INVENTATEQ
LEARN SKILLS • GET PLACED

MASTER AI SECURITY
COURSE With Placement

Build In-Demand Professional Expertise with Real-Time Hands-on AI Security Training

BEST RATED ON TOP PLATFORMS

Google Reviews ★★★★★ · Trustpilot ★★★★★ · Sulekha ★★★★★

COURSE BENEFITS

- 100% Practical & Real-Time Hands-on Labs
- End-to-End Capstone Implementation Projects
- Industry Recognized Certification Preparation
- 100% Dedicated Placement Support in MNC's & Mock Interviews

15+	500+	25K	15K
YEARS OF EXCELLENCE	HIRING PARTNERS	STUDENTS TRAINED	STUDENTS PLACED

Chat on WhatsApp
FREE Career Counselling
+91 85500 00909

YOUR FUTURE
STARTS HERE !

INVENTATEQ
LEARN SKILLS • GET PLACED

ARE YOU FACING THESE CHALLENGES ?

- Still searching for your first job after graduation?
- Worried about the Gap? And don't know how to start your career?
- Stuck in a low-salary job? and seeking for better growth opportunities?
- Fear of switching to an IT career from a non-IT background
- Not getting interview calls despite applying to 100+ jobs?

TOO MUCH THEORY
NO PROJECTS
SKILL GAP
NO GUIDANCE
?

How Inventateq Helps You

Waiting Ends. Careers Begin.
Build job-ready skills. Start applying with confidence.

Turns Gaps into Comebacks
Close skill gaps. Rebuild your career

Break Free. Move Forward
Learn in-demand skills. Take your next career step.

Doubt Out. Confidence In.
Practice real skills. Walk into interviews prepared.

Turn Rejections into Chances
Turn every setback into skills employers value.

Be Smart Learn AI
Learn AI tools. Work smarter. Stay updated

INVENTATEQ
LEARN SKILLS • GET PLACED

ABOUT INVENTATEQ

Inventateq is a leading IT training and placement company committed to transforming learners into Industry ready professionals

Our Mission
To deliver high-quality education, practical slots and career opportunities that empower individuals to achieve their dreams

Our Vision
To be a globally recognised training company known for innovation, quality and impactful learner outcomes.

Why Thousands Choose Inventateq?

15+	500+	25,000+	15,000+
Years of Excellence	Hiring Partners	Students Trained	Students Placed

We Collaborate With

Deloitte. · Capgemini · amazon · HCL · Tech Mahindra

INVENTATEQ
LEARN SKILLS • GET PLACED

WHY LEARN AI SECURITY ?

Enterprises worldwide are actively hiring certified AI Security professionals to drive critical business operations, digital transformation, and modernization.

CAREER SCOPE OF AI SECURITY

Exponential Industry Demand
Rapid enterprise adoption across global IT firms, MNCs, and technology centers

Premium Salary Compensation
Command competitive compensation packages with rapid growth milestones

Cross-Industry Opportunities
Versatile skill set applicable across technology, consulting, finance, and core sectors

Future-Proof Career Growth
Long-term job security supported by ongoing digital modernization and tooling investment

Global Certification Pathways
Direct alignment with recognized industry certifications to validate your competence

Worldwide Job Prospects
Open doors to roles in major Indian tech hubs as well as international remote positions

INDUSTRY-RECOGNIZED CERTIFICATION

INVENTATEQ
CERTIFICATE
OF ACHIEVEMENT

QR Verified · Globally Valid · ISO 9001:2015

Top-Tier Data & AI Demand. Global Analytics Roles. Premium Compensation.

Average AI Security Engineer Salary in India

₹7.5 LPA – ₹24 LPA

INVENTATEQ
LEARN SKILLS • GET PLACED

WHY INVENTATEQ ?

