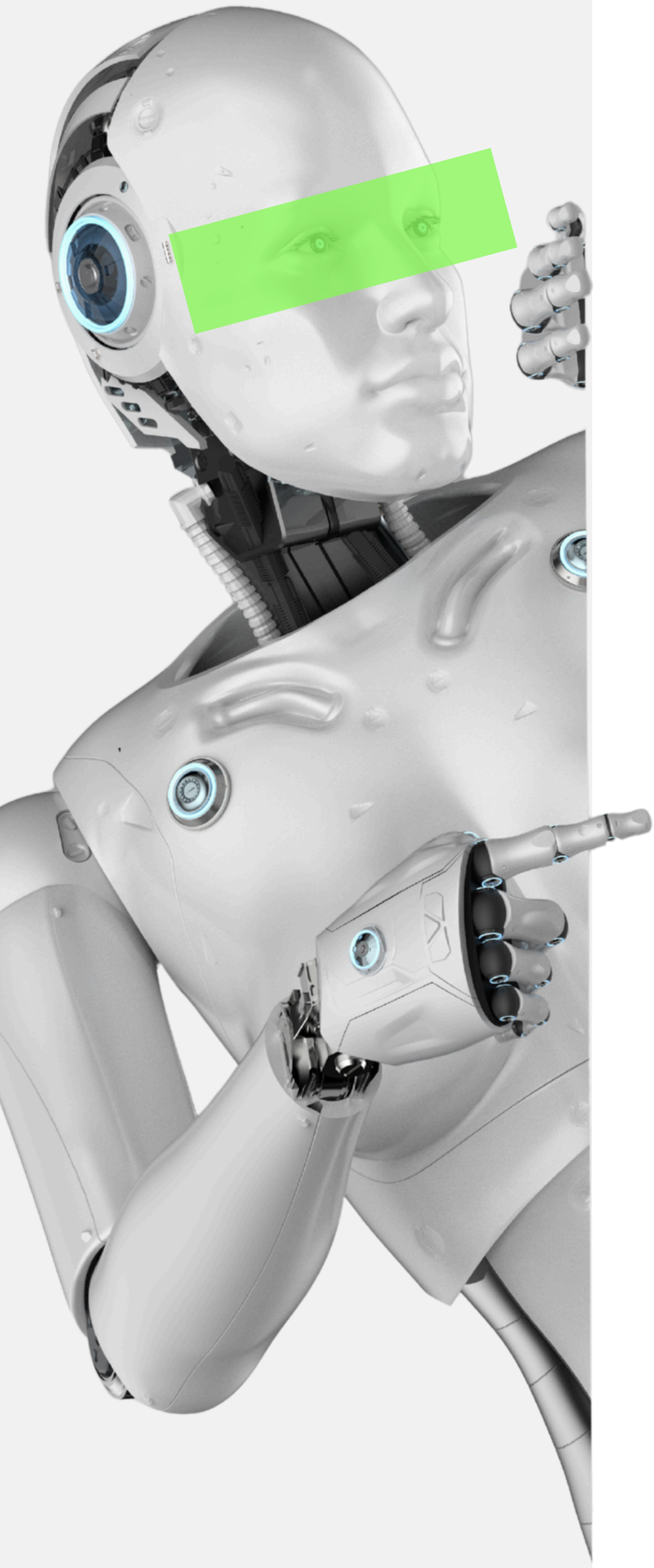


AI Security Workshop

CAN CHATGPT BE HACKED?

