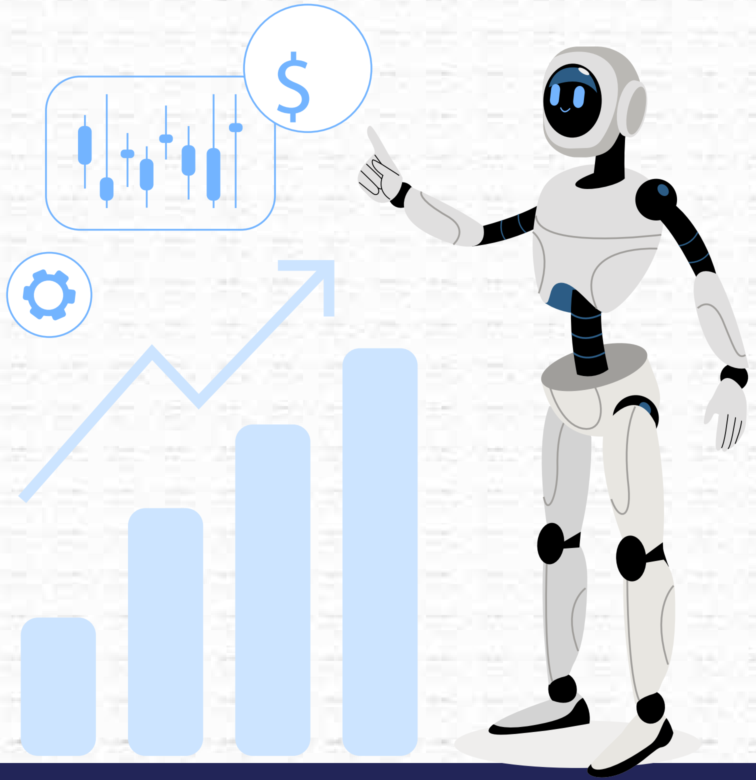
STUDY IQ IAS

Certification *in* Advanced Cybersecurity *With* GEN AI



Batch starts on 06th September

Course overview

- 150 Hours of Live, Expert-Led Virtual Training
- Integrate GenAI to Automate Cyber Defense & Threat Detection
- Master 40+ Advanced Cybersecurity and GenAI Tools
- 40+ Hands-On Projects + 1 Capstone Project
- 50+ Hours Of Additional F.O.C.U.S Practice Sessions And Coding Sprints
- NASSCOM-Endorsed Certification + Career247 Certification
- Access to 200 Hour Tech Skilling Library

☎ 76-4000-3000

Features:

150 Hours of Live Training

Interactive sessions covering Cybersecurity, AI, Cloud, DevSecOps, Vulnerability, Career Assistance.

AI-Driven Cyber Defense

Master AI-driven cybersecurity to automate threat detection and stay ahead of evolving risks.

40+ Mini Projects + 1 Capstone

Complete 40+ mini projects and a capstone, simulating real-world cyber attacks to showcase your skills.

Hands-On Security Labs Using 40+Tools

Use AI-enhanced cybersecurity systems to mitigate risks - 40+ Cybersec and GenAI tools.

☎ 76-4000-3000

Why choose this course?:

AI-Driven Cyber Defense: The Future of Cybersecurity

New age curriculum covering Cybersecurity, GenAI, Cloud, DevSecOps, and Vulnerability.

Real Threats, Real Projects

Complete 40+ mini projects and a capstone, simulating real-world cyber attacks.

Hands-on Labs with 40+ Tools

Learn the latest tools from Wireshark, Nmap, GenAI API (GPT-4o), AWS, GitHub Actions, and many more.

Career Ready Portfolio

Resume Building, LinkedIn Profile + professional portfolio with real-world ' projects.

Affordable Education

Best in class training at unmatched pricing to make quality education affordable for all.

Vernacular Language Support

Geared specifically towards rural and semi-urban learners, we teach in English and Hindi.

☎ 76-4000-3000

CyberSecurity Curriculum

Module 1.