Because we have placed over 15,000+ students and we can place you as well

STUDENT PLACEMENTS

- 100% Placement Assurance Support
- 500+ Top Tech Hiring Partners
- Resume & LinkedIn Optimization
- Industry Mock Technical Interviews
- Unlimited Interview Calls Until Placed

COURSE & PLACEMENT VIDEOS

Student Genuine Feedback
Inventateq Reviews & Student Genuine Feed...
Inventateq Bangalore Reviews
Watch Video

Practical Training Success
AWS Course in Bangalore, Best AWS Training &a...
Industry Tech Career
Watch Video

Placement Story
Inventateq HR Practical Training Student Succ...
Campus to MNC Offer
Watch Video

Interview Skills & Growth
Free Interview Skills Development Classes for...
Free Student Masterclass
Watch Video

> At Inventateq, Your Success is Our Mission !

INVENTATEQ
LEARN SKILLS • GET PLACED

GUARANTEED PLACEMENT SUPPORT

We don't just teach, we prepare you for the real world!

- Aptitude Training
- Technical Training
- Mock Interviews
- HR Interview Preparation
- Resume Preparation
- Cover Letter Preparation
- LinkedIn Profile Optimisation
- Job Portal Access
- Placement Drives & Hiring Events

OUR RECRUITMENT PARTNERS

TATA · Infosys · wipro · Capgemini · Tech Mahindra · LARSEN & TOUBRO · HCL TECH · accenture

OUR PLACEMENT STATS

Our placement record reflects consistent growth, with students securing opportunities across leading companies in diverse industries.

15,000+	500+	95%	6 LPA
Students Placed	Companies Hired	Placement Ratio	Average Package

Check Most Recent Placements

INVENTATEQ
LEARN SKILLS • GET PLACED

CAREER PROGRESSION

Job responsibilities, technical competency and portfolio evidence for each role.

ROLE PATHWAY	TYPICAL RESPONSIBILITIES	PORTFOLIO PROOF
AI Security Developer	Manage core AI systems tasks, configure tooling, and support delivery.	Practical AI systems setup files, exercise scripts, and documentation.
AI Security Specialist	Build practical AI Application workflows, implement features, and resolve issues.	Functional AI Application modules, workflow configs, and practical deliverables.
Lead AI Security Engineer	Lead AI Security technical delivery, design solutions, and set standards.	Complete AI Security capstone artifacts, technical blueprints, and reports.

INVENTATEQ
LEARN SKILLS • GET PLACED

SKILLS ROADMAP

Progress from core foundations to production-ready enterprise workflows.

MILESTONE	PRACTICAL OUTPUT	REVIEW EVIDENCE
Milestone 1 (Foundations)	Master fundamental AI systems concepts, environment setup, and tools.	Configured AI systems workspace and verified practice exercises.
Milestone 2 (Implementation)	Develop practical AI Application workflows and functional domain modules.	Working AI Application project modules and validated practice outputs.
Milestone 3 (Advanced Workflows)	Implement advanced RAG features, integrations, and optimizations.	Validated RAG configurations and technical review outputs.
Milestone 4 (Production Capstone)	Deliver an end-to-end AI Security capstone project and technical review.	Complete AI Security project portfolio artifact and defense.

INVENTATEQ
LEARN SKILLS • GET PLACED

DETAILED MODULE PLAN

12 in-depth modules • 3 Months Duration • Hands-on practical training

1 MODULE 1: AI & Cybersecurity Fundamentals

- Learning Objectives
- Understand how AI systems work and identify the security risks introduced by AI/ML technologies.
- Introduction to AI, ML and Generative AI
- AI application architecture
- Machine learning lifecycle
- Training, validation and inference
- Traditional cybersecurity vs AI security
- AI attack surface

GUIDED LAB
Log in to the system, practice basic navigation, and complete your first Learning Objectives exercise.

INTERVIEW & ASSESSMENT
Explain what Learning Objectives is used for and why companies choose it in simple words.

2 MODULE 2: LLM & Generative AI Security

- Learning Objectives
- Understand security vulnerabilities specific to Large Language Models and Generative AI applications.
- LLM architecture basics
- Tokens and context windows
- System prompts
- User prompts
- Model outputs
- LLM application architecture

GUIDED LAB
Perform a safe security inspection on Learning Objectives in a controlled lab and report risks.

INTERVIEW & ASSESSMENT
Explain common security risks in Learning Objectives and how to protect user data from attacks.

