Cyber Security - Persona - Laterals (Skill Upgrade)

Foundation - 101

Duration – 50 Hours

Program Description

The Foundation - 101 course provides a comprehensive introduction to core cybersecurity concepts for lateral professionals. Participants will learn about computer architecture, networking, virtualization, and key cybersecurity fundamentals.
This course is designed to establish a solid foundation, covering the basics of cyber threats, attacks, and enterprise network architecture.

Learning Goals

- Understand the architecture of computers and operating systems in the context of cybersecurity.
- Learn the basics of networking concepts and how they apply to security.
- Gain an understanding of virtualization and its role in modern security systems.
- Explore key cybersecurity fundamentals, including architectural vulnerabilities and cyber threats.
- Learn about enterprise network architecture and how it can be secured.

Course Topics

- Computer Architecture and Operating Systems for Cybersecurity.
- Networking Concepts and fundamentals.
- Introduction to Virtualization and its security implications.
- Key Cyber Security Fundamentals.
- Identifying Architectural Vulnerabilities.
- Understanding Enterprise Network Architecture.
- Overview of Cyber Threats and Attacks.

Core - 201

Duration – 75 Hours

Program Description

The Core - 201 program is designed for professionals looking to upgrade their skills and deepen their understanding of cybersecurity. This course focuses on threats and threat vectors, intelligence gathering, and advanced threat modeling methodologies such as STRIDE, OCTAVE, and DREAD.
Learners will also explore risk assessment, threat hunting, and operating system security controls, giving them the skills to identify and manage risks effectively.

Learning Goals

- Learn how to classify threats and identify threat vectors.
- Gain expertise in intelligence gathering and threat modeling methodologies (STRIDE, OCTAVE, DREAD).
- Understand how to conduct threat hunting and analyze potential security threats.
- Develop skills in risk assessment, determination, and management.
- Explore the role of business environment and governance in cybersecurity.
- Learn about securing operating systems through hardware hardening and security controls.

Course Topics

- Threats and Threat Vector Classification.
- Intelligence Gathering Techniques.
- Threat Modeling Methodologies: STRIDE, OCTAVE, DREAD.
- Conducting Threat Hunting and Threat Analysis.
- Risk Assessment and Management Strategies.
- Understanding Business Environment and Governance.
- Operating Systems Hardware and Hardening Techniques.
- Application Information Security Controls.

Advance - 301

Duration – 60 Hours

Program Description

The Advance - 301 program is aimed at professionals ready to tackle advanced cybersecurity topics. This course covers secure software development lifecycles (SDLC), application security controls, and advanced network security techniques. Participants will explore security in CI/CD environments, API security, Java cryptography, and vulnerability assessment.
The program also emphasizes team collaboration and simulating cyber-attacks to prepare for real-world challenges.

Learning Goals

- Master advanced application information security controls and secure SDLC processes.
- Understand how to secure modern CI/CD environments and perform API security.
- Learn how to identify and mitigate application vulnerabilities.
- Explore Java security, cryptography, and session management in-depth.
- Gain expertise in advanced penetration testing and vulnerability assessment.
- Develop skills in team collaboration for simulating and responding to cyber-attacks.

Course Topics

- Secure SDLC (Software Development Life Cycle) Practices.
- Advanced Application Information Security Controls.
- Advanced Network Security Strategies.
- Securing CI/CD (Continuous Integration/Continuous Deployment) Environments.
- Application Vulnerability Assessment and Penetration Testing.
- Security in Java I/O Package and Cryptography.
- Concurrency and Session Management in Applications.
- API Security and Authentication/Authorization.
- Error Handling and Logging in Secure Systems.
- OWASP Top 10 Vulnerabilities.
- Roles and Responsibilities of Cyber Teams.
- Team Collaboration and Cyber Attack Simulations.

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