Enterprise LLM Security: Safeguarding AI Applications in the Private Cloud

Defend the new frontier of enterprise AI — where applications, prompts, and data meet

+91-9742266597 www.saavigen.ai contact@saavigen.ai

Overview

Integrating AI into enterprise systems is no longer optional — it's essential. But every AI feature, API call, and prompt you add introduces a new attack surface. Generative AI, LLMs, and contextual prompts have opened powerful capabilities — and entirely new threat vectors.

Traditional security models weren't built for this. Defending the enterprise now means defending AI pipelines, prompt interfaces, and model interactions that process sensitive data and drive business logic.

This course helps your teams relearn how to defend in the age of GenAI. Grounded in the OWASP Top 10 for LLM Applications, it equips developers, architects, and security professionals to identify, assess, and mitigate AI-specific risks — from prompt injection and data leakage to insecure RAG design and model misuse.

Participants gain hands-on experience securing the new AI stack — applying OWASP frameworks to protect what truly matters: your enterprise data, reputation, and trust in an AI-driven environment.

Who Should Attend

- This program is built for the people responsible for making AI safe inside the enterprise — the ones integrating, governing, and defending AI systems that connect to sensitive data and mission-critical apps.
- **Ideal participants include:**
- **Application Security & Cloud Security Teams** integrating LLMs into products and workflows
- **AI Solution Architects & Platform Engineers** deploying private or API-based LLMs on enterprise cloud
- **DevSecOps & Data Protection Specialists** implementing AI security and compliance guardrails
- **Governance, Risk & Compliance (GRC) Leaders** defining policies for safe and responsible AI adoption
- **Product Owners & Innovation Teams** embedding GenAI into enterprise applications

Prerequisites:

Familiarity with APIs, data flows, and enterprise security practices. No prior ML expertise required.

Learning Outcomes

By the end of this program, participants will:

1. **Understand the New Threat Surface**
   Learn how GenAI, LLMs, and contextual prompts reshape enterprise attack vectors — from data leakage and model misuse to insecure RAG design.
2. **Apply OWASP LLM Top 10 in the Enterprise Context**
   Translate OWASP's global AI security framework into actionable controls and mitigation strategies for your organization.
3. **Secure AI Pipelines and Integrations**
   Protect data, APIs, and context flows in applications using LLMs or GenAI services — both on-prem and in private cloud.
4. **Detect and Defend Against AI-Specific Attacks**
   Simulate prompt injection, context poisoning, and model abuse — and design countermeasures that work in production.
5. **Implement Enterprise AI Governance**
   Embed security-by-design, auditability, and compliance controls across your AI development and deployment lifecycle.
6. **Build Organizational Confidence in AI Security**
   Move from reactive patching to proactive defense — enabling safe innovation without compromising trust or compliance.

Program Structure

Duration & Format

2 Days (Total 12 Hours)

A high-impact, blended experience combining live sessions, guided security labs, and team simulations.

Delivery Mode: Hybrid (In-person or Virtual)

Program Highlights

- **Blended, Experiential Learning Design**
  Combines live expert sessions, guided labs, and team simulations for hands-on mastery of AI security.
- **OWASP-Aligned Framework**
  Structured around the OWASP Top 10 for LLM Applications — bringing global AI security standards into practical enterprise context.
- **Real-World Attack–Defense Labs**
  Experience live simulations of prompt injection, context leakage, and insecure RAG design — then apply countermeasures that work in production.
- **Defense in Depth for AI Systems**
  Learn layered protection strategies for prompts, APIs, data flows, and private LLM deployments.
- **30-Day Continued Learning Platform**
  Reinforce skills post-workshop through daily "AI Defender" micro-labs, governance templates, and mentor access.
- **Corporate-Ready Security & Compliance Content**
  Designed for enterprise adoption — aligning technical defenses with compliance, privacy, and governance mandates.

Workshop Highlights

Day	Mode	Focus Area	Key Outcomes
Pre-Workshop (Optional)	Online (1 hr self-paced)	AI Security Readiness & Primer	Understand baseline AI security posture
Day 1 (6 Hours)	Live + Guided Labs	**The New AI Threat Surface** • Overview of GenAI & LLM Security Fundamentals • OWASP LLM Top 10 for Enterprise • Threat Modeling for AI Pipelines **Hands-on Labs:** Prompt Injection, Context Leakage	Identify enterprise AI risks and simulate key vulnerabilities
Day 2 (6 Hours)	Live + Simulation	**Defense in Depth & Governance** • RAG & API Hardening Techniques • Data Isolation, Access Control & Monitoring • Governance & Policy Design for Private LLMs **Red vs Blue Simulation:** Defend an enterprise AI app	Implement mitigations and governance for secure GenAI deployment
Post-Workshop (30 Days)	Online Reinforcement	Micro-Labs + Templates	Reinforce learning, deploy internal AI security playbook

Extended Learning

Pre & Post Assessments

Benchmark improvement in AI security awareness, threat modeling, and mitigation application.

Security Reinforcement Learning App (30 Days)

- Access recordings, code labs, and governance templates
- Daily micro-labs to sustain application of OWASP controls

Certification

All participants completing the workshop and post-assessment will receive

Duration & Format

2 Days (9:30 AM – 4:30 PM)

Mode: In-person / Virtual Instructor-led

Format: Blended learning with live sessions, labs & team simulation

Contact Information

For Further Inquiries

www.saavigen.ai | contact@saavigen.ai | +91-9742266597