Foundation Certificate in Cyber Security Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

The objective of the course is to provide a comprehensive but necessarily high-level overview across industry standard technology and platforms, illuminating the technology and its specific cyber governance, risk, and assurance challenges, including artificial intelligence (AI) adoption, without technically challenging the learner to hands-on labs.

On the first day the course takes the learner back to computer basics to build the individuals understanding common technology platforms through to the network layer and on via virtualisation technologies, cloud systems, telecoms and modern communications and insight into the world of protective monitoring, challenges and issues of security events logs and analysis.

Common methods of attack. Providing the learner with an insight into many of the most popular attack vectors today.

The third day will start the benefits and pitfalls of encryption. Then covering cyber law and the context in which security practitioners and organisations must operate within. Each of us has a digital footprint and the technology we use within our enterprise as an attack surface. The next module joins these two principles and explains the challenges for assurance around leaky data.

During the remainder of day four and five we introduce the layered cyber concepts and the deeper governance required throughout the entire lifecycle covering several specialist areas essential to the rounded security practitioner.

Each day provides insight into the technical subject matter with the crucial security subtext. Knowledge check exercises, where delegates work in groups to discuss and provide solutions to scenarios offering an explanation with a rationale in each instance of why this is important from a security assurance perspective. Learners will also have the opportunity to take part in a real-time ransomware response scenario exercise, ideal as a capstone event to help consolidate learning.

Prerequisites

There are no prerequisites for this course, however, participants are expected to have a basic understanding of computers and the internet.

Foundation Certificate in Cyber Security Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

- Understand the threats faced by modern networks, systems, and application platforms.
- Network fundamentals - explaining basic networking concepts including network services, physical connections, topologies and architecture, and cloud connectivity.
- Understand network security concepts and network attacks to harden networks against threats.
- Understand routing technologies and networking devices; ethernet solutions and wireless technologies including Bluetooth, WAN, LAN, MAN, PAN, and BAN
- Understand the difference between the OSI 7-layer model and the TCP/IP Model
- Understand the threats, attacks and vulnerabilities from newer custom devices that must be mitigated, such as IoT and embedded devices, DDoS attacks and social engineering attacks based on current events.
- Understand organisational risk management and compliance with regulations, such as PCI-DSS, SOX, HIPAA, GDPR, FISMA, GLBA and CCPA.
- Introduction to the risks and security challenges with AI adoption within organisations.
- Understand organisational security assessment through protective monitoring and incident response procedures, such as basic threat detection, risk mitigation techniques, security controls and basic digital forensics.
- Understand cloud computing concept and architecture.
- Understand the physical security components connected to the Internet threat they pose to your organisation. Including RFID, IOT, smart phones.
- Insider threat, the passive and active threat and how to overcome them.
- Understand physical, technical, and procedural security controls.
- Perimeter defences are not enough. Understand de-perimeterisation and how to implement layered security approach using defence in depth.
- Understand the techniques used to detect, prevent, and respond to threats.
- Identify areas of testing, audit and review and system development
- Open-source security tools for active and passive defence techniques
- Understand the difference between separation of systems and segregation of duties and how that is implemented and validated.
- Discover and analyse ‘high risk’ weakness within systems.
- Understand cryptography and its applications in a digital world.
- Analyse, attribute, and predict the threats and create an active defence posture.

Outline

Day 1

Module 1 Computing Foundation, Data Storage and Memory

- Computer system components, operating systems (Windows, Linux & Mac), different types of storage, and memory management.

Module 2 Network Computing

- Switched networks, packet switching vs circuit switching, packet routing delivery, routing, WAN, LAN, MAN, internetworking standards, OSI model 7 layers.

Module 3 Network Communications - TCP/IP protocol suite,

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Types of addresses, physical address, logical address, IPv4, IPv6, port address, specific address, WAN vs LAN, DHCP (Dynamic Host Configuration Protocol) and network access control.

Module 4 Internet Primer

- How does data travel across the internet? End to end examples for web browsing, emails, using applications - explaining internet architecture, routing, DNS.

Day 2

Module 5 Network Security

- Secure planning, policies and mechanisms, Active Directory structure, introducing Group Policy (containers, templates, GPO), security and network layers, IPSEC (IP Security), SSL / TLS (flaws and comparisons) SSH (secure shell), Firewalls (packet filtering, state full inspection and NGFW), application gateways, ACL's.

Module 6 Modern Communications

- VoIP, Smishing, Vishing, wireless LAN (WI-FI), Network Analysis and Sniffing, Wireshark. IOT communication data, SHODAN, Bluetooth, Zwave, Zigbee, PAN (personal area network), HAN (home area network), BAN (body area network) and 5G.

