CORSEN AI Academy

AI Security and Red Teaming

Course syllabus

Version 2026-11

Overview

Covers prompt injection, jailbreaking, guardrails, moderation, red teaming, and GDPR compliance for AI.

Learning objectives

- Map risks specific to applications based on language models
- Identify and prevent prompt injection attacks and jailbreak attempts
- Implement input and output validation guardrails
- Leverage moderation APIs and multi-layer filtering
- Conduct a red teaming exercise and document findings

Audience and prerequisites

Developers, engineers, and integrators looking to leverage ChatGPT via API in their applications.

Proven experience in application development and deployment.

Duration and format

Estimated duration : 1 h 45 min. 100% online self-paced course, accessible 24/7 from a browser. Progress is saved, allowing you to resume at any time. Estimated duration: 1 h 45 min.

Content

- Threats and Attack Surface (4 lessons)
- Defenses (5 lessons)
- Red teaming (3 lessons)
- Compliance (2 lessons)

Assessment

Application exercises provided throughout the lessons. Each lesson ends with its Key takeaways, supporting self-assessment. A final quiz of 5 corrected questions, at the end of the last lesson, validates acquired skills.

Accessibility

Self-paced course accessible to people with disabilities: text content compatible with screen readers, keyboard navigation, and compliant contrasts. For any adaptation needs, email hello@corsen.ai.

Price and recognition

Free

Certificate of completion issued by Corsen AI.

Access time

Immediate after account creation and email confirmation.

Corsen AI — Paris, France — SIRET 10297040700015
academy@corsen.ai — https://academy.corsen.ai