CodeCruise

SAIL SMOOTH IN TECH OCEAN

A74, TechnoPark, Andheri, Mumbai. Phone: +91 80809 75897 | +91 70345 62050 Email: ask@codecruise.in

Fundamentals of Cybersecurity

Fundamentals of Cybersecurity course is your gateway to the world of digital security. This comprehensive course is designed for anyone looking to build a solid foundation in cybersecurity, whether you're a tech enthusiast, a professional pivoting into the security field, or simply curious about how to protect yourself online.

Course Highlights:

- **Introduction to Cybersecurity:** Understand the basics of cybersecurity, including key concepts, terminologies, and the importance of protecting digital information.
- **Threats and Vulnerabilities:** Learn about common threats like malware, phishing, and ransomware, and explore various vulnerabilities that can be exploited by cybercriminals.
- **Security Best Practices:** Discover essential practices to enhance your personal and organizational security, such as creating strong passwords, using encryption, and implementing two-factor authentication.
- **Hands-On Labs:** Gain practical experience with interactive labs that simulate real-world cybersecurity scenarios, helping you apply what you've learned in a controlled environment.
- **Tools and Techniques:** Get acquainted with popular cybersecurity tools and techniques used by professionals to defend against attacks and secure systems.
- **Legal and Ethical Considerations:** Explore the legal and ethical aspects of cybersecurity, including privacy laws, regulations, and ethical hacking principles.

Why Choose This Course?

- **Beginner-Friendly:** No prior knowledge or experience in cybersecurity is required. This course is tailored for beginners, making complex concepts easy to understand.
- **Expert Instructors:** Learn from industry experts with extensive experience in the field of cybersecurity.
- **Flexible Learning:** Access course materials anytime, anywhere. Learn at your own pace with our self-paced modules.
- **Certification:** Earn a certificate upon completion to showcase your new skills and enhance your career prospects.

Tech Stack To Be Covered

Syllabus

Module 1: Basic Security Concepts

- **1.1 The CIA triad**: Learn about confidentiality, availability, and integrity. Also authenticity, nonrepudiation, and privacy.
- **1.2 Common cyber security threats**: Learn about the common cyber security threats facing individuals and organizations.
- **1.3 Understanding risk management**: Learn about assessing and understanding risk – impact/likelihood and implementing controls.
- **1.4 Security practices and documentation**: Learn about the difference between policies, procedures, standards, and regulations/laws.
- **1.5 The shared responsibility model**: What is the shared responsibility model and how does it affect cyber security?
- **1.6 Zero trust**: Learn about what is zero trust and how does it affect architecture? What is defense in depth?

Module 2: Identity & Access Management Fundamentals

- **2.1 IAM key concepts**: Learn about the principle of least privilege, segregation of duties, how IAM supports zero trust.
- **2.2 IAM zero trust architecture**: Learn about how identity is the new perimeter for modern IT environments and the threats it mitigates.
- **2.3 IAM capabilities**: Learn about IAM capabilities and controls to secure identities.

Module 3: Network Security Fundamentals

- **3.1 Networking key concepts**: Learn about networking concepts (IP addressing, port numbers, encryption, etc.)
- **3.2 Networking zero trust architecture**: Learn about how networking contributes to an E2E ZT architecture and the threats it mitigates.
- **3.3 Network security capabilities**: Learn about network security tooling – firewalls, WAF, DDoS protection, etc.

Module 4: Security Operations Fundamentals

- **4.1 SecOps key concepts**: Learn about why security operations are important and how it differs from normal IT ops teams.
- **4.2 SecOps zero trust architecture**: Learn about how SecOps contributes to an E2E ZT architecture and the threats it mitigates.
- **4.3 SecOps capabilities**: Learn about SecOps tooling – SIEM, XDR, etc.

Module 5: Application Security Fundamentals

- **5.1 AppSec key concepts**: Learn about AppSec concepts such as secure by design, input validation, etc.
- **5.2 AppSec capabilities**: Learn about AppSec tooling: pipeline security tools, code scanning, secret scanning, etc.

Module 6: Infrastructure Security Fundamentals

- **6.1 Infrastructure security key concepts**: Learn about hardening systems, patching, security hygiene, container security.

- **6.2 Infrastructure security capabilities**: Learn about tooling that can assist with infrastructure security e.g. CSPM, container security, etc.

Module 7: Data Security Fundamentals

- **7.1 Data security key concepts**: Learn about data classification and retention and why this is important to an organization.
- **7.2 Data security capabilities**: Learn about data security tooling – DLP, inside risk management, data governance, etc.

Module 8: AI Security Fundamentals

- **8.1 AI security key concepts**: Learn about the differences and similarities between traditional security and AI security.
- **8.2 AI security capabilities**: Learn about AI security tooling and the controls that can be used to secure AI.
- **8.3 Responsible AI**: Learn about what responsible AI is and AI-specific harms that security professionals need to be aware of.