

AI Integration for Security Workflow Automation (LFWS303)

Course Duration: 8 Hours

TOC

Foundations & First Workflow

- Introduction & Setup
- Why Automate Security?

Threat Intelligence Workflow

- Concepts
- Lab: Build a Threat Intelligence Enrichment Workflow
- AI Risks, Guardrails & OWASP Top 10 for LLMs

AI-Powered Threat Analysis with RAG

- Concepts
- Lab: Add AI-Powered Threat Analysis with RAG and Guardrails
- Full Pipeline & Capstone

End-to-End SOC Pipeline

- Concepts
- Lab: Build an End-to-End SOC Pipeline with a Live SIEM
- Challenge: Race to Detect and Respond
- Team Presentations

Wrap-Up & Next Steps