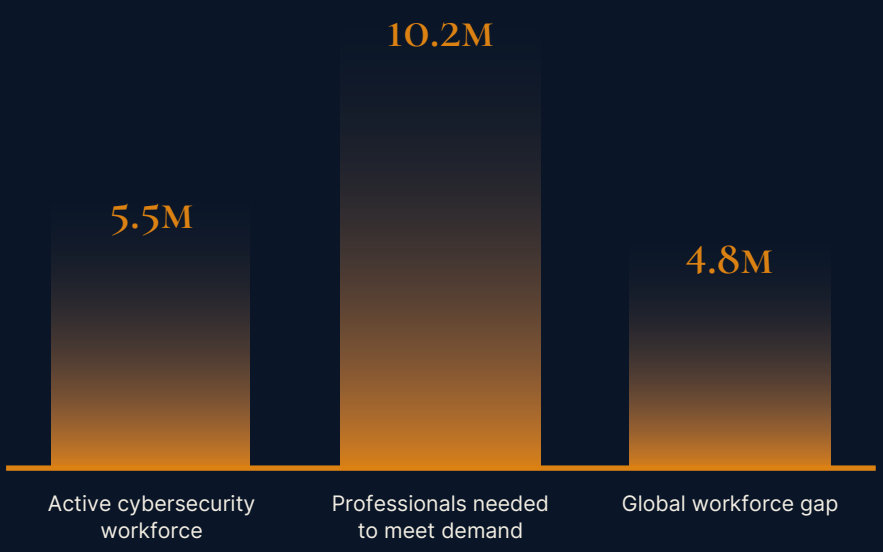
IITM PRAVARTAK
CATALYSING INNOVATION

TECHNOLOGY INNOVATION
HUB OF IIT MADRAS

Certificate Programme in Cybersecurity & Ethical Hacking in the AI Era

The world is short of 4.8 million cybersecurity professionals

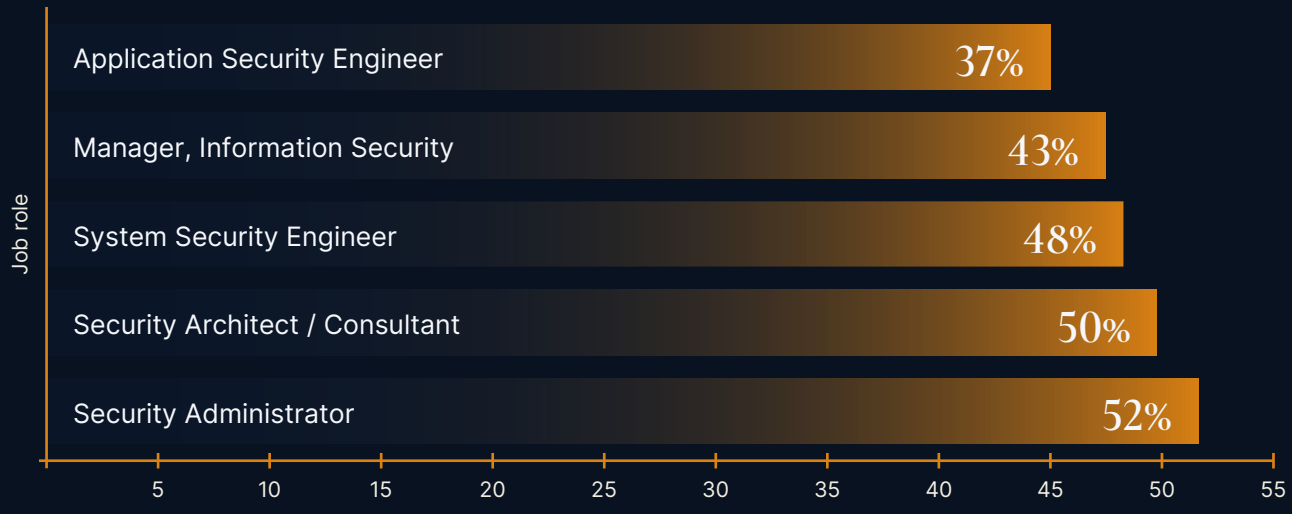
Global cybersecurity demand continues to outpace available talent



