QUANTUM-AI
THE SCHOOL OF DATA AND AI

AI-POWERED CYBERSECURITY

AI-powered cybersecurity uses machine learning and automation to detect threats, predict attacks, respond in real time, and protect systems, networks, and data from evolving cyber risks.



WHY QUANTUMAI?

QuantumAI delivers a practical,job-focused curriculum with hands-on projects using real datasets.Led by industry experts, the program provides exposure to modern tools and cloud technologies,making it suitable for both beginners and professionals looking to grow or transition into AI-Powered cybersecurity.

COURSE OVERVIEW

This course provides a comprehensive overview of AI-powered cybersecurity, covering threat detection, risk analysis, automated response, machine learning techniques, and real-time protection against modern cyber threats.



WHAT YOU WILL LEARN

Preparing for your AI-Powered Cybersecurity Executive Journey

- Program overview and learning roadmap
- AI impact on modern cybersecurity roles
- Career outcomes and role alignment

Operating Systems & Scripting for Cybersecurit

- OS security fundamentals: memory, processes, access control
- Windows & Linux security concepts
- Bash scripting for automation
- PowerShell scripting for system defense

Enterprise Infrastructure Security

- SOC workflows and security operations
- Log management and threat correlation
- Alert triage and monitoring
- IAM implementation and access control
- SIEM-based monitoring and response

Network Security & Cryptography Essentials

- Networking protocols and architectures
- Wireless and network security
- Traffic analysis using Wireshark
- Cryptography fundamentals and tools

Application and Web Application Security

- Secure SDLC principles
- OWASP Top 10 vulnerabilities
- Threat modeling techniques
- DevSecOps practices
- Application vulnerability management

AI Foundations for Cybersecurity Professionals

- Machine Learning fundamentals
- NLP and Deep Learning concepts
- Generative AI in cybersecurity
- AI ethics and responsible AI usage
- AI-driven threat detection and response

AI-Powered Blue Team Strategies

- AI-based detection and response automation
- Behavioral analytics for threat identification
- Threat intelligence integration
- LLM usage in defensive security

Ransomware and Malware Analysis

- Malware lifecycle analysis
- Payload tracking and lateral movement
- Sandboxing techniques
- Reverse engineering basics
- Digital forensics and mitigation

Ethical Hacking and VAPT

- Reconnaissance and enumeration techniques
- Vulnerability assessment methodologies
- Penetration testing workflows
- Exploit simulation and risk prioritization
- Attacker behavior analysis

AI-Enhanced Red Team Tactics

- AI-assisted reconnaissance
- Automated exploitation techniques
- Persistence and post-exploitation
- Adversarial attack simulation
- LLMs for red team operations

Advanced AI in Cybersecurity

- LLMs for SOC automation
- AI-driven phishing detection
- Threat triage using AI
- Adversarial AI defense techniques
- Risk mitigation across AI systems

Portfolio Project

- Real-world cybersecurity problem solving
- Red team and blue team integration
- AI-driven security implementation
- End-to-end capstone project development



Get in Touch

09870400650 info@quantumaico.com www.quantumaico.com

2nd Floor, Old dlf, C-1B, near Dr Lal Pathlabs, South City, Block C,
Old DLF Colony, Sector 14, Gurugram, Haryana 122001