एसटीपीआई STPI | SAHAYAK Beyond Academics



TECHNOLOGY SKILLING & EMPLOYABILITY INITIATIVE

Proposer:

iact™ Makes Computer Learning Easy

BUILDING SKILLS | ENHANCING EMPLOYABILITY | TRANSFORMING LIVES

PROPOSED INDUSTRY-READY TRAINING PROGRAMMES

CYBERSECURITY – INTERMEDIATE

PROGRAMME POSITIONING

The proposed Cybersecurity – Intermediate programme is designed as an affordable, industry-oriented professional training programme for students, graduates and early-career learners seeking practical skills in cybersecurity, network security, system security, vulnerability management, security monitoring and incident response.

The 300-hour structured learning pathway, delivered over 12–14 weeks, provides learners with an intermediate-level understanding of cybersecurity concepts while maintaining a strong practical and application-oriented approach.

The curriculum covers key areas including network security, operating-system security, endpoint protection, identity and access management, vulnerability assessment, web and application security fundamentals, security monitoring, SIEM, threat intelligence, incident response, cloud security fundamentals and security automation.

The programme aims to bridge the gap between academic cybersecurity learning and industry requirements while developing practical competencies relevant to SOC, IT security, network security and cybersecurity support roles.

DURATION	TOTAL HOURS	PROPOSED FEE
12–14 Weeks	300 Hours	INR 18,000 – INR 20,000/-

PROGRAMME FOCUS

Cybersecurity fundamentals, network security, system and endpoint security, identity and access management, vulnerability assessment, web security, security monitoring, SIEM, threat intelligence, incident response, cloud security, security automation, hands-on laboratories and an industry project.

MODULE-WISE CURRICULUM

Module	Module Title	Hours
1.	Cybersecurity Fundamentals & Security Operations Cybersecurity concepts, CIA triad, threat landscape, attack surfaces, security controls, security policies, risk concepts, security operations and cybersecurity roles	25
2.	Networking & Network Security TCP/IP, OSI model, network protocols, ports and services, DNS, DHCP, routing concepts, firewalls, VPN, network segmentation, secure network architecture and network monitoring	35
3.	System & Endpoint Security Windows/Linux security, system hardening, user privileges, endpoint protection, access controls, patch management, secure configuration and endpoint monitoring	30
4.	Identity & Access Management Authentication, authorization, MFA, password security, RBAC, privileged access, account management, access policies and identity security	25
5.	Vulnerability Assessment & Security Testing Vulnerability concepts, CVE/CVSS fundamentals, vulnerability scanning, asset identification, risk classification, remediation, security testing methodology and reporting	30
6.	Web & Application Security Fundamentals Web architecture, HTTP/HTTPS, common web vulnerabilities, OWASP concepts, authentication/session security, input validation, secure coding principles and application security testing	30
7.	Security Monitoring & SIEM Security logs, log sources, event analysis, SIEM concepts, dashboards, correlation, alerts, detection rules, security monitoring and alert triage	35
8.	Threat Intelligence & Incident Response Threat intelligence concepts, IOC, TTPs, threat analysis, incident response lifecycle, incident identification, containment, eradication, recovery and incident reporting	32
9.	Cloud Security & Security Automation Cloud security fundamentals, IAM, cloud networking, security configuration, logging, shared responsibility, Python/scripting fundamentals and automation of routine security tasks	32
10.	Industry Project End-to-end cybersecurity project involving security assessment, monitoring, incident investigation or security implementation	18
	Total Hours	**300 Hours**

EMPLOYABILITY & CAREER READINESS PROGRAMME

Employability will be integrated as a parallel and continuous layer throughout the training programme, ensuring that learners develop both technical cybersecurity competencies and workplace-readiness skills.

Key Components

- Career orientation and cybersecurity career pathways
- Communication and interpersonal skills
- Workplace behaviour and professional conduct
- Professional etiquette and workplace readiness
- Resume development and optimisation
- AI-assisted resume development
- LinkedIn and professional profile development
- Cybersecurity interview preparation
- Technical interview practice
- Mock interviews and assessment simulations
- Group discussions and presentation skills
- Aptitude and employability assessment preparation
- Industry interactions and expert sessions
- Individual career counselling and mentoring
- Internship and experiential learning opportunities
- Employer engagement and industry connect
- Placement assistance and placement drives
- Entrepreneurship and self-employment orientation



IACT EDUCATION PVT. LTD.

D-306, West Vinod Nagar, IP Extension, New Delhi - 110 092

rajeev@iacteducation.com | www.iacteducation.com

Mob.: 98100 18664