Cybersecurity with Generative AI

Empowering the Next-Gen Security Professionals

A comprehensive course designed to prepare cybersecurity professionals for the AI-driven future of digital defense

Why Cybersecurity Meets Generative AI Now

AI Revolution in Security

GenAI and Large Language Models (LLMs) are revolutionizing cybersecurity defense and attack surfaces, creating new opportunities and vulnerabilities

Emerging Threat Landscape

New threats like prompt injection, AI supply chain risks, and adversarial attacks demand specialized skills and updated defense strategies

Career-Critical Skills

Hands-on mastery of AI-powered security tools is essential for future-ready cybersecurity careers in an evolving digital landscape

Course Overview: From Foundations to Security DevOps & Labs

Comprehensive Learning Path

Our structured approach takes you from AI fundamentals to advanced security implementation, ensuring practical skills development at every stage.

01

Foundations

Understand GenAI, LLMs, AI security risks, and ethical considerations in modern cybersecurity

02

Security DevOps

Integrate AI into secure software development and deployment pipelines

03

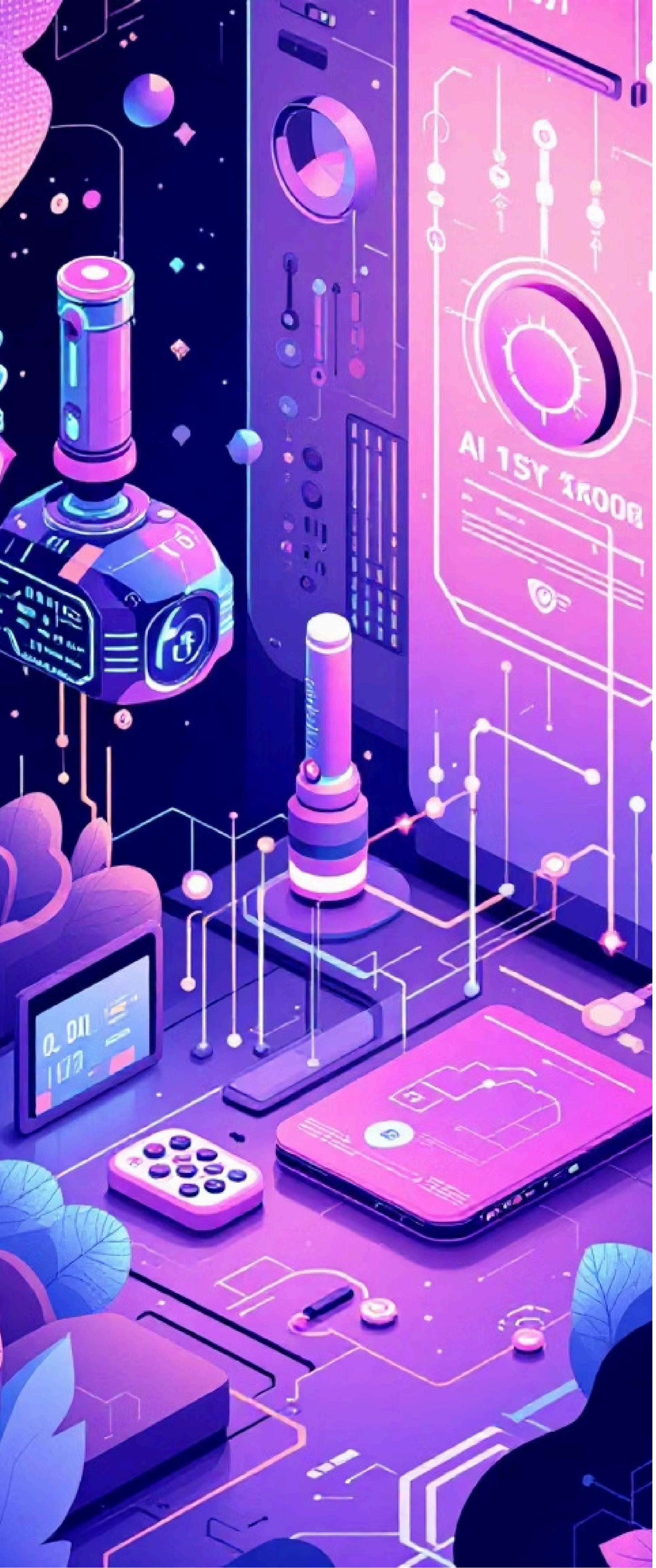
Security Labs

Practice with open-source tools like LangChain, Huggingface, and AWS Bedrock

04

Capstone Projects

Real-world simulations to build job-ready expertise and portfolio



Module 1: Foundations of Generative AI & Cybersecurity

1

GenAI & LLM Architecture

Introduction to Generative AI, Large Language Model architectures, and AI security fundamentals

- Transformer architectures and attention mechanisms
- AI model training and inference processes
- Security implications of AI systems

2

Ethical & Legal Frameworks

Comprehensive coverage of ethical, legal, and regulatory frameworks in AI cybersecurity

- AI governance and compliance requirements
- Privacy protection in AI systems
- Responsible AI development practices

3

Hands-On Lab

Practical experience exploring prompt injection attacks and effective mitigation techniques

- Prompt injection vulnerability assessment
- Defense strategy implementation
- Real-world attack simulation

