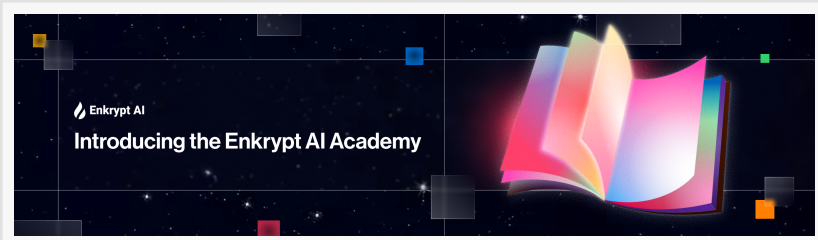
Enkrypt AI Launches Enkrypt AI Academy to Advance Enterprise AI Security Education



BOSTON, MA, UNITED STATES, February 9, 2026 /EINPresswire.com/ -- Enkrypt AI announced the launch of the Enkrypt AI Academy, a free, structured learning platform designed to strengthen AI security, compliance, and governance capabilities across the global AI ecosystem.

As organizations accelerate adoption of generative AI, large language models (LLMs), retrieval-augmented generation (RAG) systems, and agent-based workflows, security and compliance teams face an expanding threat landscape. At the same time, AI engineers and product teams often lack centralized, practical resources that address how to design and deploy secure AI applications from the outset.

> AI safety, governance, security, and risk aren't the same. Confusing them creates real exposure in AI deployments. The Enkrypt AI Academy delivers clear, practical guidance for production teams."
> *Sahil Agarwal, CEO, Enkrypt AI*

The Enkrypt AI Academy was created to address this industry-wide gap — and to make AI security knowledge broadly accessible to the engineers building the next generation of AI systems.

Building AI Security as a Community Standard

The Academy isn't just an enterprise training program. It is designed as an open resource for the global AI engineering community.

By offering the platform free of charge, Enkrypt AI aims to:

- Establish shared terminology across AI safety, governance, security, and risk
- Provide practical implementation guidance to developers shipping AI features
- Equip security teams with updated threat models for LLMs, RAG systems, and agents
- Support compliance leaders in operationalizing AI governance frameworks

As AI systems increasingly power customer-facing applications, regulated workflows, and

automated decision systems, secure design practices must become a default standard — not an afterthought.

Advancing Practical, Implementation-Focused Learning

The Academy provides a structured, production-informed curriculum for developers, security engineers, compliance leaders, and product teams.

The program includes:

- A structured curriculum covering the full AI security lifecycle
- Short, role-specific learning modules
- Video walkthroughs and applied demonstrations
- Practical guardrail and red teaming guidance
- Self-paced progress tracking

The curriculum spans six core domains:

- **Foundations** — AI architecture and threat modeling fundamentals
- **Guardrails** — Protections against injection attacks, data leakage, and unsafe outputs
- **Red Teaming** — Adversarial testing methodologies
- **Policies and Compliance** — Operationalizing governance controls
- **Endpoints and Integrations** — Securing models, APIs, and agent frameworks
- **MCP Security** — Protecting emerging protocol layers connecting AI to tools and data

Together, these domains reinforce secure-by-design development practices across the AI lifecycle.

Availability

The Enkrypt AI Academy is now live and accessible online. Developers, security professionals, and AI leaders can register and begin coursework immediately.

For more information, visit: https://academy.enkryptai.com

About Enkrypt AI:

Enkrypt AI is an enterprise AI security, compliance, and governance platform purpose-built to secure AI, agents, multimodal systems, and MCP. The company delivers ultra-low-latency, policy-based guardrails that enforce security, safety, and compliance in real time—helping prevent risks such as prompt injection, sensitive data exposure, unsafe outputs, and noncompliant agent

behavior across models and toolchains. Enkrypt AI's red teaming engine provides comprehensive, policy-driven, multimodal attack simulation across models and agents. At the same time, its MCP Scan Hub and Secure MCP Gateway help protect MCP servers, tools, and agent toolchains end-to-end. Serving enterprises in regulated industries, including finance, healthcare, insurance, and government, Enkrypt AI helps organizations ship fast, ship safe, and stay ahead. For more information, visit

Sheetal Janala
Enkrypt AI
email us here
Visit us on social media:
LinkedIn
YouTube
X