59%
of cybersecurity teams report a critical or significant skills gap in 2025

88%
of teams experienced at least one security consequence linked to skills gaps

Cybersecurity hiring is accelerating in India



Source: ISC2 Cybersecurity Workforce Studies 2024 & 2025 (n=16,029 in 2025; latest gap estimate: 2024); Naukri JobSpeak Index, Dec 2025 & June 2026

Programme highlights

IITM Pravartak Faculty Masterclasses	Exclusive live online masterclasses delivered by IITM Pravartak faculty
Live Online Sessions by Domain Experts	Weekly live sessions with industry experts featuring practical tools and real-world cybersecurity use cases
IITM Research Park Campus Immersion (Optional)	Two immersive 2-day campus experiences at IIT Madras Research Park
Industry Capstone Project	Pick one real Indian cyber breach scenario and build an end-to-end AI-powered cybersecurity solution
Networking Opportunities	Connect with IITM Pravartak faculty, industry experts and mentors to gain insights that can help advance your career

Certificate Eligibility

Minimum 65% overall attendance and 30% marks in the cumulative evaluation score

PEDAGOGY

How you learn

Live Online Classes
6 hours of live classes a week with practitioner faculty

Ethical Hacking and Defence
Learn to break into systems the way real attackers do, then defend them

Real Indian Breach Cases
Learn from cases like Star Health, JLR, Angel One and more

AI Copilot Workflows
Use AI tools like Claude and Security Copilot in everyday security work

Real-World Capstone
Work on real-world projects and scenarios

From Cloud to Boardroom
Understand data protection rules and learn to explain security risk

CAREER PATHWAYS

See where this programme takes you

Designed for where you are right now. Two specialised pathways, each built for your exact background, ambition, and career inflection point.

Tech Freshers · Students
& Recent CS/IT Graduates

Upskillers · 1–4 years
IT / DevOps / Cloud / Engineering

PROGRAMME JOURNEY

10-month learning pathway

PHASE 1	Foundation	Weeks 1–10 10 weeks
PHASE 2	Core & Immersion I	Weeks 11–28 18 weeks
PHASE 3	Industry Readiness	Weeks 29–37 9 weeks
PHASE 4	Capstone & Immersion II	Weeks 38–40 3 weeks

PHASE 1

Foundation

10 WEEKS · WEEKS 1 - 10

F1 : CYBER-ECONOMICS & INDIAN BREACH CASES (2 WEEKS)

Open the programme with the boardroom lens. Map attacker P&L economics across 5 Indian cases (Star Health, JLR, Angel One, Pune SME, BigBasket) covering five sectors and five attack types. Build a CyVaR model with an AI Breach Simulator and produce an industry-specific one-page Cyber Risk Briefing.

F2 : BUG TO RANSOMWARE: FIRST PRINCIPLES (2 WEEKS)

The 50-year chain from software bugs to memory corruption to exploits to malware to ransomware and the parallel detection stack (AV to IDS to EDR to SIEM). Write YARA and Snort rules. Trace Morris Worm to Stuxnet to WannaCry to LockBit as the foundational arc.

F3 : PROGRAMMING, AI PRIMER & AI CO-PILOT WORKFLOWS FOR SECURITY (2 WEEKS)

Python and Bash for security automation, REST APIs (VirusTotal, AbuseIPDB), AI/ML primer for security tooling. Use Cursor, Copilot, and Claude as daily coding partners with evaluation discipline – the 'prompt then verify' habit that prevents AI-generated security flaws from shipping.

F4 : NETWORKS, OS INTERNALS & IDENTITY (2 WEEKS)

OSI / TCP-IP, packet analysis with Wireshark, iptables firewall rules, Windows and Linux internals, Sysmon configuration and Active Directory architecture - the technical floor every defender and attacker is expected to have.