Modules 2 & 3: Securing GenAI Applications & DevOps Integration

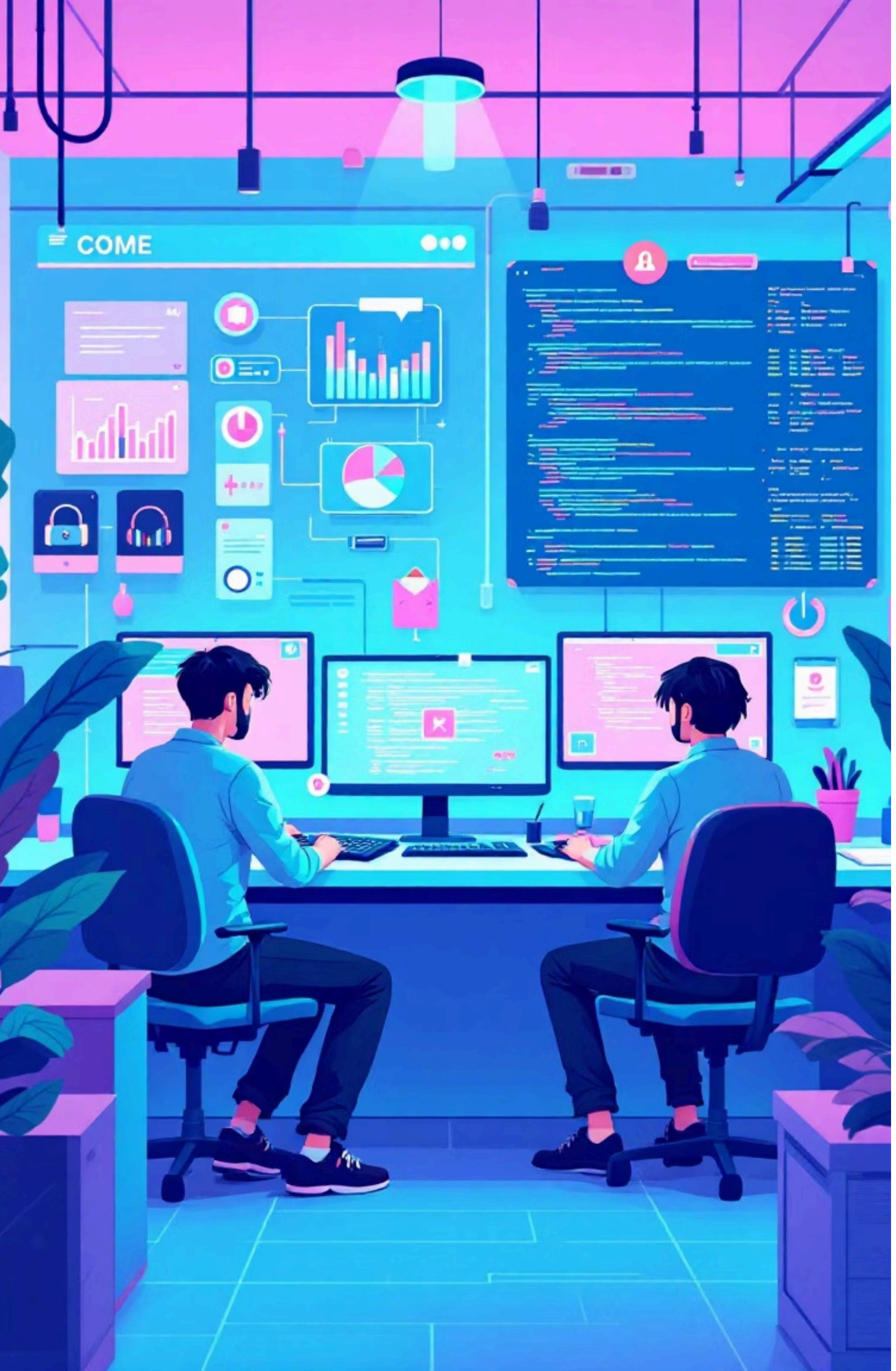
Module 2: Application Security

- Architecture design patterns for secure AI systems
- Secure LLM deployment strategies
- Cloud and on-premise security implementations
- Data protection and model security

Module 3: MLSecOps Integration

- Securing AI/ML development pipelines
- Threat modeling for AI systems
