

## Tech-Trail Program

Cybersecurity
Track



## **COURSE OVERVIEW**

This advanced 12-week cybersecurity training program is designed to produce world-class cybersecurity experts equipped with the skills, tools, and strategies to tackle the ever-evolving challenges in the digital landscape. Whether you're a beginner or looking to upskill, you will gain a deep understanding of core cybersecurity principles, practical hands-on experience with cutting-edge tools, and the ability to apply your knowledge to real-world scenarios.

The program culminates in a capstone project, where participants showcase their expertise through a practical, industry-relevant cybersecurity challenge.

## Course Objectives



Equip participants with foundational and advanced cybersecurity knowledge.

- Provide practical experience with tools and techniques used by cybersecurity professionals globally.
- Prepare participants for internationally recognized certifications like CEH, CISSP, and CompTIA Security+.
- **O4** Develop ethical hackers, penetration testers, and security analysts ready for the workforce.

Foster strategic thinking and problem-solving skills for real-world cybersecurity challenges.

## Course Prerequisites



Basic computer literacy and familiarity with operating systems like windows

Access to a laptop/PC with a minimum of 8GB RAM (16GB recommended).

Stable internet connection.

A strong interest in cybersecurity and a passion for learning



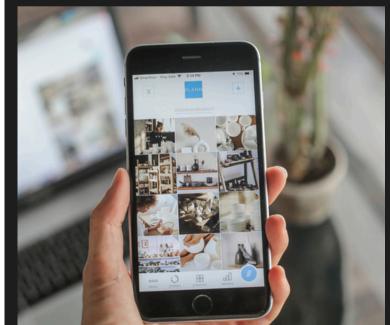


## KEY FEATURES

- Globally Recognized Certificate
- Extensive practical exercises with industry-standard tools.
- Lifetime Access to recorded sessions & study materials
- Direct access to industry professionals for mentorship.
- Weekday and weekend class options.







## CURRICULUM OVERVIEW



MONTH 1

Foundations of Cybersecurity



#### **Introduction to Cybersecurity**

- Overview of Cybersecurity
- Cybersecurity Frameworks and Standards (NIST, ISO/IEC 27001)
- Types of Cyberthreats and vulnerabilities
- Understanding Footprinting and its types
- Information Gathering Techniques for Footprinting and Reconnaissance

#### **Practical Exercises**

- Setting up a virtual cybersecurity lab
- Case study of cybersecurity incidents and their lessons.
- Conducting searches and network scans with reconnaissance tools.

#### Week 2

#### Basics of Networking for Cybersecurity

- Ethical and legal considerations of reconnaissance.
- OSI Model and TCP/IP Fundamentals
- Network Protocols: HTTP, HTTPS, FTP, DNS, SMTP
- Firewalls, Routers, and Switches Basics
- Using Wireshark for Network Traffic Analysis
- Basics of Virtual Private Networks (VPNs).

- Setting up a basic firewall rule in a simulated network.
- Monitoring live traffic with Wireshark.

#### Threat Landscape and Attack Vectors

- Types of Cyber Threats: Malware, Phishing,
   Ransomware, Social Engineering
- Common Attack Vectors (Email, Web, Network)
- Anatomy of a Cyberattack

#### **Practical Exercises**

- Simulating phishing attacks using phishing tools.
- Identifying malicious email samples.

#### Week 4

#### System Security and Endpoint Protection

- Operating System Security (Windows and Linux).
- Endpoint Security Tools and Techniques.
- Patch Management and Vulnerability Scanning.

- Setting up and managing endpoint security software.
- Conducting vulnerability scans using Nessus.

## MONTH 2

Intermediate Cybersecurity practices



Identity and Access Management (IAM)

- Authentication, Authorization, and Access Control.
- Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC).
- Privileged Access Management (PAM).

#### **Hands-On Activities:**

- Implementing IAM solutions like Active Directory.
- Configuring MFA for secure

#### Week 6

**Cryptography and Secure Communications** 

- Basics of Cryptography: Symmetric vs.
   Asymmetric Encryption.
- Hashing Algorithms and Digital Signatures.
- SSL/TLS for Secure Communication.

#### **Hands-On Activities:**

- Encrypting and decrypting files using OpenSSL.
- Configuring SSL/TLS on a web server.

#### Web Application Security

- OWASP Top 10 Vulnerabilities.
- Secure Coding Practices.
- Common Attacks: SQL Injection, XSS, CSRF.

#### **Practical Exercises**

- Penetration testing for web apps using Burp Suite.
- Writing secure code snippets to mitigate vulnerabilities.

#### Week 8

#### Malware Analysis and Social Engineering

- Types of Malware: Viruses, Trojans,
   Ransomware.
- Social Engineering Techniques.
- Static and Dynamic Malware Analysis.

- Analyzing malware in a sandbox environment.
- Simulating phishing attacks

## MONTH 3

Advanced Cybersecurity practices



Penetration Testing and Ethical Hacking

- Phases of Penetration Testing.
- Tools for Penetration Testing (Metasploit, Nmap).
- Reporting and Documentation.

#### **Practical Exercises**

- Performing penetration tests on simulated environments.
- Exploiting vulnerabilities to gain access.

#### Week 10

Cybersecurity Governance, Risk, and Compliance (GRC)

- Cybersecurity Policies and Procedures.
- Risk Assessment and Management.
- Compliance Standards (GDPR, HIPAA, PCI DSS).

- Conducting a mock risk assessment.
- Mapping policies to compliance frameworks.

#### **Emerging Trends in Cybersecurity**

- Al and Machine Learning in Threat Detection.
- Blockchain Security.
- Threat Intelligence and Predictive Analytics.

#### **Practical Exercises**

- Exploring Al-based cybersecurity tools.
- Analyzing blockchain vulnerabilities.

#### Week 12

#### Capstone Project Presentation

- Participants work on a real-world cybersecurity scenario:
- Designing a secure network architecture.
- Conducting a penetration test.
- Developing an incident response plan.
- Present findings and receive feedback from experts.

#### **Certification:**

 Certificate of Competence for successfully completing the course.

# GRADUATE STARTER KITS

Graduates of the CyberSecurity Program will be equipped with the following resources to confidently launch their careers;

Personalized CV and Linkedin optimization for Cyber Security Experts

**Hands-on-lab Portfolio** 

**Abbfem Alumni Membership** 

**Exclusive Access to Internship &**Freelancing Opportunities

# TRAINING DELIVERY



#### **Duration**

3-Months (2 classes weekly) each class is 4hours

## **Learning Mode**

- Virtual Classes Conducted on Zoom
- Physical Trainings conducted at any of our Training hubs located in the UK and in Nigeria

## **Training Schedule**

Weekdays - 10am-2pm daily Weekends ; Saturday - 10am- 3pm daily Sunday- 3pm -6pm daily



**Si**gn up now to secure your spot and take the first step toward a rewarding tech career

#### **Contact details**

Email: training@abbfem.com

Teelphone: +234907-764-8016, +447448813936

#### **Abbfem Training Hubs**

Nigeria: Eleganza House, 15b Joseph Harden Street, Marina, Lagos Island, Lagos state. Nigeriia

**United Kingdom**: 350A Icentre, Howard Way, Newport Pagnell, MK16 9PY, United Kingdom