cirvee

Cybersecurity Fundamentals Program

Duration: 4 Months (16 Weeks)
Mode: Physical & Virtual

Summary

Gain practical cybersecurity skills to secure systems, analyze threats, and investigate incidents using the same tools and techniques used by global security teams.

Course Overview

The **Cirvee Cybersecurity Fundamentals Program** is your complete introduction to the world of cyber defense, ethical hacking awareness, SOC operations, and global security standards.
Designed for beginners and aspiring analyst-level professionals, this program blends foundational theory with **70% hands-on labs,** simulations, and real Nigerian cybersecurity scenarios.
You'll learn how attackers operate, how to secure systems, how to analyze logs like a SOC Analyst, and how to respond to incidents using tools such as **Wireshark, pfSense, ELK Stack, Splunk, Kali Linux, and Nmap.**
By the end of the program, you'll understand how networks work, how to detect threats, how to investigate breaches, and how to protect organizations using industry best practices.

This program also prepares you for:
Level 2 – Cirvee Ethical Hacking (Offensive Security)

Certifications: CompTIA Security+, Cisco CyberOps Associate, EC-Council CND, ISO 27001 Foundation

Modules Overview

01. **Orientation & Cyber Landscape**

Understand cybersecurity fundamentals, the CIA triad, threat actors, and modern attack types.

02. **Computer Systems & OS Basics**

Explore Windows & Linux security basics, permissions, processes, event logs, and command-line essentials

03. **Networking Fundamentals I**

Learn IP addressing, ports, protocols, routing paths, and how data moves across networks.

04. **Networking Fundamentals II**

Dive deeper into DNS, DHCP, NAT, VPNs, and firewall concepts using Wireshark and pfSense.

05. **Endpoint & System Hardening**

Apply security configurations, patching, antivirus/EDR basics, and privilege management.

06. **Identity & Access Management (IAM)**

Master MFA, SSO, RBAC, and Zero Trust principles — and learn how access controls shape security.

07. **Security Operations Center (SOC) Basics**

Understand SOC tiers, alert lifecycles, incident triage, and analyst workflows.

08. **SIEM & Log Analysis**

Collect, search, and correlate logs using ELK/Splunk. Build your first detection rules and analyze security events.

09. **Incident Response Essentials**

Learn how to detect, contain, and investigate security incidents using structured IR methodology.

10. **Vulnerability Management**

Perform vulnerability scans, interpret CVE/CVSS scores, and prepare patch/remediation plans.

11. **Malware & Threat Intelligence**

Analyze malware behavior, identify IoCs, and use threat intel tools like VirusTotal, Any.Run, and MITRE ATT&CK.

12. **Governance, Risk & Compliance (GRC)**

Understand NDPR, NIST, and ISO 27001 — and learn to build simple security policies and risk registers.

13. **Introduction to Ethical Hacking**
Learn recon, scanning, and enumeration techniques in a safe lab environment using Kali Linux.

14. **Scanning & Enumeration (Deep Dive)**
Use Nmap, Masscan, and Zenmap to map networks, fingerprint systems, and identify attack surfaces.

15. **Exploitation Awareness & Defensive Response**
Understand how exploits work, how attackers escalate privileges, and how to detect attacks in SIEM.

16. **Capstone Project & Presentation**
Secure a fictional company's network while performing SOC analysis and presenting your defensive strategy and findings.

Career Opportunities

After this program, you can work as a:

- Cybersecurity Analyst
- SOC Support Analyst
- Information Security Associate
- IT Security / Network Support
- Vulnerability Management Assistant
- Entry-Level Ethical Hacking Trainee

Stay Cirvee Tip

"You don't just learn to stop attacks — you learn how attackers think, and that awareness is your greatest defense."

Visit Us

07047007055

"Cirvee" on google map

www.cirvee.com

Stay Connected

@cirvee

@hellocirvee

Cirvee Academy

Cirvee