3 MODULE 3: OWASP Top 10 for LLM Applications

- Learning Objectives
- Learn the major security risks affecting modern LLM applications.
- OWASP LLM security framework
- LLM application threat modeling
- LLM01 – Prompt Injection
- LLM02 – Sensitive Information Disclosure
- LLM03 – Supply Chain
- LLM04 – Data and Model Poisoning

GUIDED LAB
Perform a safe security inspection on Learning Objectives in a controlled lab and report risks.

INTERVIEW & ASSESSMENT
Explain common security risks in Learning Objectives and how to protect user data from attacks.

4 MODULE 4: AI Application & API Security

- Learning Objectives
- Secure AI-powered applications and APIs against common application security threats.
- AI API architecture
- REST API security
- Authentication
- Authorization
- API keys
- OAuth fundamentals

GUIDED LAB
Perform a safe security inspection on Learning Objectives in a controlled lab and report risks.

INTERVIEW & ASSESSMENT
Explain common security risks in Learning Objectives and how to protect user data from attacks.

5 MODULE 5: Data Security, Model Security & Privacy

- Learning Objectives
- Protect AI training data, user data, models and sensitive information.
- AI data security
- Data classification
- PII protection
- Data anonymization
- Data encryption
- Secure data storage

GUIDED LAB
Perform a safe security inspection on Learning Objectives in a controlled lab and report risks.

INTERVIEW & ASSESSMENT
Explain common security risks in Learning Objectives and how to protect user data from attacks.

6 MODULE 6: Adversarial Machine Learning

- Learning Objectives
- Understand attacks that manipulate machine-learning models and develop basic defensive techniques.
- Adversarial ML fundamentals
- Adversarial examples
- Evasion attacks
- Poisoning attacks
- Model manipulation
- Model robustness

GUIDED LAB
Perform a safe security inspection on Learning Objectives in a controlled lab and report risks.

INTERVIEW & ASSESSMENT
Explain common security risks in Learning Objectives and how to protect user data from attacks.

7 MODULE 7: RAG & Vector Database Security

- Learning Objectives
- Secure Retrieval-Augmented Generation applications and their data sources.
- RAG architecture
- Embeddings
- Vector databases
- Retrieval pipelines
- Document ingestion
- Context injection

GUIDED LAB
Perform a safe security inspection on Learning Objectives in a controlled lab and report risks.

INTERVIEW & ASSESSMENT
Explain common security risks in Learning Objectives and how to protect user data from attacks.

8 MODULE 8: AI Red Teaming & Security Testing

- Learning Objectives
- Develop practical skills for attacking and evaluating AI systems from a security perspective.
- AI red teaming
- AI threat modeling
- Attack planning
- Vulnerability discovery
- Prompt attack techniques
- Automated AI security testing

GUIDED LAB
Perform a safe security inspection on Learning Objectives in a controlled lab and report risks.

INTERVIEW & ASSESSMENT
Explain common security risks in Learning Objectives and how to protect user data from attacks.

9 MODULE 9: AI Agents & Autonomous AI Security

- Learning Objectives
- Understand security risks introduced by AI agents and tool-using AI systems.
- AI agents
- Agent architecture
- Tools and function calling
- Autonomous workflows
- Agent permissions
- Agent memory

GUIDED LAB
Perform a safe security inspection on Learning Objectives in a controlled lab and report risks.

INTERVIEW & ASSESSMENT
Explain common security risks in Learning Objectives and how to protect user data from attacks.

10 MODULE 10: AI Governance, Risk & Compliance

- Learning Objectives
- Understand how organizations manage AI security risks and compliance requirements.
- AI governance
- AI risk management
- Security policies
- Responsible AI
- Privacy
- Risk assessment

GUIDED LAB
Perform a safe security inspection on Learning Objectives in a controlled lab and report risks.

INTERVIEW & ASSESSMENT
Explain common security risks in Learning Objectives and how to protect user data from attacks.

11 MODULE 11: AI Security Monitoring & Incident Response

- Learning Objectives
- Learn how to monitor AI applications and respond to AI-specific security incidents.
- AI security logging
- Monitoring
- Security alerts
- AI abuse detection
- Incident response
- Investigation

GUIDED LAB
Perform a safe security inspection on Learning Objectives in a controlled lab and report risks.