Module 1.1 Introduction to Cybersecurity (5 hours)

Overview of cybersecurity, CIA triad, common threats (malware, phishing, DDoS)

Incident response: SolarWinds, Colonial Pipeline

Labs:

Identify phishing indicators in a fake email

Analyze the Colonial Pipeline breach and document the attack chain

Module 1.2: Core Concepts in Information Security (5 hours)

Authentication, AAA, least privilege, zero trust

Risk management, security policies, and frameworks

Labs:

Map AAA concepts using a role-based access simulation

Perform a risk assessment for a mock organization

Module 1.3: Linux Security Fundamentals (5 hours)

Linux architecture, file systems, permissions

User management, SSH security, system logs

Labs:

Configure users, groups, and file permissions on a Linux VM

Harden SSH and enable log monitoring with auditd

Module 1.4: Networking and Security Foundations (5 hours)

OSI/TCP/IP models, DNS, encryption

Firewalls, VPNs, IDS, TLS/SSL

Labs:

Perform packet capture and protocol analysis with Wireshark

Configure and test firewall rules using pfSense or iptables

Module 2.

Module 2.1: What is Machine Learning & Deep Learning (2 hours)

ML vs. DL, supervised vs. unsupervised learning

Use cases in cybersecurity: threat detection, malware classification

Neural networks, deep learning fundamentals, algorithms

Labs:

Train an ML model for threat detection

Explore deep learning models for anomaly detection

Module 2.2: What is Large Language Models (LLMs) (2 hours)

Training, fine-tuning, and deployment of LLMs

Risks: bias, hallucination, misuse

Ethical concerns, fine-tuning for cybersecurity tasks

Labs:

Fine-tune an LLM and test for biases

Analyze LLMs in real-world threat detection

Module 2.3: What is Generative AI (2 hours)

Text, image, and code generation (GPT, DALL·E, Copilot)

Applications, threats, and solutions in cybersecurity

Ethical concerns and AI-generated content detection

Labs:

Outwit an AI-generated phishing email

Simulate a phishing attack with GPT-4o Mini and build a detection

Module 2.4: What is AI Agents & Agentic AI Systems (10 hours)

Basics of AI agents: reactive, deliberative, goal-based

LangChain, LangGraph, vulnerabilities in agent systems

Protocol vulnerabilities: MCP, prompt injection, overfitting

Labs:

Review an AI-generated agent script for over-permissions

Compare secure vs insecure agent memory handling

Module 2.5: Understanding Threats to AI Agents (4 hours)

Common attack vectors, memory poisoning, and over-permissioned execution

Securing agent workflows and protocols

Real-world case studies of agent exploitation

Labs:

Secure an AI agent from prompt injection

Build a secure agent system to prevent exploits

Module 3.

Module 3.1: How Generative AI & Agentic AI Systems are Impacting SDLC (15 hours)

Overview of Modern SDLC with AI

LLMs in SDLC phases (Plan, Design, Code, Test, Release)

Tools: GitHub Copilot, Claude Code, Replit, Amazon Q, Codium, ChatGPT

LLM-generated code vulnerabilities, API and secrets exposure

Exploitation of AI-supported pipelines

Secure code review using AI

Risks in auto-generated frontend/backend/infra

Labs:

Use AI to generate a login module and analyze its security flaws

Write secure vs. insecure config files (YAML, ENV) with AI

Upload LLM-generated backend code to AI chatbot for vulnerability analysis

Prompt LLM to generate an API and discover flaws using AI threat modeling

Evaluate RAG-based SDLC workflows for data leakage or prompt injection attack surfaces

Module 4.

Module 4.1: Cloud Security Fundamentals (6 hours)

Cloud service models: IaaS, PaaS, SaaS

Shared responsibility model, AWS, Azure, GCP

Cloud threats, misconfigurations, governance principles

Securing cloud data and networks

Labs:

Explore IAM roles and policies in AWS free tier

Identify misconfigurations in simulated cloud architecture

Module 4.2: Securing Cloud Infrastructure (9 hours)

IAM policies, role-based access
Securing networks with VPCs, security groups
Encryption with KMS, key vaults
Cloud vulnerability scans, monitoring access logs

Labs:
Configure secure VPC with subnets and security groups
Encrypt S3 buckets and manage access using KMS

Module 4.3: OWASP Cloud Security and Threat Detection (7 hours)

OWASP Top 10 Cloud vulnerabilities
Detecting misconfigurations in S3, IAM, APIs
Monitoring with AWS CloudTrail, Azure Monitor
Identifying insecure interfaces and endpoints

Labs:
Scan cloud resources using ScoutSuite
Monitor activity with AWS CloudTrail and detect anomalies

Module 4.4: Cloud Incident Response (8 hours)

Preparing and responding to cloud incidents
Data breaches, account compromises, and automation
Compliance with GDPR, SOC 2, and ISO standards
Building cloud-specific IR playbooks

Labs:
Investigate simulated cloud breach, isolate root cause
Automate incident response using Terraform and AWS Config rules

Module 5.

