Course 3 — AI for Threat Detection & Security Operations

Tier: 2 (Practitioner-Tutor) · **Days:** 3 · **Cohort max:** 16 · **Ratio:** 1:16
Prerequisites: SOC/security analyst experience.
Tools provisioned: Anomaly-detection sandbox, LLM access, sample log corpus, SIEM sandbox.

Day 1 — AI/ML in anomaly detection: network traffic, user behavior; interpreting model outputs for security alerts; false positive management.
Day 2 — LLMs for log analysis and threat-intel summarization: prompt injection risks in AI systems; securing AI pipelines.
Day 3 — Capstone: build a lightweight anomaly detection prototype or LLM-assisted incident report generator; present findings with confidence levels.

Capstone artifact: Prototype + threat model document.
Tutor certification: Tier 2 (domain: security) + rubric calibration.
Kit-specific notes: All log data synthetic/de-identified; tutor FAQ covers "AI flagged a false positive — how to teach that moment."

www.adeptelitesconsulting.com
info@adeptelitesconsulting.com • +254 182 837 692
GUIDING GROWTH WITH EXPERTISE