Cipher Knights Academy

info@cipherknight
+44 7424 96756

Cybersecurity Fundamentals

Duration: 6 Weeks
Format: Online/In-Person

Skill Level: Beginner
Prerequisites: Basic Computer Skills

Certifications:
ISC2 CC | Cisco CyberOps

Course Description

This intensive 6-week program provides foundational knowledge in cybersecurity concepts, tools, and best practices aligned with industry standards (NIST, MITRE ATT&CK, CIS Controls). Students will gain hands-on experience with security technologies while preparing for entry-level cybersecurity certifications.

Weekly Curriculum

Week 1: Cybersecurity Foundations

- Understanding the cybersecurity landscape
- CIA Triad: Confidentiality, Integrity, Availability
- Threat actors and attack vectors
- Security governance frameworks (NIST CSF, ISO 27001)
- Risk management fundamentals

Hands-on Lab:

- Threat intelligence analysis with VirusTotal
- Creating security policies for a mock organization

Week 2: Network Security Essentials

- TCP/IP model and key protocols
- Network segmentation strategies
- Firewalls and intrusion detection systems
- Common network attacks (MITM, DDoS, DNS poisoning)
- Secure network design principles

Hands-on Lab:

- Wireshark traffic analysis
- Configuring VLANs in Cisco Packet Tracer

Week 3: Identity & Access Management

- Authentication methods (MFA, biometrics)
- AAA framework (Authentication, Authorization, Accounting)
- Role-Based Access Control (RBAC)
- Active Directory fundamentals
- Cloud IAM concepts

> **Hands-on Lab:**
>
> - Configuring Group Policy in Windows Server
> - Implementing MFA in a cloud environment

Week 4: Threat Defense & Endpoint Security

- Malware types and analysis
- Endpoint protection solutions (AV, EDR, XDR)
- Defense in depth strategy
- MITRE ATT&CK framework
- Vulnerability management

> **Hands-on Lab:**
>
> - Malware analysis in sandboxed environment
> - Using Sysinternals for process monitoring

Week 5: Security Operations

- SOC roles and responsibilities
- SIEM fundamentals and log analysis
- Incident response lifecycle
- Threat hunting techniques
- Digital forensics basics

> **Hands-on Lab:**
>
> - Splunk log analysis exercise
> - Incident response simulation

Week 6: Governance & Compliance

- Security policies and standards
- Risk assessment methodologies
- Compliance frameworks (GDPR, HIPAA, PCI-DSS)
- Business continuity planning

- Career pathways in cybersecurity

> **Hands-on Lab:**
>
> - Creating a risk assessment matrix
> - Developing an incident response plan

Certification Alignment

Certification	Covered Domains	Preparation Level
ISC2 Certified in Cybersecurity (CC)	All 5 domains	Complete preparation
Cisco CyberOps Associate	Security monitoring, host-based analysis	Partial coverage
CompTIA Security+	Threats, attacks, architecture	Foundation level

Required Tools & Resources

Tool	Purpose	Download Link
VirtualBox	Virtualization platform	https://www.virtualbox.org/
Kali Linux	Security testing platform	https://www.kali.org/get-kali/
Wireshark	Network protocol analyzer	https://www.wireshark.org/
Splunk	SIEM platform	https://www.splunk.com/
MITRE ATT&CK	Threat framework	https://attack.mitre.org/

Capstone Project

Students will complete a comprehensive security assessment of a mock organization, including:

- Network vulnerability scan
- Security policy review
- Incident response simulation
- Risk assessment report

Assessment Criteria

Component	Weight	Description
Weekly Labs	30%	Hands-on technical exercises
Quizzes	20%	Concept knowledge checks
Capstone Project	40%	Comprehensive security assessment
Participation	10%	Engagement in discussions