Bsates

Cyber Security

in collaboration with ST IIT Bombay

Duration

2 Days

14 Hours of Learning

Venue

Indian Institute of Technology, IIT Delhi

Introduction

This workshop has been designed to provide a holistic learning experience. The curriculum balances theoretical knowledge and hands-on practice, ensuring participants gain both foundational understanding and practical expertise. Interactive sessions, real- world use cases, and collaborative hackathons help embed key concepts effectively. The structured flow, from basic concepts to advanced applications, caters to diverse learning paces while promoting teamwork and problem-solving. This methodology ensures a robust, engaging, and outcome-driven learning journey for all participants.

3rd Floor, Forum, DLF cyber city, DLF Phase 3, Sector 24, Gurugram, Haryana 122002

DAY 1: Fundamentals and Core Concepts

Session 1: Introduction to Cybersecurity)

Topics:

- What is Cybersecurity & its importance
- CIA triad (Confidentiality, Integrity, Availability)
- Types of cyber threats: Malware, Phishing, Ransomware, Social engineering
- Cybersecurity trends & global cyber incidents

Outcome: Participants understand the basics of cybersecurity, threat landscape, and the need for strong security measures.

Session 2: Network Security Essentials

Topics:

- Basics of computer networks (TCP/IP, ports, protocols)
- Firewalls, Intrusion Detection & Prevention Systems (IDS/IPS)
- Secure network architecture & VPNs

Hands-on Activity: Using Wireshark to analyze network packets

Outcome: Participants gain practical exposure to securing networks and identifying suspicious traffic.

Session 3: Cryptography & Data Protection

Topics:

- Encryption basics (symmetric vs. asymmetric)
- Hashing & digital signatures
- SSL/TLS & HTTPS security
- Password management & secure authentication

Hands-on Activity: Encrypting and decrypting messages using open-source tools
Outcome: Participants understand how encryption protects data and practice basic cryptography.

Session 4: Web Application Security

Topics:

- OWASP Top 10 vulnerabilities (SQL Injection, XSS, CSRF, etc.)
- Safe coding practices
- Penetration testing basics

Hands-on Activity: Demonstration of a simple SQL Injection & its prevention
Outcome: Participants recognize common web vulnerabilities and learn defense mechanisms.

Wrap up & Reflection

Recap of Day 1 Concepts
Review the day's activities and key learnings.

Q&A Session
Open discussion for clarifications.

Preview of Day 2
Overview of Cyber attacks, Cloud & Mobile Security

Bsates

DAY 2: Advanced Practices and Applications

Session 5: Cyber Attacks & Defense Mechanisms

Topics:

- Anatomy of a cyber attack (attack lifecycle)
- Malware analysis basics
- Defense strategies (endpoint security, patch management, backups)

- Case Study: Real-world ransomware attack analysis
- Outcome: Participants understand how attacks unfold and how to design preventive defenses.

Session 6: Cloud & Mobile Security

Topics:

- Cloud computing risks & security models
- Mobile app vulnerabilities
- Secure configurations & multi-factor authentication

- Outcome: Participants learn key security practices for cloud and mobile environments.

Session 7: Cybersecurity Tools & Hands-on Practice

Topics:

- Introduction to tools: Nmap, Metasploit, Burp Suite
- Basic vulnerability scanning
- Ethical hacking overview

- Hands-on Activity: Scanning a test system for vulnerabilities
- Outcome: Participants develop basic skills in using professional cybersecurity tools.

Session 8: Cyber Laws, Ethics & Career Pathways

Topics:

- Indian IT Act, GDPR, and data protection laws
- Ethics in cybersecurity & responsible disclosure
- Career opportunities & certifications (CEH, CISSP, CompTIA Security+, etc.)

- Group Activity: Discussion on ethical dilemmas in cybersecurity
- Outcome: Participants become aware of legal frameworks, ethical responsibilities, and career options in cybersecurity.

Workshop Outcomes

By the end of the 2 days, participants will be able to:

✅ Understand fundamental cybersecurity concepts & threats

✅ Identify and mitigate network & web vulnerabilities

✅ Use basic cybersecurity tools for scanning & testing

✅ Recognize real-world cyberattacks and defense strategies

✅ Apply ethical & legal perspectives in cybersecurity practices

✅ Explore career opportunities and future learning paths

What Next ?

For Students:

- Enroll in cybersecurity MOOCs (Coursera, edX, Cybrary)
- Join Capture The Flag (CTF) competitions
- Start with beginner-friendly tools like Wireshark & TryHackMe

For Professionals:

- Aim for certifications (CompTIA Security+, CEH, CISSP depending on role)
- Participate in bug bounty programs (HackerOne, Bugcrowd)
- Stay updated with cybersecurity news & threat intelligence reports

Bsates

3rd Floor, Forum, DLF cyber city, DLF Phase 3, Sector 24, Gurugram, Haryana 122002