- Incident response for AI security breaches
- Continuous security monitoring

Practical Labs: Fine-tune open-source LLMs for specialized cybersecurity use cases, including threat detection and automated response systems.



Modules 4-6: Advanced Labs & Real-World Application

Module 4: Model Evaluation

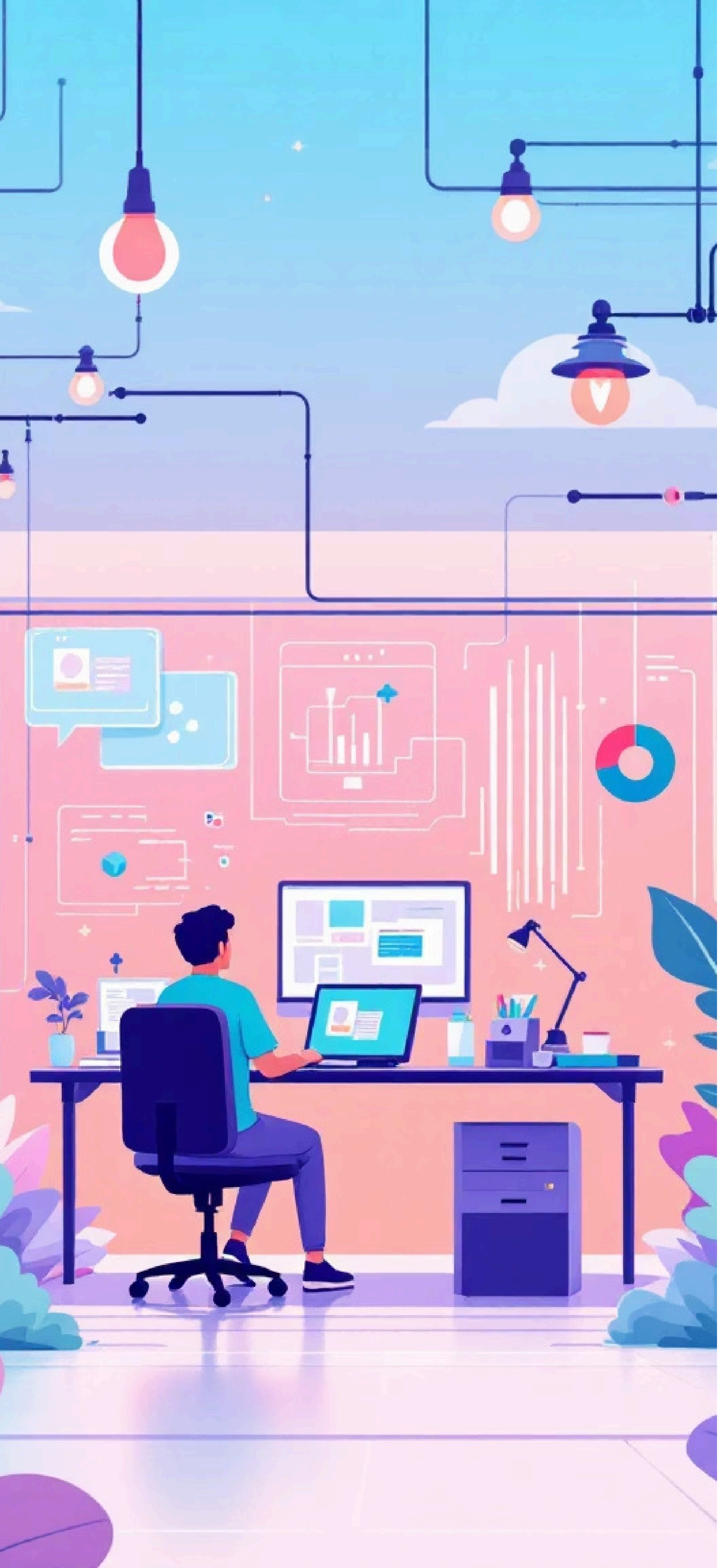
Open vs. closed-source LLM evaluation and comprehensive security trade-off analysis for enterprise deployments

