwan

Course	**Lawful Interception Training**
Synopsis	Designed exclusively for National government that has deployed or is in consideration of deploying LI infrastructures. The training will expose participants to the principles of Lawful Interception, its regulations and limitations. It is designed to help LEAs understand LI planning, deployment and operations.
Curriculum	ETSI and CALEA Framework & standard, Deployment, LI Solution Suite, Data Analysis and Evidence Admissibility, Case Study
Target Audience	Law Enforcement Agents, National Security Personnel, ISP Personnel, Min of Justice Personnel, Project Manager, Consultants
Expected Outcome	Participants will master the operation of the LI infrastructure, protocols and service delivery
Duration/ Loc	4 Days | UK | Nigeria | Kenya

Course	**National Security Surveillance Training**
Synopsis	Stripped of technical jargons, this practical-based training is designed and managed in conjunction with our partners and it takes place in a highly specialized training centre in Taiwan. Delegates will be introduced to the common nature of social uprising, how to conduct social sentinel surveillance and data analysis.
Curriculum	National Security vs National Development, Rumor and its Nature, Social Sentinel vs Target Surveillance, Methodology of Full Scale of Network Surveillance at National Level, Deployment of Network Surveillance, Case Study on Different Countries
Target Audience	RESTRICTED to National Security Operatives and "non-techies" on whose desk the buck stops.
Expected Outcome	Based purely on agreed Terms of Reference. However, delegates will understand the various vectors of threats, identify risks and vulnerabilities, identify corresponding controls and treatments to mitigate risks, implement and manage an Effective Information Security Strategy Program.
Duration/Loc	3 Days | Taiwan

Course	**WIRESHARK Certified Network Analysis**
Synopsis	The bulk starts and ends on the wire. This is the mysterious dark place where the core cybercrime perpetrators have reigned supreme. To test a candidate's knowledge and ability to troubleshoot, optimize and secure a network based on evidence found by analyzing traffic captured with the world's most popular and widely-deployed analyzer.
Curriculum	Communication Protocols, TCP/IP, Wireshark Regular Expressions (Regex), Lab Solutions.
Target Audience	Private individuals, Cyber Investigators, Network Administrators, IT Auditors/Managers.
Duration	4 Days
Expected Outcome	Certified WCNA.
Duration/Loc	4 Days | UK | Nigeria | Kenya