Module 5.1: DevSecOps using AI APIs and Models (10 hours)

DevSecOps in the GenAI Era
Integrating LLMs in CI/CD pipelines securely
Threat modeling with AI APIs, secure IaC
Realtime vulnerability scanning and API-level validation using LLMs
Protecting GenAI apps with LangChain Guard/Rebuff

Labs:
Build a GPT-4o Mini-powered DevSecOps bot to review PRs
Detect secrets in backend repos and patch them

Module 5.2: AI-Powered Threat Intelligence & Security Automation (5 hours)

Building Threat Intelligence Lifecycle with Generative AI

Collecting and analyzing IOCs using AI

Mapping APT behaviors to MITRE ATT&CK

Creating actionable threat reports with LLMs

Labs:

Audit leaked emails with GPT-4o Mini, build AI-powered phishing radar

Use MISP with LLM agents to create actionable threat reports

Module 5.3: Cybersecurity Tools and Automation (5 hours)

Automating Threat Response with AI + Python/Shell

Introduction to Generative AI Plugins

Integrating Security Tools using APIs and Webhooks

Developing GenAI-driven automation use cases

Labs:

Build a security automation script using Python and AI

Integrate security tools using AI-generated webhook logic

Module 6.

Module 6.1: Foundations of LLM Security (6 hours)

LLM security risks, OWASP LLM Top 10

Real-world prompt injection & jailbreaks

PoisonPrompt, backdoor attacks, AI hallucination risks

Emerging threats: AI worms, autonomous agent attacks

Labs:

Simulate and defend against prompt injection attacks

Mitigate hallucinated dependencies causing AI-based supply chain attacks

Module 6.2: LangChain, Agent Protocols & LangGraph (7.5 hours)

LangChain architecture, multi-agent systems

MCP & agent communication protocols

Risks in memory, tool use, and agent delegation

Labs:

Build an AI agent using LangChain

Secure a LangChain model for data processing

Module 6.3: Attack Surface Mapping & Exploit Simulation (6.5 hours)

AI attack surface, taxonomy, and LLM vulnerabilities

RAG & vector retrieval poisoning

Simulating LLM-enhanced injections and hallucination risks

Labs:

Analyze AI attack surface and identify vulnerabilities

Simulate LLM injection attacks and apply mitigation strategies

Module 6.4: Identity & Access Security for GenAI Systems (1.5 hours)

Enforcing MFA, access control in prompt APIs, and model hosting

Module 6.5: Monitoring and Auditing (2.5 hours

Anomaly detection in LLM behavior

Logging, audit trails, and automated penetration testing with LLMs

Module 7.

Capstone 1: Botnet Analysis with GPT-4o

- Data Cleaning: Process 92,000+ network flow records (normal & attack traffic).
- Attack Characterization: Compare botnet vs. normal traffic to spot attack patterns.
- AI Detection: Use GPT-4o for summarizing, rule generation, and remediation.
- Malware Propagation: Trace malware spread and identify affected endpoints.

Capstone 2: Malware Reverse Engineering with GPT-40

- File Analysis: Extract metadata and compute hashes from malware samples.
- Static/Dynamic Analysis: Disassemble code and analyze runtime behavior.
- AI Insights: Use GPT-4o for IOCs, code interpretation, and malware classification.
- Detection & Remediation: Generate detection rules and suggest fixes.

Capstone 3: PCAP Analysis for SOC Analysts

PCAP Ingestion: Analyze large PCAP files for suspicious activity.

Attack Timelines: Correlate session data to map attacker actions.

AI Detection: GPT-4o to summarize activity, detect anomalies, and suggest rules.

Incident Response: Recommend detection actions and alerts.

Capstone 4: Web App Pen Testing with GPT-4o

Vulnerability Discovery: Exploit XSS, CSRF, SQLi, and IDOR in OWASP Juice Shop.

Exploitation Guidance: Use GPT-4o to suggest payloads and interpret responses.

Learning Exploitation: Teach vulnerabilities and techniques in plain language.

Fix Recommendations: Propose security fixes and document attacks.

