CYBERIUM
SIMULATOR

XE109

FOUNDATION · LEVEL 1

AI Fundamentals

6
MODULES

447
LAB TASKS

85
CTF CHALLENGES

73
TOPICS

6
COURSE BOOKS

257
SLIDES

6 COURSE BOOKS INCLUDED



This program teaches you to use AI tools properly and to judge what they hand back. You will start with how machines actually learn — supervised, unsupervised and reinforcement learning, each through a worked case study — then open up a language model and see tokens, embeddings, the context window, and how the next word is chosen. From there you work with generative AI directly: writing prompts, getting structured output you can check, and building retrieval and agent workflows that stay reliable. The program then turns to what goes wrong — prompt injection, leaked data, bias, deepfakes, and deciding when not to use AI at all — before you run models yourself, choosing one for the job and sizing it to your hardware. It ends on real work: classifying phishing, investigating an incident, and knowing when to escalate to a person. Throughout, the emphasis is on checking AI output against something trustworthy rather than taking it on faith.

CURRICULUM & WHAT EACH MODULE COVERS

	MODULE	TASKS
01	**AI Foundations** Supervised Learning Case Study: Spam Detection · Regression Case Study: Predicting House Prices · How Machines Learn: Core Mechanics · Unsupervised Learning Case Study · *+4 more*	42
02	**How AI Works** Tokenization – Turning Text into Numbers · Where Answers Come From · Embeddings and Semantic Similarity · Next-Token Prediction and Sampling · *+8 more*	56
03	**Working with Generative AI** Verifying AI Output Before You Trust It · Structured Output & JSON Validation · Evaluating & Classifying AI Outputs · Conversations & Context Management · *+7 more*	63
04	**AI Security, Safety & Trust** Verifying AI Claims Against Trusted Sources · Protecting Sensitive Data from AI Tools · Prompt Injection and Trust Boundaries · Human Oversight and Automation Bias · *+8 more*	78
05	**AI Tools & Ecosystem** Selecting and Matching Models to Real Jobs · Running Models Locally: Loaders and Servers · Quantization and Sizing Models to Hardware · Memory Budgeting for a Running Model · *+10 more*	96
06	**AI in Practice** Verifying Code Against a Reference Implementation · Human Oversight and Approval for Automated Actions · Verifying AI Outputs Across Different Domains · Three Approaches to Classifying Phishing · *+12 more*	112

GOOD TO KNOW

Starts from zero — no prior experience needed · Self-paced or trainer-led · Cy, the AI helper, answers in the student's own language

HOW EVERY MODULE RUNS

Lab → Extra at 80% → Timed test at 85% → Slides at 90%

A REAL TASK FROM MODULE 4 — AI SECURITY, SAFETY & TRUST

"Work in /opt/ailab/course/m4 in a terminal on the lab machine. Read theory/injection-cases.txt (I1–I6). Which cases are indirect prompt injection? Enter their IDs in number order with nothing between them."

Finish with a capstone project · interview preparation

DATA AS OF 2026-11-09 · V261109