F5 : CRYPTOGRAPHY, THREAT INTEL & ATT&CK (2 WEEKS)

Cryptography fundamentals (symmetric, asymmetric, hashing, TLS, PKI). Threat intelligence at strategic, tactical, and operational levels. MITRE ATT&CK matrix, Kill Chain, OSINT primer, and threat modelling (STRIDE, PASTA). Map a real Indian breach (Cosmos Bank or AIIMS) to ATT&CK techniques.

TOOLS YOU'LL USE

PYTHON · BASH · WIRESHARK · NMAP · IPTABLES · SYSMON · YARA · SNORT · SONARQUBE · CURSOR · COPILOT · CLAUDE · MITRE ATT&CK NAVIGATOR · GOOGLE SHEETS (CYVAR)

PHASE 2

Core & Immersion I

18 WEEKS · WEEKS 11–28

C1 : RECON, SCANNING & WEB APPLICATION ATTACKS (2 WEEKS)

OSINT mastery (Shodan, Maltego, Recon-ng), Nmap scanning, OWASP Top 10 deep dive (SQL injection, XSS, CSRF, broken access control) and Burp Suite workflow on DVWA.

C2 : EXPLOITATION & POST-EXPLOITATION (2 WEEKS)

Metasploit framework end-to-end, password attacks (John, Hashcat), Meterpreter post-exploitation, Linux privilege escalation, and pivoting fundamentals.

C3 : AD ATTACKS, MALWARE ANALYSIS & AV EVASION (2 WEEKS)

BloodHound and SharpHound for AD attack paths, Kerberoasting, Pass-the-Hash, DCSync, Golden Ticket. Static and dynamic malware analysis with Ghidra. AV evasion through obfuscation and packing.

C4 : AI SECURITY & CTF PRACTICE (1 WEEK)

Adversarial ML (FGSM, PGD), OWASP LLM Top 10, prompt injection, deepfake detection, and full pentest cycle on OWASP Juice Shop with HackTheBox practice.

IMMERSION I

RED TEAM CTF CHALLENGE

An optional 2-day on-campus event at IIT Madras Research Park. Red Team CTF with reconnaissance through privilege escalation, AD compromise and final flag capture. Includes 1-on-1 GitHub portfolio review with mentors, industry panel with cybersecurity professionals from Indian industry and applied workshops on offensive and defensive craft.

C5 : SOC Operations & Microsoft Sentinel (2 WEEKS)
SOC tier model, SIEM architecture, Microsoft Sentinel workspace setup, log ingestion via Azure Monitor Agent, and KQL detection queries calibrated to ATT&CK techniques.

PHASE 2

C6 : THREAT HUNTING, EDR & INCIDENT RESPONSE (2 WEEKS)

Hypothesis-driven threat hunting, Microsoft Defender for Endpoint, advanced KQL with entity graphs, SANS PICERL incident response lifecycle, and ransomware IR simulation in Sentinel.

C7 : SOAR, PHISHING & AI-AUGMENTED SOC (1 WEEK)

Logic App playbooks for automated containment, Microsoft Security Copilot promptbooks for multi-stage attack analysis, phishing header analysis (SPF/DKIM/DMARC), and the SOC 2.0 operating model with human-in-the-loop controls.

C8 : CLOUD SECURITY, ZERO TRUST & MULTI-CLOUD (2 WEEKS)

Zero Trust architecture, Azure Entra ID, Conditional Access, Privileged Identity Management, Defender for Cloud (CSPM), Azure network security, IaC security with Terraform + Checkov, plus comparative coverage of AWS / GCP equivalents.

C9 : DEVSECOPS, CONTAINER & SUPPLY CHAIN SECURITY (1 WEEK)

CI/CD security in GitHub Actions (SAST/DAST/SCA), Trivy container scanning, Kubernetes hardening with pod security standards and RBAC, and software supply chain (SolarWinds analysis, SBOM, Sigstore signing).