Module 8:

- Grammar, Reading Comprehension Drills: Improve professional writing and speaking clarity for cybersecurity contexts.
- Email and Report Writing for Analysts: Focus on creating concise, clear, and actionable cybersecurity emails and reports.
- Optimizing LinkedIn, GitHub, Notion for Portfolio & Branding: Learn to showcase your cybersecurity skills and projects online.
- Resume Teardown + STAR Method for Crafting Bullet Points: Improve your resume and highlight key achievements using the STAR method.
- Behavioral Interview Prep + Mock Interviews with Feedback: Prepare for common cybersecurity interview questions using mock interviews with expert feedback.

40+ Cybersec And GenAI Tools You Will Master

pfsense

Terraform

aws

GitHub Actions

AWS WAF

Amazon CloudTrail

Jenkins

wireshark

CI/CD

snyk

MISP Threat Sharing

Nessus vulnerability scanner

Amazon Inspector

NMAP

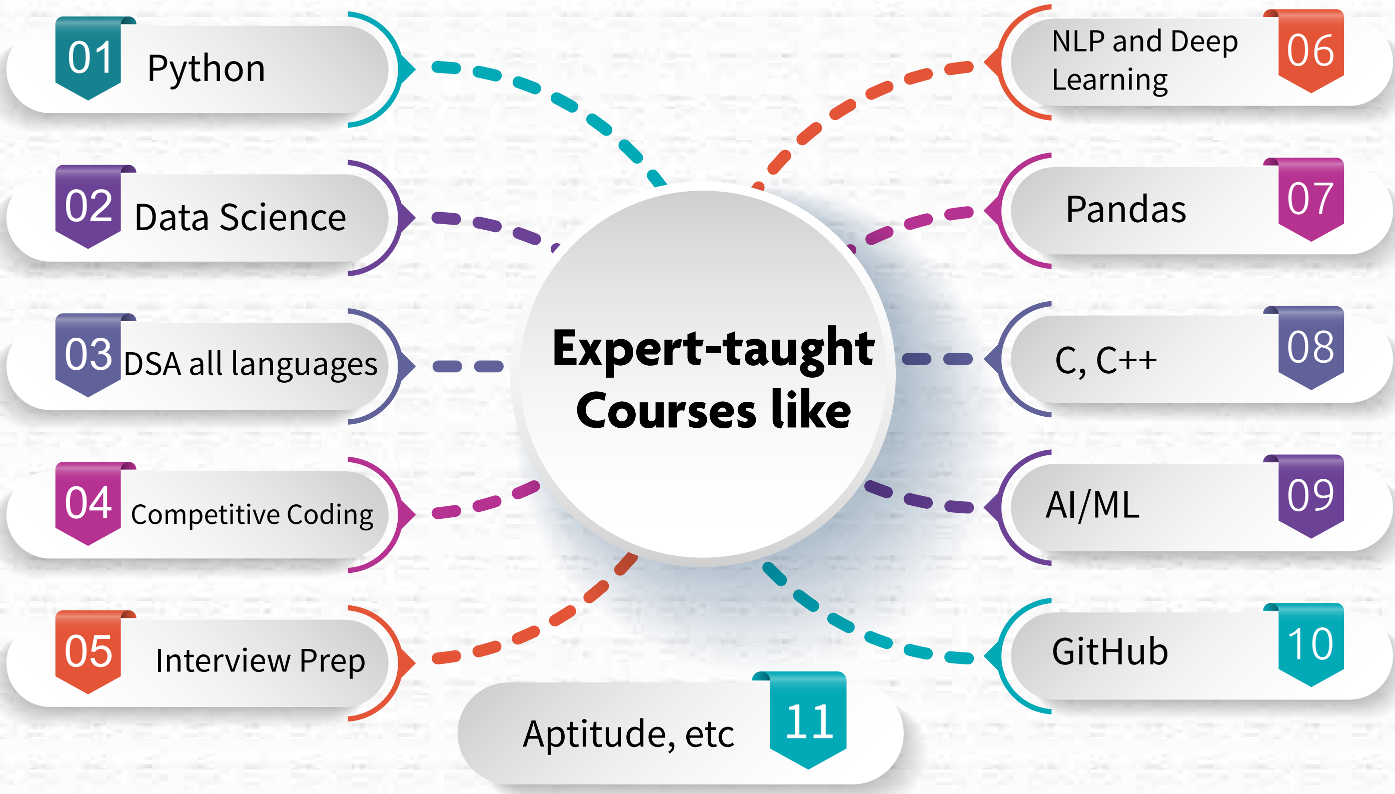
☎ 76-4000-3000

40+ Mini Projects + 1 Capstone Projects

- Analyze Network Traffic, Identify Attack Patterns And Trace Malware Propagation Using AI.
- Explore Vulnerabilities In Web Apps, Exploit Weaknesses And Recommend Fixes With AI Guidance.
- Extract Metadata, Analyze Malware Behavior And Generate Detection Rules With AI Assistance.
- Perform A Risk Assessment With Smart AI Tools For Better Security.
- Analyze PCAPs, Detect Suspicious Activity And Suggest Incident Response Actions Using AI.
- Simulate A Phishing Attack And Use GenAI To Detect And Block It.

☎ 76-4000-3000

