Cyber Security

TS
TECH TEACH
EDUCATIONALSOLUTIO

OUR MISSION :

"Our mission is to empower learners worldwide through innovative technology, personalized learning experiences, and accessible educational resources. We strive to cultivate a community where every individual can achieve their full potential, regardless of their background or circumstances."

OUR VALUES :

"To pioneer the future of education by leveraging cutting-edge technology to make learning more engaging, effective, and inclusive. We envision a world where education transcends boundaries, creating opportunities for lifelong learning and fostering a society enriched by knowledge and creativity."

COURSE CURRICULUM:

Week 1: Introduction to Cybersecurity

- Day 1-2: Orientation and Overview
  - Introduction to the organization and its cybersecurity team
  - Overview of the cybersecurity field
  - Importance of cybersecurity in today’s digital age
- Day 3-4: Basic Concepts
  - Understanding networks and the internet
  - Fundamentals of information security (CIA Triad: Confidentiality, Integrity, Availability)
  - Common cybersecurity terminologies
- Day 5: Cybersecurity Threat Landscape
  - Types of cyber threats (malware, phishing, DDoS, etc.)
  - Overview of recent cyber-attacks and case studies

COURSE CURRICULUM:

Week 2: Network Security

- Day 1-2: Network Fundamentals
  - Introduction to network architecture (LAN, WAN, VPN, etc.)
  - TCP/IP model and OSI layers
- Day 3-4: Network Security Measures
  - Firewalls and intrusion detection/prevention systems
  - Network monitoring and traffic analysis
- Day 5: Hands-on Lab
  - Setting up and configuring a basic firewall
  - Network scanning using tools like Nmap

COURSE CURRICULUM:

Week 3: System Security

- Day 1-2: Operating System Security
  - Securing Windows and Linux systems
  - Patch management and system hardening
- Day 3-4: Endpoint Security
  - Antivirus and anti-malware solutions
  - Endpoint detection and response (EDR) tools
- Day 5: Hands-on Lab
  - Configuring security settings on a Windows/Linux machine
  - Simulating malware detection and response

COURSE CURRICULUM:

Week 4: Application Security

- Day 1-2: Secure Software Development
  - ○ Secure coding practices and common vulnerabilities (OWASP Top 10)
  - ○ Code review and static analysis tools
- Day 3-4: Web Application Security
  - ○ Introduction to web application vulnerabilities (SQL injection, XSS, CSRF, etc.)
  - ○ Security testing methodologies (DAST, SAST)
- Day 5: Hands-on Lab
  - ○ Conducting a basic web application penetration test
  - ○ Using tools like Burp Suite and OWASP ZAP

COURSE CURRICULUM:

Week 5: Identity and Access Management (IAM)

- Day 1-2: IAM Fundamentals
  - Authentication vs. authorization
  - Single Sign-On (SSO), Multi-Factor Authentication (MFA)
- Day 3-4: Access Control Models
  - Role-Based Access Control (RBAC)
  - Least privilege and zero trust models
- Day 5: Hands-on Lab
  - Configuring IAM policies in a cloud environment (e.g., AWS IAM)
  - Implementing MFA for a web application

COURSE CURRICULUM:

Week 6: Incident Response and Forensics

- Day 1-2: Incident Response Planning
  - Incident response lifecycle (preparation, detection, containment, eradication, recovery, lessons learned)
  - Building an incident response team
- Day 3-4: Digital Forensics
  - Introduction to digital forensics tools and techniques
  - Forensic investigation process
- Day 5: Hands-on Lab
  - Simulating a cyber incident and response
  - Conducting a basic forensic analysis

COURSE CURRICULUM:

Week 7: Cloud Security

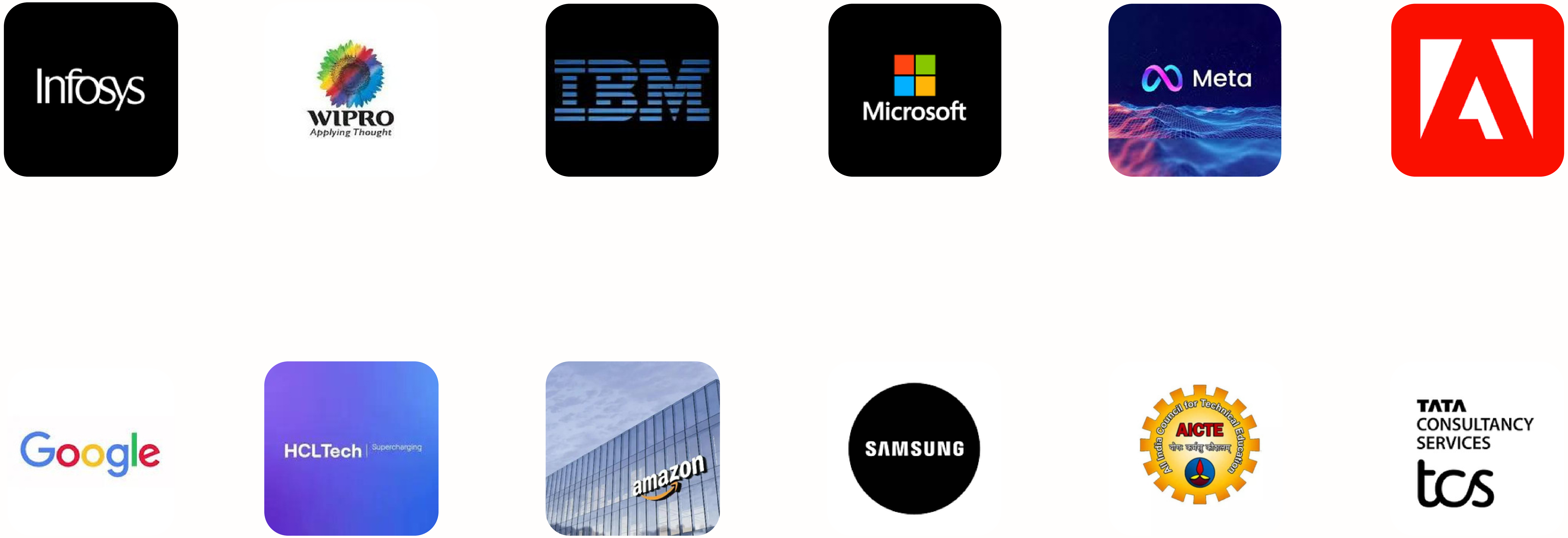
- Day 1-2: Cloud Security Fundamentals
  - Overview of cloud service models (IaaS, PaaS, SaaS)
  - Shared responsibility model
- Day 3-4: Securing Cloud Environments
  - Cloud security best practices
  - Cloud-native security tools
- Day 5: Hands-on Lab
  - Configuring security settings in a cloud environment (e.g., AWS, Azure, GCP)
  - Conducting a cloud security assessment

COURSE CURRICULUM:

Week 8: Capstone Project and Presentation

- Day 1-4: Capstone Project
  - Interns work on a comprehensive cybersecurity project that incorporates elements from previous weeks
  - Possible projects: Developing a security policy, conducting a full security assessment, or creating a security awareness program
- Day 5: Presentation and Feedback
  - Interns present their projects to the cybersecurity team and receive feedback
  - Wrap-up session and discussion on career paths in cybersecurity

Our Partners Company's



TS

TECH TEACH

EDUCATIONALSOLUTIO

FOR SUPPORT

+91 9652379012

www.techteachedsols.com

tech.ed.sols@gmail.com

THANK YOU

www.techteachedsols.com