INTERVIEW & ASSESSMENT
Explain common security risks in Learning Objectives and how to protect user data from attacks.

12 MODULE 12: DevSecOps & Secure AI Deployment

- Learning Objectives
- Integrate AI security practices into the software development and deployment lifecycle.
- Secure AI development lifecycle
- Git security
- CI/CD security
- Container security
- Secrets management
- Dependency security

GUIDED LAB
Perform a safe security inspection on Learning Objectives in a controlled lab and report risks.

INTERVIEW & ASSESSMENT
Explain common security risks in Learning Objectives and how to protect user data from attacks.

INVENTATEQ
LEARN SKILLS • GET PLACED

REAL-WORLD PORTFOLIO PROJECTS

Practical industry scenarios, tools applied, and demonstrable project outcomes.

Project 1: Learning Objectives

What it is: Set up the core AI Cybersecurity environment and configure essential business settings.

What you do: Initialize base configurations, create clean templates, and verify workflow controls.

Tools used: AI Security, AI Cybersecurity, Learning Objectives

Project outcome: Working project foundation configured and tested according to best practices.

Project 2: Secure AI development lifecycle

What it is: Build practical OWASP Top 10 modules to handle everyday business operations.

What you do: Create core functional components, validate input data, and prevent common errors.

Tools used: AI Security, OWASP Top 10, Learning Objectives

Project outcome: Functional business module ready to run and demo with zero manual errors.

Project 3: Git security

What it is: Connect Data Security Model with Learning Objectives to automate data and team workflows.

What you do: Set up automated pipelines, link required services, and run end-to-end tests.

Tools used: AI Security, Data Security Model, Learning Objectives

Project outcome: Live automated workflow pipeline documented with clear usage guides.

Project 4: CI/CD security

What it is: Optimize RAG Vector Database workflows for security, speed, and reliability.

What you do: Audit performance bottlenecks, apply security rules, and optimize execution speed.

Tools used: AI Security, RAG Vector Database, Learning Objectives

Project outcome: Production-grade technical deliverable ready to add to your personal portfolio.

Project 5: Container security

What it is: Implement advanced AI Agents Autonomous features matching real industry requirements.

What you do: Configure custom settings, automate repetitive tasks, and test business logic.

Tools used: AI Security, AI Agents Autonomous, Learning Objectives

Project outcome: Production-grade technical deliverable ready to add to your personal portfolio.

Project 6: AI Security End-to-End Capstone

What it is: Build a complete, production-ready AI Security project bringing all skills together.

What you do: Design, code, test, and document a full project workflow from scratch to launch.

Tools used: AI Security, AI Security Monitoring, Learning Objectives

Project outcome: Verified capstone project ready to showcase on your resume and interview calls.

INVENTATEQ
LEARN SKILLS • GET PLACED

ASSESSMENT FRAMEWORK

Module tests, practical evaluations, capstone and completion criteria.

COMPONENT	ASSESSMENT FOCUS	PASS EVIDENCE
Module Knowledge Quizzes	Core AI systems principles, industry terminology, and workflow concepts	Consistent passing score across syllabus unit evaluation tests
Lab Submissions & Practice Reviews	Hands-on AI Application implementation, configuration, and practical exercises	Working lab deliverables satisfying practical evaluation rubrics
Hands-On Mini Projects	Independent problem-solving using intermediate RAG techniques	Functional project artifacts addressing realistic domain scenarios
Final Production Capstone	End-to-end AI Security implementation, quality review, and delivery	Complete capstone submission with technical walkthrough review
Technical Mock Viva	Technical reasoning, troubleshooting approaches, and communication	Successfully defending project decisions in structured mock panels

INVENTATEQ
LEARN SKILLS • GET PLACED

RESUME, GITHUB & LINKEDIN

Evidence-based resume writing and professional project presentation.

- Security portfolio of vulnerability scan reports, packet traces, and playbooks.
- Detailed AI systems diagrams, component specifications, and end-to-end workflows.
- Visual project sheets, live demonstration walkthroughs, and verified functional outputs.
- Project documentation covering AI Application setup, configuration steps, and test notes.
- Direct resume bullet points highlighting hands-on AI Security tools and technical outcomes.
- Structured practice for technical interview pitches, walkthroughs, and viva defense.