Get access to 200+ skilling courses



Expert-taught Courses like

01 Python

02 Data Science

03 DSA all languages

04 Competitive Coding

05 Interview Prep

06 NLP and Deep Learning

07 Pandas

08 C, C++

09 AI/ML

10 GitHub

11 Aptitude, etc

Demo Videos

Demo video 1: https://youtu.be/9pkY_Fg0atA

Demo video 2: https://youtu.be/H3PXGPOFelo

☎ 76-4000-3000

Career Path in Cybers ecurity

Your journey from beginner to expert in the dynamic world of Cybersecurity

Salary growth

Experience rapid salary growth as you move up in Cybersecurity. Start with entry-level roles and progress to high-paying leadership positions

Career In Cybersecurity

Experience rapid salary growth as you move up in Cybersecurity. Start with entry-level roles and progress to high-paying leadership positions.

Career path

Experience rapid salary growth as you move up in Cybersecurity. Start with entry-level roles and progress to high-paying leadership positions.

Career Assistance

1.Resume Building
2.Interview Preparation
3.Mock Interviews
4.CyberSecurity Portfolio

☎ 76-4000-3000

Who Should Do Cybersecurity With GenAI Program?

Aspiring Cybersecurity Individuals

Individuals aiming to launch a career in Cybersecurity or related fields.

Career changers

Professionals from non-technical backgrounds eager to transition into the high-demand field of Cybersecurity.

IT engineers and graduates

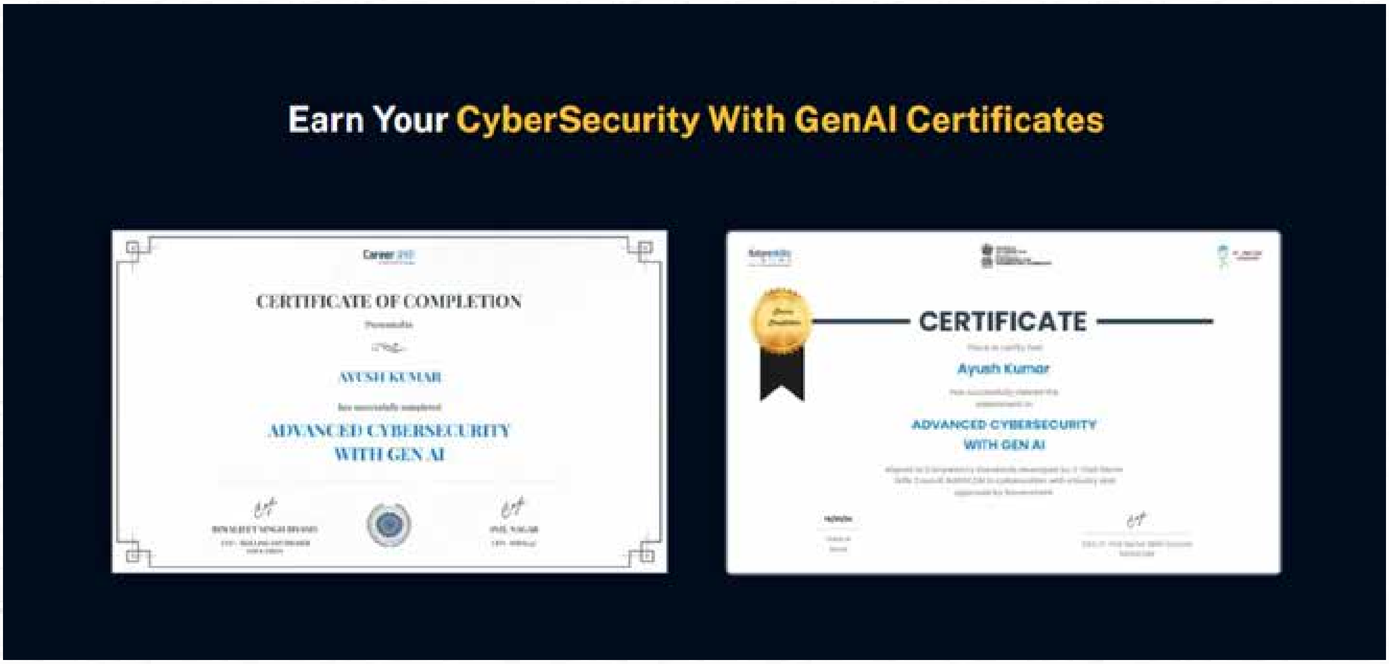
Students or professionals with technical degrees who want to specialize in Cybersecurity

