

GENERATIVE AI Testing



Gen AI Testing

Module 1: Foundations of AI Testing

- ✓ Difference between traditional software vs AI systems
- ✓ AI application architecture (Model → Prompt → App → UI)
- ✓ Probabilistic outputs vs deterministic validation
- ✓ AI defect categories overview
- ✓ AI testing lifecycle and evaluation approach

Module 2: LLM Fundamentals

- ✓ Tokens, context window, cost
- ✓ Temperature, randomness control
- ✓ Prompt engineering basics
- ✓ RAG vs Fine-tuning
- ✓ LLM inference pipeline

Module 3: AI Defects

- ✓ Hallucination detection
- ✓ Prompt injection attacks
- ✓ Bias and fairness
- ✓ Inconsistency behavior
- ✓ AI bug reporting

Module 4: AI Test Design

- ✓ AI test case format
- ✓ Evaluation criteria design
- ✓ Statistical testing
- ✓ Boundary & edge cases
- ✓ Test library creation

Module 5: Hallucination Testing

- ✓ Oracle design
- ✓ Golden datasets
- ✓ Open vs closed domain testing
- ✓ Rate measurement
- ✓ Reporting

Module 6: Security Testing

- ✓ OWASP LLM Top 10
- ✓ Injection testing
- ✓ Jailbreaking
- ✓ RAG poisoning
- ✓ Security reporting

Module 7: Bias Testing

- ✓ Bias taxonomy
- ✓ Counterfactual testing
- ✓ Statistical validation
- ✓ Consistency testing
- ✓ Compliance

Module 8: RAG Testing

- ✓ RAG architecture testing
- ✓ Context validation
- ✓ RAGAS metrics
- ✓ Negative testing
- ✓ Source attribution

Module 9: AI Agents Testing

- ✓ Agent architecture
- ✓ Tool testing
- ✓ Memory testing
- ✓ Multi-agent validation
- ✓ Trace debugging

Module 10: Red Teaming

- ✓ Threat modeling
- ✓ Jailbreak testing
- ✓ Adversarial testing
- ✓ Toxicity testing
- ✓ Report writing

Module 11: Python & API Testing

- ✓ Python basics
- ✓ API testing
- ✓ Async testing
- ✓ Env management
- ✓ Error handling

Module 12: Pytest

- ✓ Test structure
- ✓ Fixtures
- ✓ Mocking
- ✓ Reporting
- ✓ Test pyramid

Module 13: DeepEval

- ✓ Evaluation metrics
- ✓ Custom metrics
- ✓ Dataset creation
- ✓ Integration
- ✓ CI gating

Module 14: RAGAS

- ✓ Pipeline setup
- ✓ Metrics
- ✓ Dataset creation
- ✓ Regression testing
- ✓ CI integration

Module 15: Prompt Testing

- ✓ Versioning
- ✓ Regression testing
- ✓ A/B testing
- ✓ Adversarial testing
- ✓ Optimization

Module 16: Agent Automation

- ✓ Framework setup
- ✓ Unit testing
- ✓ State testing
- ✓ Trace assertions
- ✓ Regression testing

Complimentary Workshops:

- ✓ UI Testing with Playwright
- ✓ Performance Testing in Gen AI
- ✓ Security Automation in Gen AI testing
- ✓ CI/CD in Gen AI Testing
- ✓ LLMOps