COURSE TABLE OF CONTENTS

Promptfoo

OEM: Open Source • Duration: 1 Day (4 hrs)

COURSE MODULES & TOPICS

Module 1: Foundations and Setup

- Evaluation and red teaming objectives
- Application scope and test limits
- Install Promptfoo
- Run a small baseline evaluation (LAB)

Module 2: Providers and Test Cases

- Prompts and variables
- Model providers and HTTP targets
- Test datasets
- Connect a training application
- Create YAML test cases (LAB)

Module 3: Red Team Configuration

- Application purpose
- Relevant plugins
- Custom policies
- Attack strategies
- Generate and run tests for prompt injection
- Test for disclosure and policy violations (LAB)

Module 4: Results and Retesting

- Results viewer and evidence review
- Export results
- Regression test selection
- Compare baseline with revised application
- Rerun failures (LAB)