2-Day AI Security Hands-on Workshop

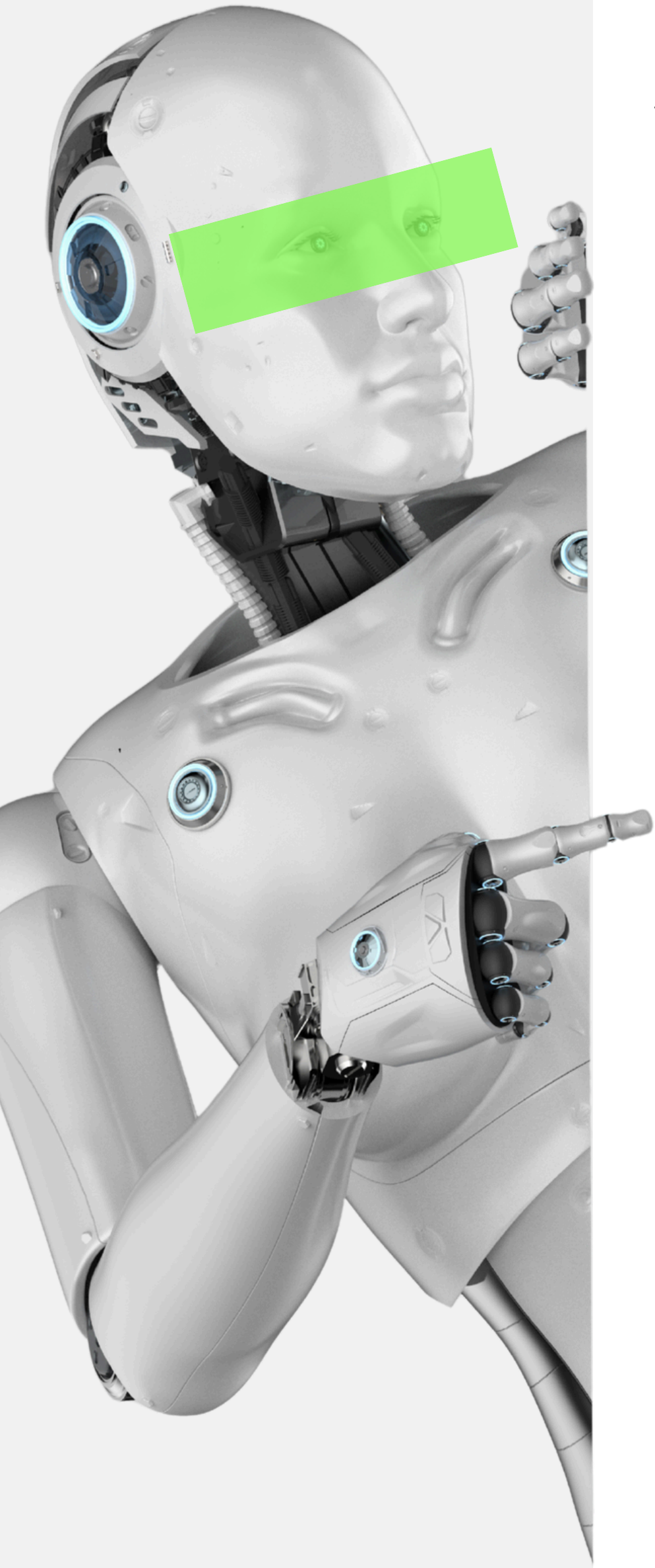
Prompt Injection • RAG Security •
Guardrails • AI Red Teaming

Learn how AI apps can
be attacked
and how enterprises
secure them
with practical demos
and real-world
AI security use cases.

Are you ready for the
future of AI Security?

Break • Protect • Red Team AI Apps

2 Days | 2 Hours/Day | Total 4 Hours



Workshop Curriculum

2 Days | 2 Hours/Day | Total 4 Hours

Day 1: Can ChatGPT Be Hacked?

- AI Security Basics
- System Prompt vs User Prompt
- Prompt Injection Live Demo
- AI Data Leakage Scenario
- OWASP LLM Top Risks
- Student Prompt Challenge

Day 2: Enterprise AI Security

- RAG Security
- Company PDF Chatbot Demo
- AI Guardrails & PII Masking
- AI Agent Security
- AI Red Team Report Preview
- Career Roadmap

Hands-on Highlights

- Prompt Injection Demo
- PDF Chatbot Demo
- Guardrails Before/After
- Red Team Report Preview

Register Now