Cyber Security - Persona- Freshers (Bootcamp)

Basic Level

Duration – 50 Hours

Program Description

The Basic Level Cyber Security program introduces freshers to foundational concepts in cybersecurity. Covering essential areas such as network security, risk management, penetration testing, and identity management.

This course equips learners with the skills required to understand and mitigate basic security risks. It also covers digital forensics and the legal aspects of cybersecurity, helping participants develop a holistic view of the cybersecurity landscape.

Learning Goals

- Understand the fundamentals of network security and how to protect digital assets.
- Learn risk management strategies for identifying and addressing potential security threats.
- Gain knowledge in identity and access management to secure sensitive data.
- Develop skills in basic penetration testing and incident response processes.
- Explore web application security and digital forensics.
- Learn how to report, log, and audit security incidents, and understand the relevant legal frameworks.

Course Topics

- Introduction to Network Security.
- Risk Management principles and practices.
- Identity and Access Management.
- Basics of Penetration Testing.
- Understanding the Incident Response Process.
- Web Application Security fundamentals.
- Digital Forensics techniques.
- Reporting, Logging, Auditing, and Cybersecurity Laws.

Intermediate Level

Duration – 70 Hours

Program Description

The Intermediate Cyber Security Bootcamp is designed for individuals with foundational knowledge looking to deepen their skills. This course dives into Java security, API security, cryptography, vulnerability assessments, and penetration testing.

Participants will also learn to manage concurrency and session security, team collaboration in cyber ranges, and advanced threat landscape concepts. It is an intensive bootcamp that prepares learners to handle more complex security challenges.

Learning Goals

- Develop a deep understanding of security in Java, including I/O packages, authentication, and cryptography.
- Learn how to implement API security and secure communication channels.
- Gain expertise in vulnerability assessment and penetration testing.
- Understand concurrency and session management to secure applications.
- Learn to handle error logging and implement security best practices in software.

Course Topics

- Security in Java I/O Package, Authentication, and Authorization.
- API Security and Java Cryptography.
- Concurrency and Session Management.
- Error Handling and Logging in applications.
- OWASP Top 10 vulnerabilities and best practices.
- Vulnerability Assessment and Penetration Testing techniques.
- Cyber range collaboration and team roles.
- Threat Landscape, Zero Trust Architecture, and Advanced Persistent Threats.

Advance Level

Duration – 150 Hours

Program Description

The Advanced Level Cyber Security program is tailored for individuals looking to specialize in high-level security strategies. It covers incident response, business continuity planning, endpoint security, and advanced threat mitigation techniques.

This course focuses on building robust security systems with an emphasis on advanced threat landscapes, zero trust architecture, and persistent threats. Learners will also gain skills in Security Information and Event Management (SIEM) for monitoring and managing security events.

Learning Goals

- Master incident response techniques and managing post-incident aftermath.
- Learn how to design and implement business continuity plans to ensure operations during a crisis.
- Explore endpoint security solutions and Security Information and Event Management (SIEM).
- Understand and address advanced threats, including zero-trust architecture and persistent threats.
- Develop strategies for defending against advanced threat landscapes in real-world scenarios.

Course Topics

- Incident Response and handling post-incident aftermath.
- Business Continuity Planning for crisis management.
- Endpoint Security strategies for protecting devices.
- Security Information and Event Management (SIEM).
- Advanced Threat Landscape and mitigation techniques.
- Zero Trust Architecture for enhancing security posture.
- Handling Advanced Persistent Threats (APTs).

The modules will be tailored to address UPS-specific supply chain problem statements