GenAI Practitioners

GenAI Practitioners Applying AI to Cybersecurity Challenges.

☎ 76-4000-3000

Earn Your CyberSecurity With GenAI Certificates



Earn Your CyberSecurity With GenAI Certificates

CERTIFICATE OF COMPLETION

[illegible]

AYUSH KUMAR

has successfully completed

ADVANCED CYBERSECURITY WITH GEN AI

[illegible]

CERTIFICATE

[illegible]

Ayush Kumar

[illegible]

ADVANCED CYBERSECURITY WITH GEN AI

[illegible]

Meet Your Faculty

Dipanshu Parashar 10+ YOE

10+ years in Cybersecurity, TEDx Speaker, IIT Faculty, founder of Virtual Cyber Labs

Prabodh Ranjan 10+ YOE

Trained 5,000+ ,Co-Founder of KloudStac, Ex-ANZ, Siemens Technology

Bhavesh Dutta 7+ YOE

CEH Certified Trainer & Cyber Crime Investigator , Guest Faculty at IIT Kanpur .

☎ 76-4000-3000

Advanced Cybersecurity Using GenAI Program Fees

Program fees include tuition, materials, and other resources. Flexible payment options or scholarships may be available to eligible students.

- 6 Months Skill-Based Cohort (Live) Learning
- 150 Hours of Live Virtual Training
- 40+ Industry Projects And Choice Of 4 Capstone Projects
- 40+ Cybersecurity and GenAI Tools Covered
- 50+ Hours Of Additional F.O.C.U.S Practice Sessions And Coding Sprints
- Access to 200+ Course Skilling Library
- Financing Options Available

Advanced Cybersecurity Using GenAI Program Fees ₹ 60,000/-
Inclusive of all taxes

Flexible EMI plans, powered by our trusted Finance Partners

BAJAJ FINSERV

Propelld

JODO

☎ 76-4000-3000

Frequently Asked Questions

General Questions

1. What is the Advanced Cybersecurity with GenAI Certification program?

➔ What is the Advanced Cybersecurity with GenAI Certification program?
A 150-hour, live, hands-on program focused on next-gen cybersecurity principles, cloud security, and AI-powered threat detection. This course includes the integration of Generative AI to automate cybersecurity tasks, such as threat detection, secure coding, and incident response.

2. Who should enroll?

➔
1. Freshers with a BTech/BE (especially those aiming for cybersecurity careers)
2. Aspiring cybersecurity professionals
3. Engineers and tech enthusiasts seeking hands-on cybersecurity experience
4. Job seekers and career changers aiming for advanced cybersecurity roles in AI-driven environments

3. What are the key benefits?

➔
1. Master 40+ cybersecurity and GenAI tools
2. Complete 40+ mini projects and 1 capstone project
3. Gain expertise in AI-driven cybersecurity defense
4. Learn industry-standard tools like Wireshark, GitHub Copilot, AWS, and more
5. Receive dual certification from Career247 and NASSCOM
6. Build a professional portfolio with real-world projects

4. How is this different from other cybersecurity courses?

➔ This course uniquely integrates Generative AI to automate cybersecurity tasks, focusing on AI-driven threat detection, secure cloud environments, and DevSecOps. It also covers both foundational and advanced cybersecurity techniques, making it ideal for tech enthusiasts aiming to stay ahead in the cybersecurity field.