C10 : OT AND ICS SECURITY FUNDAMENTALS (2 WEEKS)

Operational Technology and ICS security fundamentals. OT versus IT architecture, the Purdue Enterprise Reference Architecture, ICS components (PLC, RTU, HMI, SCADA), OT protocols (Modbus, DNP3, OPC-UA), the IT/OT convergence risk and the OT incident chain from Stuxnet through the JLR breach. NIST SP 800-82 and IEC 62443 frameworks, passive OT vulnerability assessment, OT-specific incident response, and Indian regulatory context (CEA cybersecurity guidelines for the power sector, MeitY guidance on critical infrastructure).

TOOLS YOU'LL USE

BURP SUITE · METASPLOIT · BLOODHOUND · GHIDRA · HACKTHEBOX · MICROSOFT SENTINEL · KQL · DEFENDER XDR · LOGIC APPS · SECURITY COPILOT · AZURE (ENTRA, CONDITIONAL ACCESS, DEFENDER FOR CLOUD) · TERRAFORM · CHECKOV · TRIVY · KUBERNETES · ICS-CERT ADVISORIES · IEC 62443 REFERENCES

PHASE 3

Industry Readiness

9 WEEKS · WEEKS 29–37

I1 : AI FOR CYBERSECURITY DEEP (2 WEEKS)

ML for anomaly detection (Isolation Forest, autoencoders), NLP for phishing detection (BERT classifier), agentic AI architecture for security workflows with human-in-the-loop gates and RAG over security knowledge bases (FAISS + embeddings) with hallucination-defence discipline.

I2 : AI PRODUCT SECURITY & RED TEAMING (2 WEEKS)

Building secure AI products as a security professional – LLM red teaming, adversarial ML defence (FGSM/PGD with adversarial training), AI security audit frameworks, ISO 42001 AI management system principles and MITRE ATLAS mapping.

I3 : ISO 27001 & RISK MANAGEMENT (2 WEEKS)

ISMS structure (Clauses 4-10), Annex A 93 controls, statement of applicability, risk assessment process, audit evidence standards, and a mock ISO 27001 audit on a sample organisation with non-conformity raising.

I4 : DPDP ACT, PRIVACY & GRC OPERATIONS (2 WEEKS)

DPDP Act 2023 deep dive (data fiduciary obligations, consent architecture, data principal rights, Section 9 minor protection), 72-hour CERT-In reporting, vendor risk management, and AI-assisted compliance artefact drafting (AI-augmented breach notification with human review).

I5 : CYBER RISK STRATEGY & BOARDROOM COMMUNICATION (1 WEEK)

Translating technical risk into financial language, CyVaR in board reports, cyber insurance fundamentals, sector-specific obligations (RBI, SEBI, IRDAI, MeitY) and stakeholder communication for the CISO seat, the boardroom layer that distinguishes a security professional from a security operator.

PHASE 3 • CAPSTONE & IMMERSION II

AI-ACCELERATED INCIDENT RESPONSE ON AN INDIAN BREACH SCENARIO

An optional 2-day on-campus event at IIT Madras Research Park. Red Team CTF with reconnaissance through privilege escalation, AD compromise and final flag capture. Includes 1-on-1 GitHub portfolio review with mentors, an industry panel with cybersecurity professionals from Indian industry and applied workshops on offensive and defensive craft.

- STAR HEALTH-STYLE
  Healthcare data exfiltration
- JLR-STYLE
  Manufacturing IT/OT ransomware
- ANGEL ONE-STYLE
  Fintech cloud misconfiguration
- PUNE SME-STYLE
  SME ransomware double extortion
- BIGBASKET-STYLE
  E-commerce credential breach

Note: Due to the evolving nature of the industry expectations and partner institute feedback, some syllabus aspects may change. Any updates will be communicated during the course of the programme. The project deliverables or case studies for your batch may differ, as per the decision of the institute or course faculty.