Module 7 Virtualisation & Cloud Technologies

- Virtualisation definitions, virtualisation models, Cloud Security Alliance (CSA), terminologies, ISO/IEC 27017 is an information security framework for organisations using (or considering) cloud services. Virtual models, virtual platforms, what is cloud computing, cloud essentials, cloud service models, security & privacy in the cloud ISO 27018, multi-tenancy issues, infrastructure vs data security. Cloud Security Technical Reference Architecture from Cybersecurity & Infrastructure Security Agency (CISA)

Module 8 Protective Monitoring (Security Information Event Management SIEM)

- Security Information Event Management (SIEM) processes and architecture, SOAR security orchestration, automation, and response. SIEM features, user activity monitoring, real time event correlation, log retention, file integrity monitoring, security auditing & automation auditing, what to audit, implementation guidelines, what to collect, Windows Event Log, UNIX Syslog, logging at an application level, audit trail analysis, approaches to data analysis.

Module 9 Common Methods of Attack

- Cyber exploits, understanding malware, cross site scripting, SQL Injection, virus, worm, DDOS, input validation, ransomware, buffer-overflow, targeted attacks, cyber threat intelligence, MITRE ATT&CK®, D3FEND Matrix | MITRE D3FEND™, Cyber Kill Chain and advanced persistent threats (APT).

CyberFish DoJo Ransomware response scenario

Day 3

Module 10 Encryption

- Uses of encryption technology, symmetric / asymmetric key encryption, public and private keys, weaknesses, decryption, hashing, digital signatures, PKI, certificates authorities, data at rest and in

transit, SSL/TLS, and SSL stripping.

Module 11 Cyber and the Legal Framework

- Legislation, chain of custody, reporting and assurance within the context of a legal framework, Artificial Intelligence (AI) Governance, EU General Data Protection Regulation (GDPR & DPA), California Consumer Privacy Act (CCPA), Federal Computer Fraud and Abuse act versus Computer Misuse Act. HIPAA, Sarbanes Oxley (SOX). The Federal Information Security Management Act (FISMA), Freedom Act and Federal Trade Commission Act (FTCA).

Module 12 Digital Footprints

- Internet foundations, WHOIS (Inc. worked example), Internet analysis, search engines, OSINT techniques offensive and defensive, Tools for finding information on people and companies, username searchers, email searching, passwords, surface, dark and deep web. Data breach websites. Phishing, Spear Phishing, Whaling, Deep Fake attack. Social Engineering attacks.

Module 13 Information Assurance

- Overview – Drivers for Information Assurance, CIA Triad, what do attackers want? Threats to your organisation and the capabilities

Day 4

Module 14 Risk Management and Risk Treatment

- Business context and risk management approach, return on security investment (ROSI/ROI), risk management lifecycle, who delivers risk management - where in the lifecycle, understanding the context, legal and regulatory. Risk Treatment - Identify the ways of treating risks, methods of gaining assurance, understanding the nature of inherent/residual risk, collecting evidence that supports decisions, risk management decisions.

Module 15 Physical Security

- Physical security - lighting, CCTV, fencing, intrusion detection, screening, destruction, UPS and generators, access, and control of entry.

Module 16 Personnel Security

- People, employees, contractors, customers (resource, vulnerability, threat), recruitment, screening, Social Engineering, Common People Exploits, T&C's, in role, change in role, termination, insider threat, supply chain challenges.

Module 17 Service Assurance & Standards

- Assurance perspective - including CPA/CAPS, FIPS, CE, Common Criteria, SPF. Summary of common industry standards. (Inc. OWASP, ISO27001/2, PCI-DSS)

Day 5

Module 18 Software Security Assurance

- Principles for software security, (securing the weakest link, defence in depth, failing securely, least privilege, separation of privilege), IA design principles.

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Module 19 Secure Development Process

- Secure by Design, Secure Development Life Cycle (SDLC). AI Governance in the System Development Life Cycle: Insights on Responsible Machine Learning Engineering. Testing, audit and review and system development. UAT (user acceptance testing. White, grey, and black box testing.

Module 20 Threat Modelling and STRIDE

- What is threat modelling, threat modelling processes, STRIDE: Risk Mitigation options

Module 21 Introduction to Security Architecture

- Security design architecture, enterprise design frameworks (TOGAF, ZACHMAN, SABSA), patterns (NCSC, Open Security Architecture).

Module 22 Security Best Practice

- Reduce the attack surface, defence in depth, test security, weaknesses and vulnerabilities, secure coding, learn from mistakes, NCSC 10 steps to cybersecurity and NIST Cybersecurity framework.

Exams and Assessments

Exam Information

Candidates will receive individual emails to access their APMG candidate portal, typically available two weeks post exam.

Knowledge Check – Quiz

End of module knowledge check – exam style questions

Duration 50 Minutes

Questions 50, multiple choice (4 multiple choice answers only 1 of which is correct)

Pass Mark 50%

Following the exam, candidates will receive individual emails to access their APMG candidate portal, typically available two weeks after the exam date.