5. Do I need a technical background?

- While some basic tech knowledge is helpful, the course is designed for professionals with varying levels of expertise. Practical, hands-on sessions will guide you through each concept and tool, with minimal need for deep coding knowledge.

6. What's the duration and weekly schedule?

- The program is 150 hours in total, delivered live over 6 months (25 weeks). Classes are conducted on Saturdays and Sundays from 7 PM to 10 PM and F.O.C.U.S Classes and Coding Sprints will be conducted on Alternative Tuesdays from 7 PM to 9 PM.

Program Structure & Curriculum

1. What are the learning outcomes of this program?

- By the end of the program, you will be able to
  1. Mitigate cybersecurity threats using AI-powered tools
  2. Secure cloud and network infrastructure
  3. Automate cybersecurity tasks with Generative AI
  4. Integrate security into DevSecOps pipelines
  5. Protect AI systems from cyber attacks
  6. Build a career-ready portfolio with real-world project

2. What topics are covered in the course

1. Fundamentals of Cybersecurity
2. Generative AI & AI Agents
3. AI-Native SDLC & Secure Engineering Pipelines
4. Cloud Security
5. DevSecOps with Generative AI
6. AI Vulnerability Analysis & Defensive Engineering

3. What projects are included?

- 40+ mini projects such as AI-powered phishing detection and cloud security testing

  1 Capstone project, where you choose from: Botnet Analysis, Malware Reverse Engineering, or Web App Pen Testing using GPT-4o.

4. Which tools will I learn in this program?

➔ You will gain hands-on experience with tools like Wireshark, Nmap, pfSense, AWS CloudTrail, GitHub Copilot, GPT-4o, and many more essential cybersecurity and AI tools.

5. What is Generative AI's role in this program?

➔ Generative AI plays a crucial role in automating cybersecurity tasks, such as detecting threats, securing systems, and analyzing incidents. You will work with AI tools to enhance threat detection and defense strategies in real-world scenarios.

6. What is the passing criteria?

➔ To complete the course, you must:

1. Attend at least 80% of live sessions
2. Score at least 80% on assignments and assessments
3. Submit the Capstone project

Career Assistance

1. What career support is offered?

➔ You will receive comprehensive career support, including resume building, LinkedIn optimization, interview preparation, and guidance on applying for cybersecurity roles. No guaranteed job placements or interviews.

2. What roles can this course lead to?

➔ Roles include Cybersecurity Analyst, AI Security Engineer, Penetration Tester, Cloud Security Architect, Incident Response Specialist, DevSecOps Engineer, and more.

3. Which companies hire GenAI-powered cybersecurity professionals?

➔ Key employers include TCS, Infosys, Wipro, Cognizant, IBM, Accenture, Zscaler, and leading cybersecurity startups.

4. What career assistance criteria do I need to meet to receive support?

➔ To qualify for Career Assistance, you must:

1. Attend at least 80% of live sessions
2. Score a minimum of 80% on assignments and assessments

5.What career support does Career247 provide?

- Career247 provides tailored career guidance, including:
  1. Resume building and LinkedIn optimization
  2. Interview preparation with mock interviews and feedback
  3. Assistance in applying for relevant roles
  4. Professional portfolio building through mini projects and the Capstone project

Fees & Enrollment

1.What is the course fee?

- The program fee is ₹60,000 (inclusive of all taxes), with financing options available.

2.Are there any scholarships or promotions available?

- Yes, limited scholarships are available for deserving candidates. Please inquire with us for more details.

3.Do you offer EMI or loan options?

- Yes, EMI and loan options are available to make the course more affordable.

4.How do I enroll in the program?

- Refunds are processed according to Career247 Terms &Conditions.

Technical and support queries

1.What are the tech requirements for this course?

- You will need a laptop or desktop with a stable internet connection to access course materials and participate in live sessions.

2.How are doubts and questions resolved during the course?

- You can resolve doubts during live Q&A sessions, and support is available via email throughout the course.

3. What if I miss a live session?

- Recordings of all live sessions will be provided to ensure you do not miss out on any material.

4. Will I get one-on-one mentorship?

- While there is no formal one-on-one mentorship, you will receive feedback and support during interactive classes and from your peers.

5. How long will I have access to the course materials?

- You will have access to all course materials for 6 months after completing the course.

6. Will I receive printed handouts or books?

- No, all materials are provided digitally via the learning platform.

☎ 76-4000-3000