COURSE TABLE OF CONTENTS

AI Redteaming

OEM: Koenig Original • Duration: 2 Days (16 hrs)

COURSE MODULES & TOPICS

Module 1: Introduction to AI Redteaming

- Understanding AI redteaming
- AI threat modelling
- AI attack vectors
- Redteaming methodologies
- Case study: AI vulnerabilities

Module 2: Practical AI Security Assessment

- AI penetration testing
- Vulnerability assessment tools
- Securing AI deployments
- Incident response in AI systems
- Best practices for AI security

© Koenig Solutions