AI Security for Information Security Professionals

הקמה והובלה של תכנית אבטחת AI ארגונית מקצה־לקצה

Module 1: AI Security Framework
- Defining AI assets (models, data, prompts, RAG, agents, plugins)
- Building an AI security program: policies, standards, approval workflows
- Risk classification methodology
- Minimum requirements for AI projects

Module 2: Model Protection & Lifecycle Management
- Security across AI lifecycle: data → training → evaluation → deployment → monitoring
- Security gates and checkpoints
- Version control and configuration management

Module 3: LLM/GenAI Security (OWASP Top 10)
- Prompt injection (direct & indirect)
- Sensitive data exposure
- Supply chain risks (plugins, libraries, third-party services)
- Permission and capability management
- External enforcement mechanisms (logging, monitoring, controls)

Module 4: Agentic AI Security
- Threat scenarios: unauthorized tool use, destructive actions, policy bypass
- Capability control: allowlisting, scoped permissions, temporary access
- Human-in-the-loop and dual approval
- Fail-safe design principles
- Audit logging and incident reconstruction

Module 5: Ethics, Regulation & Third-Party Risk
- Governance frameworks: ISO 42001, NIST AI RMF
- Accountability, transparency, human oversight
- Documentation requirements for auditability
- Vendor contractual requirements
- Integration with existing GRC processes
- Risk acceptance procedures

תאריך פתיחה: 17.05.2026

בימי ראשון ורביעי

בין השעות 17:30 - 21:30

במשך 4 מפגשים (20 שעות אקדמיות)

שם המרצה: ניצן לוי, מנתח מערכות מוסמך מטעם לשכת מנתחי מערכות מידע בישראל, בעל תואר שני, מרצה מוסמך מטעם ISC2 ו-ISACA

הקורס היברידי: בקמפוס אוניברסיטת בר-אילן ובזום, סימולטנית

קהל יעד: אנשי אבטחת מידע בעלי ניסיון של למעלה משנתיים

בפיקוח אקדמי של אוניברסיטת בר-אילן

לתאום ראיון קבלה ורישום:
03-5772015
hitech.school@biu.ac.il

בית הספר להייטק וסייבר
היחידה ללימודי תעודה
אקדימה לימודי המשך בר-אילן