భారతీయ సాంకేతిక విజ్ఞాన సంస్థ హైదరాబాద్
भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

Program Partner
CyberAI

Powerd By
MINDGRAPH



Certification Program in
Cybersecurity x GenAI
by IIT Hyderabad

Secure your seat today to lead the digital frontier

Course Duration
07 Weeks

Registration Ends
31 Dec 2026

www.aicybercourse.ai.iith.ac.in

Program features
Why Choose This Program?

This program stands out for its focus on bridging the gap between theoretical foundations and practical applications. Participants will benefit from:

Practical Applications

Gain hands-on experience with real-world scenarios to build actionable expertise.

Case Studies

Learn through detailed case studies that provide insights into the challenges and solutions implemented by leading organizations.

Live Industry Applications

Engage with live applications from top industry experts, enabling you to stay ahead in this dynamic field.

Comprehensive Curriculum

A meticulously curated syllabus that covers key areas of cybersecurity and AI, including threat detection, predictive analytics, and ethical hacking.

Guidance from Renowned Faculty

Learn from esteemed IIT Hyderabad faculty and industry leaders who bring a wealth of knowledge and expertise to the program.

Program Duration

The program spans **4 months**, providing a structured learning experience.

Delivery Mode

The course is delivered **online**, allowing flexible learning from anywhere.

Certification

Upon completion, you will receive a **certificate from IIT Hyderabad**, adding credibility and recognition to your skills.

The clock's ticking!. Join Us

Registration Ends on
31 Dec 2026

Duration
07 Weeks
Online, 6-8 hours a week

Program fee

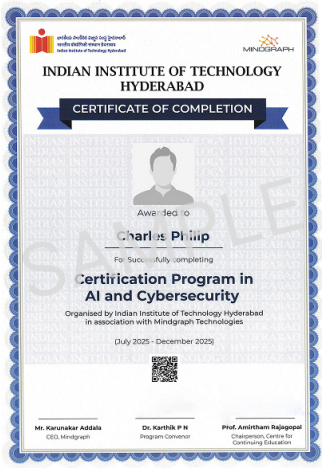
Reserve Seat :	**₹ 25,000**
1st Installment (November 2026):	**₹ 50,000**
2nd Installment (December 2026):	**₹ 50,000**
Total:	**₹1,25,000**

www.aicybercourse.ai.iith.ac.in

Benefits
Certificate Recognition

Elevate your career with the Certification Program in AI and Cybersecurity by IIT Hyderabad. Designed for professionals aiming to excel in the fields of cybersecurity and artificial intelligence, this program offers a comprehensive and hands-on learning experience. Participants will master the skills needed to tackle real-world challenges in network security, threat detection, and AI-driven cybersecurity solutions, paving the way for a rewarding and impactful career.

This program stands out for its focus on practical applications, live industry insights, and advanced tools, making it the ideal choice for professionals ready to advance their expertise.



Industry-Relevant Insights: Benefit from live industry applications and case studies guided by top experts and practitioners.

Prestigious Certification: Earn recognition with a certificate from IIT Hyderabad, enhancing your professional credentials and career prospect

Skill Covered

- Fundamentals of AI
- Core cybersecurity concepts
- Intrusion detection system development and optimization
- IoT security techniques
- Statistical and deep learning for anomaly detection
- Behavior analysis
- Biometric authentication
- Vulnerability scanning and assessment
- Adversarial attack countermeasures
- Data poisoning mitigation
- Model extraction prevention
- Advanced adversarial attack countermeasures
- Differential privacy techniques
- Federated learning
- Robust defense development
- Adversarial training techniques

Course
Cybersecurity x GenAI

Weekend 01

LLM Fundamentals

Annotated inference notebook with tokenization, context budget and decoding observations.

Weekend 02

Prompt Engineering & System Prompts

Versioned prompt template, serialized conversation and six-case behavior log.

Weekend 03

Trust Boundaries & Threat Modeling for AI

Data-flow diagram and threat register with assets, actors, boundaries, controls and residual risks.

Weekend 04

RAG Architecture End to End

Runnable RAG notebook, indexed corpus manifest and retrieval/answer evaluation table.

Weekend 05

Tool Use & Agentic Architectures

Tool schema, validated dispatcher, bounded agent loop and four-case execution log.

Weekend 06

Auth, Permissions & Data Flow in AI Pipelines

Identity/data-flow map, permission matrix and automated allow/deny tests for two tenants.

Weekend 07

Code Generation & Static Analysis Basics

Context inventory, reviewed generated patch, taint trace, static-analysis findings and integrated prerequisite portfolio.

Our Flexible Approach

Each Weekend **04 Classes**	Each Class **45 Minutes**
Contact Hours **3 Hours**	Self-Study Hours **0.75 hours**

www.aicybercourse.ai.iith.ac.in

Course
Program scope and delivery

Audience and entry skills

Learners who can read basic Python, use an IDE and terminal, understand JSON/HTTP, and explain basic web authentication. Complete environment setup before Weekend 1.

Scheduling

Weekend numbers are relative; dates and clock times can be assigned by the instructor. All 28 sessions are 45 minutes. Self-study is optional and excluded from contact hours.

Learning evidence

Keep one portfolio: inference notebook, prompt tests, threat model, RAG pipeline, agent traces, permission tests and reviewed code. Use Assessment for the readiness discussion.

Curriculum status

Draft teaching plan. Assessment thresholds are proposed for prerequisite readiness; institutional certification and attendance requirements are not specified.

Learning progression

Inference → prompt stack → trust boundaries → RAG → tool use → permissions → coding assistants. Each week extends one synthetic document assistant.

Scope

This plan covers the seven prerequisites. Dedicated RAG and coding-assistant attack modules begin after the readiness review and are not included in the 21 contact hours.

Workbook navigation

Read this overview first, then the relevant weekend tab. Lab Setup lists the shared environment. Assessment provides proposed criteria. References contains source URLs.

Source Edition

OWASP identifiers in this workbook use the explicitly versioned 2025 list. The week-to-risk mappings and class activities are curriculum design choices.

About CyberAI

Elevate your career with the Certification Program in AI and Cybersecurity by IIT Hyderabad. Designed for professionals aiming to excel in the fields of cybersecurity and artificial intelligence, this program offers a comprehensive and hands-on learning experience. Participants will master the skills needed to tackle real-world challenges in network security, threat detection, and AI-driven cybersecurity solutions, paving the way for a rewarding and impactful career.

This program stands out for its focus on practical applications, live industry insights, and advanced tools, making it the ideal choice for professionals ready to advance their expertise.

OUR VISION

To lead the world in creating a secure digital future by merging Artificial Intelligence and Cybersecurity, empowering professionals to outpace tomorrow's challenges today.

OUR VALUES

- Purpose-Driven Innovation
- Empowerment Through Knowledge
- Integrity in Action
- Excellence for the Future
- Community & Collaboration

OUR MISSION

To equip ambitious minds with cutting-edge skills in AI and cybersecurity. Through hands-on learning, we empower learners to lead the charge in the digital frontier with resilience and innovation.

CyberAi
4th Floor, Tower E,
TRP Building,
IITH, Kandi, Sanga Reddy,
Telangana, 502284

Program Partner CyberAI | Powerd By MINDGRAPH

भारतीय सांकेतिक विज्ञान संस्थ हैदराबाद
भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad



www.aicybercourse.ai.iith.ac.in