COURSE SYLLABUS

Navigating the AI-Driven Cyber Threat Landscape

Audience	Cybersecurity professionals with baseline knowledge of CIA triad, NIST CSF, access control, and incident fundamentals
Format	6-8 hours remote — discussion, scenario work, and guided exercises
Level	300-level (intermediate to advanced)
Outcome	Students leave with a practical 30/60/90-day security improvement plan for AI-era threats

Module 1: AI Threat Shift

Covers how AI is changing the attack surface through AI-assisted phishing, deepfakes, synthetic identity fraud, and attacks on AI systems themselves. Focuses on verification controls, AI model integrity, and the limits of defensive AI.

Module 2: Identity and Zero Trust

Explains what Zero Trust looks like in practice across users, devices, APIs, cloud, SaaS, and non-human identities. Emphasizes privileged access, continuous verification, agentic AI risks, and identity hygiene gaps that still drive breaches.

Module 3: Exposure, Ransomware, and Resilience

Connects CTEM to remediation planning and prioritization. Covers ransomware mechanics, containment sequencing, recovery priorities, business continuity under AI-speed threats, and post-quantum readiness basics.

Module 4: Governance, AI Risk, and Supply Chain

Focuses on AI governance, shadow AI, model and data ownership, executive liability, regulatory obligations, and third-party risk. Also covers supply chain exposure across vendors, open-source dependencies, CI/CD, identity integrations, and cloud interfaces.

Capstone Scenario

Brings together four simultaneous threat threads: deepfake fraud, anomalous SaaS/API access, third-party identity breach, and ransomware with suspected exfiltration. Participants work through containment, escalation, communications, and a 30/60/90-day remediation plan.