INVENTATEQ
LEARN SKILLS • GET PLACED

OUR STUDENT

Meet the learners who turned their goals into successful careers through dedication, skill, and continuous growth.

READ REVIEWS

MS. SNEHA
Placed at Wipro (9.5 LPA)

"The practical lab sessions gave me the confidence to transition into enterprise roles. Working on real-world datasets helped me clear technical interviews effortlessly!"
Course Completed : **AI Security Specialist**
G ★★★★★

MR. HARSHIT
Placed at Accenture (11.2 LPA)

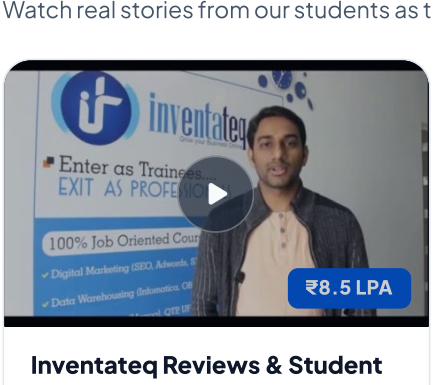
"Inventateq's focus on industry capstone projects and mock interviews was game-changing. The mentors guided me through every real-world implementation hurdle."
Course Completed : **AI Security Specialist**
G ★★★★★

MR. KARTHIK
Placed at Capgemini (10.5 LPA)

"Moving from beginner theory to hands-on enterprise tools was seamless. The portfolio defense preparation helped me crack my MNC placement round!"
Course Completed : **AI Security Specialist**
G ★★★★★

WATCH VIDEOS

Watch real stories from our students as they talk about their journey, growth, and placement success.



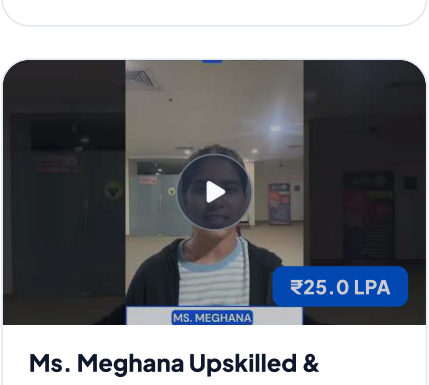
Inventateq Reviews & Student Genuine Feedback Bangalore
Course Video 1 • Student Feedback
Watch Story

AWS Course in Bangalore, Best AWS Training & Certificate with Placement
Course Video 2 • Student Feedback
Watch Story

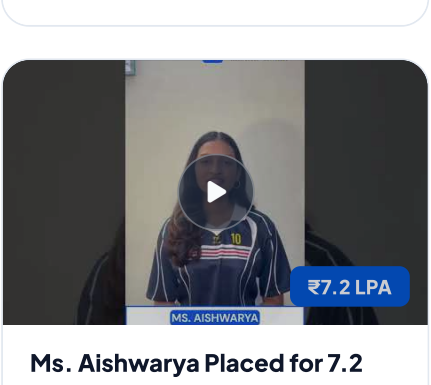
Inventateq HR Practical Training Student Success & Placement
Course Video 3 • Student Feedback
Watch Story

Classes @ INVENTATEQ.COM
₹6.8 LPA

Free Interview Skills Development Classes for Freshers & College Students
Course Video 4 • Student Feedback
Watch Story



Ms. Meghana Upskilled & Placed at 25 LPA
Top Offer • Enterprise Consultant
Watch Story



Ms. Aishwarya Placed for 7.2 LPA Package
Verified Offer • Software Dev
Watch Story

INVENTATEQ
LEARN SKILLS • GET PLACED

CONTACT US

JOB HUNTING ENDS HERE
Start your career with AI Security course that gets your Dream Job!

ADMISSIONS & COUNSELLING
+91 85500 00909
Call Now · WhatsApp

CAREER & PLACEMENT DESK
+91 78993 32878
Call Now · WhatsApp

OFFICIAL PORTAL
www.inventateq.com

EMAIL US
info@inventateq.com

LEARNING MODES
Classroom & Online