
1. Microsoft & Data Security Council of India have jointly under the aegis of the Ministry of Electronics & IT (MeitY)-Initiative- Information Security Education & Awareness (ISEA) are launching Project CyberShikshaa for skilling women engineering graduates in the niche field of Cyber Security. C-DAC being R&D institution for the design, development and deployment of electronic and ICT technologies, would be conducting training programs exclusively for women and also making them industry ready by imparting the requisite technical skills in the domain of Cyber Security, in association with National Institute of Electronics & Information Technology (NIELIT). The program shall also entail placement assistance for the deserving candidates with the potential recruiters looking to hire for various job roles in Cyber Security.

2. This Skills Development Initiative will act as catalyst for change with access to opportunities to all deserving women candidates enrolled for the program.

The Program details are:

Program Details : 04 MONTHS dedicated training program for women
No. of Participants : 500 WOMEN to be trained during First Phase
Location/Agency : C-DAC Centres of Noida, Mohali, Hyderabad and NIELIT Patna.
Course Fee : Free

The eligibility criteria are:

i. Exclusive for Women
ii. Engineering Graduates
iii. Age Bracket -21 to 26 Years Old
iv. Family Income Less than 5 Lacs per annum
Pre-requisites:
Operating systems concept, computer network, fundamentals of algorithms and data structure, Programming skills (C / C++), PHP, JavaScript, Windows usage, Linux usage, Basics of scripting languages.

Module 1: System Fundamentals

Module 2: Introduction to cyber security
Fundamentals of information security - CIA Triad, Cyber Security Controls, understanding threats, attacks categories, hacking process, Understanding the network security, basics of cryptography, fundamental of web/mobile application security, data centre security, cloud computing and data security.

Module 3: Cryptography
Introduction to cryptography, Symmetric-Asymmetric cryptography & cryptographic algorithms, Hash functions, Applications of cryptography- IPsec, Pretty Good Privacy, Secure Socket Layer (SSL), TLS Understanding digital certificates and signatures.

Module 4: Network Security and countermeasures
Introduction to network security – topology, Network configuration, understanding ports, protocols - TCP/IP, UDP, ARP, Operational processes, Network scanning, understanding packets and network specific attacks, vulnerabilities, DMZ, Packet filtering, firewalls, Iptables, TMG threat management gateway, network security tools (scanners, sniffers etc) and countermeasures

Module 4: Web Server and Application Security
Client-Server Relationship, Vulnerabilities in web server and applications, Attack methods- Buffer overflow, SQL injection, cross side scripting, session hijack etc., Secure Coding Practices, OWASP top 10 vulnerabilities and mitigation techniques, Web Application vulnerability scanning tools (Nesus), Web application security challenges.

Module 5: Security Auditing
Audit planning (scope, pre-audit planning, data gathering, audit risk), Risk management, Risk analysis, 3 phase approaches – Risk assessment, mitigation and reassessment, Log analysis, OS auditing: Windows auditing, Linux auditing and Device auditing.

Module 6: Cyber Forensics
Cyber Forensics phases (Preservation, Identification, Extraction, Documentation, Interpretation), EDR, tools and standard operating procedures for Disk forensics, Social media and network forensics, Mobile and CDR forensics.