Module 5: Advanced Engineering

Prompt engineering mastery, model fine-tuning techniques, and adversarial defense laboratory exercises

Module 6: Capstone Project

Build and secure a complete GenAI-powered cybersecurity tool from conception to deployment



Hands-On Security Labs with Open-Source Tools

LangChain & Huggingface

Master these powerful frameworks for building secure AI applications and deploying production-ready language models

Google Colab & AWS Bedrock

Leverage cloud platforms for scalable AI security testing, model training, and enterprise deployment scenarios

Vector Database Security

Secure RAG pipelines, implement AI agent defense mechanisms, and protect sensitive data in vector storage systems

✓ **CTF Challenges:** Participate in Capture-the-Flag style challenges designed to simulate real-world cyber threats and test your defensive capabilities.

Who Should Enroll & Career Benefits

Target Audience

Cybersecurity professionals, DevOps engineers, AI enthusiasts, and security architects looking to specialize in AI security

Skill Development

Gain cutting-edge expertise in AI-powered security operations, threat mitigation, and secure AI system design

Career Advancement

Certification opens doors to high-demand roles in AI security architecture, threat intelligence, and secure AI development

> "The intersection of AI and cybersecurity represents the next frontier of digital defense. This course prepares you for that future."

DataXSchool Learning Centres & Locations

Multi-City Presence

State-of-the-art facilities in Bengaluru, Bhubaneswar, and Berhampur with cutting-edge technology infrastructure

Flexible Learning

Choose from in-person, virtual, and hybrid learning modes to fit your schedule and learning preferences

Expert Instructors

Learn from industry veterans with extensive experience in AI development, cybersecurity, and enterprise security architecture

Experience world-class education infrastructure designed specifically for advanced cybersecurity and AI training.

Join the Future of Cybersecurit y

with Generative AI

Master AI-Security Fusion

Protect tomorrow's digital world by mastering the convergence of artificial intelligence and cybersecurity

Comprehensive Learning

Hands-on labs, expert guidance, and real-world projects designed to accelerate your career transformation

Enroll Now at DataXSchool

Learn More About the Program

Transform your cybersecurity career today – The future of digital defense starts with your next decision.