Modules	Content Coverage
Module 1: System Fundamentals	Enterprise Architecture, Computer Architecture and Components, Operating System Basics, Networks and Services Basics, Application and Database Fundamentals, Virtualisation and its Components, Cloud Fundamentals
Module 2: Need for Cyber Security	Overview of Cyber Security, Types of Cyber Attacks, Ecosystem of Cyber Security
Module 3: Introduction to Cyber Security	Fundamentals of Information Security, Understanding Threats, Attack Categories and Hacking Process, Understanding the Network Security Basics of Cryptography, Fundamentals of Web/Mobile Application Security, Data Centre Security, Cloud Computing and Data Security
Module 4: Network Security Threats and Countermeasures	Types of Firewall, Inspection Techniques, Layers, Protocols and ports, Firewall Features, Network Level Attacks and Detection Techniques, Security Recommendations, Countermeasures and Security Baseline, Network Analysis and Monitoring
Module 5: Cryptography	Introduction to Cryptography, Types of Cryptography, Uses of Cryptography, Understanding Digital Certificate and Signature, Application of Cryptography in Real World, Cryptographic Attacks
Module 6: Web Server and Application Security	Web Application Architecture, Vulnerabilities in Web Server and Applications, Proxy Setup, Testing Methodology, Secure Coding practices, Identity and Access Management, OWASP Testing Guide 4.1 Mitigation Techniques and Reporting, Web Application Vulnerability Scanning Tools, Burp Suite Intruder/Repeater, Bug Bounty Programs and Certifications
Module 7: Security Auditing and SOC	Basic Understanding towards Auditing, Basic Understanding of Risk Management, Importance of Digital Footprint, Understanding the Importance of Log Analysis, Reporting the Audit Findings, SOC activity
Module 8: Introduction to Cyber Forensics	Overview of Cyber Forensics, Cyber Kill Chain, Phases of Cyber Forensics Recognise How a Cyber Attack Happens