Information Security Fundamentals

Duration: 1 day

- **Introduction to Information Security**
  - Definition and Objectives of Information Security
  - Importance of Information Protection in Organizations
  - Key Terms and Concepts
- **The CIA Triad – Core Principles**
  - **Confidentiality**: Purpose and Implementation Examples
  - **Integrity**: Data Consistency, Detection Mechanisms
  - **Availability**: Concepts of Uptime and Reliability
  - Interdependencies and Balance Among the Principles
- **Understanding the Threat Landscape**
  - Threat vs Risk vs Vulnerability
  - Classification of Threats (Internal, External, Accidental, Intentional)
  - Common Threat Actors and Their Characteristics
  - Typical Threat Vectors (e.g., Phishing, Malware, Network Intrusion)
- **Types of Vulnerabilities**
  - Technical Vulnerabilities: Software Bugs, Misconfigurations
  - Human Vulnerabilities: Social Engineering, Unintentional Errors
  - Organizational and Process Weaknesses
- **Basic Risk Concepts in Information Security**
  - Core Definitions and Formula: Risk = Threat × Vulnerability × Impact
  - Identification and Categorization of Risks
  - Examples of Risk Scenarios in IT Environments
- **Security Control Categories**
  - Preventive, Detective, and Corrective Controls
  - Technical Controls: Access Control, Encryption, Firewalls
  - Administrative and Physical Controls
  - Role of Policies and Security Awareness
- **Overview of Security Standards and Frameworks**
  - Purpose and Benefits of Security Standards
  - Introduction to ISO/IEC 27001 and NIST Cybersecurity Framework (Conceptual)
  - Alignment of Controls with Organizational Needs

- **MITRE ATT&CK Framework**
    - Introduction to the MITRE ATT&CK Framework
    - Understanding TTPs (Tactics, Techniques, and Procedures)
    - Using MITRE for proper alert handling and incident response
- **Best Practices for Secure Data Handling**
    - Encryption, Data Masking, and Secure Storage Practices
    - Secure Data Sharing and Disposal
- **Mobile Security**
    - Securing Mobile Devices and Apps
    - Mobile Device Management (MDM) Policies
- **Basic Cyber Hygiene Practices**
    - Purpose and Benefits of Security Standards
    - Regular Software Updates and Patch Management
    - Strong Authentication and Password Management
    - Monitoring and Incident Reporting
- **Review and Summary**
    - Recap of Key Concepts
    - Clarifications and Final Q&A