COURSE SYLLABUS

Using AI in Cybersecurity Operations Course (Self-Paced)

Put AI tools to work in daily security operations, from summarizing logs and triaging alerts to recognizing the risks AI introduces.

> Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/using-ai-in-cybersecurity-operations-course-self-paced

support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: Understanding AI and Machine Learning for Security Operations

- Lessons:
  - What Generative AI and Large Language Models Are
  - How Machine Learning Already Supports Detection
  - Where AI Fits in the SOC Workflow
  - Capabilities and Limits of Current AI Tools
- Applied activity: given a short description of a SOC's daily alert volume, learners identify which stages of the workflow, collection, triage, investigation, and response, are reasonable candidates for AI assistance and which are not.

Module 2: Applying AI to Detection, Log Analysis, and Alert Triage

- Lessons:
  - Using AI to Summarize and Triage Log Data
  - AI-Assisted Threat Detection and Correlation
  - Reading AI-Generated Alerts and Screenshots: A Walkthrough
  - Validating AI Output Before Acting On It
- Applied activity: learners review screenshots of an AI tool's summarized output for a batch of security logs and a related alert, then decide what to escalate, what to dismiss, and what needs human follow-up before either.

Module 3: Prompt Injection and the Adversarial AI Threat Landscape

- Lessons:
  - How Prompt Injection Attacks Work
  - MITRE ATLAS and Adversarial Tactics Against AI Systems
  - The OWASP Top 10 for Large Language Model Applications
  - Data Poisoning, Model Manipulation, and Supply Chain Risk

- Applied activity: learners review a screenshot of a flagged prompt injection alert from an AI-enabled security tool and identify which part of the input triggered the flag and which MITRE ATLAS tactic it maps to.

Module 4: Governance and Responsible Use of AI in Security Operations

- Lessons:
  - The NIST AI Risk Management Framework Overview
  - CISA Guidance on Secure AI Deployment
  - Human Oversight and Policy for AI-Assisted Work
  - Building a Responsible AI Adoption Plan for a Security Team
- Applied activity: learners draft a short, one-paragraph acceptable-use statement for AI tools on a hypothetical security team, based on the module's governance material.