AI Security & Red Teaming

OWASP LLM Top 10, prompt injection, data leakage and guardrails.

DURATION	FORMAT	LEVEL	LABS
24 hours	Onsite, online or hybrid	Advanced	Cloud sandbox included

About this programme

Security programme for teams building or approving LLM applications: the OWASP Top 10 for LLM applications, hands-on red teaming of chatbots, RAG and agents, and the layered defences that reduce real risk.

Who it is for: Application security engineers, AI engineers and security architects

What your team will be able to do

- Threat-model LLM, RAG and agent applications
- Execute and document prompt-injection and data-exfiltration attacks in a lab
- Apply layered guardrails: input/output filtering, least-privilege tools and sandboxing
- Set up continuous red teaming and AI security testing in the SDLC

Before you start

- Application security experience, such as the OWASP Top 10
- Basic understanding of how LLM applications use prompts and retrieval

Course outline

We send the module-by-module outline with your proposal, adapted to your team's tools and goals.

Assessment and certification

How learning is checked

- A short knowledge check on day one and again at the end, so you can see each person's progress
- Graded hands-on labs in every module, reviewed by the trainer
- A final exercise that applies the programme to a problem like your team's own

Certificate and exams

- Participants who complete the programme receive a Cognitive Networks AI certificate of completion.

Formats and cohort size

- Onsite: At your office or a venue you choose, in full days.
- Online, live: Instructor-led over video, usually in half-day sessions so people can keep up with work.
- Hybrid: Some days in a room together, the rest online. Useful when a team works across cities.

Cohort size: 15 to 25 people per trainer. Larger teams run as parallel cohorts on the same outline, so everyone learns the same thing.

Pricing: We quote per cohort, based on duration, format and number of cohorts. There is no per-seat price list: tell us your team and we send a proposal within one business day.

Bring this programme to your team

Request a proposal at cognitivenetworks.ai/contact?programme=ai-security-red-teaming

reachus@cognitivenetworks.ai · Bangalore +91 72043 05303 · Dallas +1 (303) 827-7415