YOUR PORTFOLIO

Graduate with proof, not just a certificate

Six published artefacts you can choose to work on.

01

Cyber Risk Briefing for the Boardroom

A business-style report that puts a rupee value on a company's cyber risk, built on real Indian breach cases.

RISK · COMMUNICATION

02

Ethical Hacking Report

A full penetration testing report: find the weaknesses in a target system the way an attacker would, then show how to fix them.

ETHICAL HACKING · PENETRATION TESTING

03

Security Operations & Incident Response Pack

Detect, investigate, and respond to a live attack using the same tools (Microsoft Sentinel) real security teams use.

CYBER SECURITY · AI

04

Cloud Security Project

Secure a modern cloud setup against misconfiguration and attack, the way Indian product companies need.

CLOUD SECURITY · DEVSECOPS

05

AI for Security Project

Use AI to spot threats and speed up response, the skill that sets a 2026 security professional apart

AI SECURITY · AUTOMATION

06

Capstone: AI-Powered Breach Response

Respond end-to-end to a real Indian breach scenario, from detection to a leadership report.

CAPSTONE · END-TO-END DEFENCE

FACULTY & MENTORS

Learn from those who've done it

Prof. Dr. Noor Mahammad SK

IIITDM Kancheepuram

An Associate Professor and Head of the Department of Computer Science and Engineering at IIITDM Kancheepuram. He earned his PhD in Computer Science and Engineering from IIT Madras, along with an MTech in Electronics Design Technology and a BTech in Electronics and Communication Engineering. With over 22 years of teaching and 20 years of research experience, his expertise spans Computer Architecture, Reconfigurable Computing, VLSI Design, Network System Design, Hardware for AI, High-Performance Computing and Digital Signal Processing. He leads the High Performance Reconfigurable Computing System Engineering (HPRCSE) Group at IIITDM Kancheepuram and has successfully led multiple sponsored research and industrial consultancy projects while mentoring doctoral scholars and advancing research in next-generation computing systems.

Mr. Syed Mohamed A

Guest Faculty, IITM Pravartak

Mr. Syed Mohamed A is a Guest Faculty and Subject Matter Expert at IITM Pravartak Technologies Foundation. He is best known for his work in data centre operations, cloud infrastructure and artificial intelligence. He plays a key role in building India's digital workforce. He leads online content creation and on-site training. He also acts as a Chief Technology Officer (CTO) for partner initiatives.

Mr. Syed Mohamed helps run training programmes for diploma and engineering students across India. For example, he helps teach the Certified Intelligent Data Centre – Operations & Maintenance (CIDC-O&M) Program. This course trains students on how to manage the physical and logical parts of data centers. Data centres are large buildings full of computers that store and process internet data.

He helped launch a program to train over 2,000 students from Tier 2 and Tier 3 cities. Tier 2 and Tier 3 cities are smaller, growing towns away from big cities. He partners with tech groups like GenZeal and Vertiv to offer these skills.

...and visiting industry practitioners

ADMISSIONS

A simple 3-step admission process

1

Apply Online

Pay ₹99 and complete a short application form

2

Counselling Session

Our admissions team reviews your profile and schedules a 20-minute call

3

Enrol & Begin

Receive your offer letter, complete payment and join the cohort

INVESTMENT

Investment in your leadership future

Entrance Test Fee	₹99

Registration Fee	₹4,000
Programme Fee	₹121,900
Total Fee	₹125,900 + GST

Pay your preferred way

Upfront Payment	₹144,562

Pay in Parts	INSTALMENT 1 ₹60,000	INSTALMENT 2 ₹84,562

EMI via NBFC Partners	₹18,472 PER MONTH × 9

Note: Custom EMI options are also available through our NBFC partners.
Refund policy is subject to the terms and conditions of the programme.

For any queries, WhatsApp us at
+918792974750

For any queries, contact us at
IITMPravartak.programs@masaischool.com