AI-Augmented Cybersecurity: Vibe Coding Edition

What You Will Learn

* **Master** the principles of Context Engineering, aka “vibe” coding, moving beyond simple prompts to create intelligent AI partners.
* **Learn** to leverage an AI-first code editor to build and maintain context for complex security tasks.
* **Gain hands-on practice** framing cybersecurity challenges, defining rules, and managing AI-generated code and analysis.
* **Discover** how to optimize your interactions with LLMs to improve accuracy and reduce costs (Tokenomics).

Course Overview

This course introduces cybersecurity professionals to the next evolution of AI interaction: Context Engineering. Go beyond the limitations of "vibe coding" and one-shot prompts to build a persistent, context-aware AI workspace. You will learn how to effectively embed project-specific rules, documentation, and codebases into an AI-first editor, transforming your AI assistant into a true subject matter expert for your specific security challenges.

By mastering the art of Context Engineering, you can dramatically accelerate and enhance critical security operations, including:

* **Code Analysis** (e.g. auditing for vulnerabilities, deobfuscating malicious scripts)
* **Incident Response** (e.g. drafting reports, correlating IoCs, analyzing logs)
* **Threat Intelligence** (e.g. summarizing CTI reports, etc.)

Course Outline

Module 1: Foundations of Context Engineering

* Introduction: The Evolution from "Vibe Coding" to Context Engineering
* Core Concepts: What is Context and Why It's Critical for AI Accuracy
* The AI-First Editor: Introducing the Tools (e.g. Cursor)
* Use Case Deep Dive: Applying Context Engineering to a Real-World Security Scenario

Module 2: Building & Managing Your Context

* Cursor Fundamentals: Using '@' to Reference Files, Symbols, and Documentation
* Defining Persistent Rules: Crafting .cursor-rules to Guide the AI's Behavior
* Restoration Methods & Git Basics: Using Version Control as Your Safety Net
* Configure a workspace with rules for analyzing a suspicious Python script.

Module 3: *Advanced Application & Optimization*

* Task Framing & Specification: Deconstructing Complex Security Problems for the AI
* Tokenomics & Saving Money: Understanding How Context Impacts Cost and Performance
* Strategies for Efficient Context: Managing Context Windows and Optimizing for Speed
* Use your configured workspace to analyze, refactor, and document the suspicious script, while managing the AI's output with Git.

Who Should Attend

Security engineers, analysts, SOC staff, threat hunters, detection engineers, incident responders, AppSec pros, and aspiring career-switchers who want market-ready, **AI-era skills**.

This includes, but is not limited to:

* Security Engineers

* Security Analysts
* Threat Intelligence Professionals
* SOC (Security Operations Center) Personnel
* Cybersecurity Managers and Leaders
* Anyone interested in leveraging AI for cybersecurity

Audience Skill Level

Beginner to Intermediate (comfortable with basic security concepts; labs are scaffolded).

Student Requirements

Students should be comfortable with:
- Using Linux shell and SSH
- Basic networking concepts and services (e.g. TCP/IP, DNS, DHCP, etc…)

Students will benefit from having:
- Some Python scripting knowledge is recommended, but not required.
- Some YAML scripting familiarity is recommended, but not required.
- Some basic SaaS LLM experience (e.g. ChatGPT) is recommended, but not required.

What Students Should Bring

Students will need to bring to the class:
* A laptop with admin access to install software (e.g. PuTTY, Chrome, etc.).
* Browser (Chrome/Firefox), SSH client, terminal (e.g. PS, Bash, Zsh, etc.).
* The Laptop needs to be able to join a wireless network and access cloud services hosted in common Cloud Service Providers (e.g. AWS, Azure, & GCP), as well as common LLM providers (e.g. OpenAI, Anthropic, Gemini, etc.).

What Students Will Be Provided With

Students will need to bring to the class:
* A copy of the course slides
* Access to our Discord server, to continue the conversation after the event.

Trainer

Bryce Kunz (@TweekFawkes) loves researching red team techniques for bleeding edge services (e.g. LLMs, Generative AI, Cloud, etc.). Previously Chief Strategy Officer (CSO) at Stage 2 Security // UltraViolet Cyber, supported the NSA (network exploitation & vulnerability research), Adobe (built a red teaming program for cloud services), and DHS (incident response). Bryce holds numerous certifications (e.g. OSCP, CISSP, …), has spoken at various security conferences (i.e. BlackHat, DerbyCon, BSidesLV, etc …) and teaches classes at BlackHat (e.g. AWS & Azure Exploitation).

Experience

Date: Week of October 20th, 2025
Duration: 2 Hours
Format: In-Person at Adobe's Office in Bucharest Romania
Location: Anchor Plaza, Bd. Timișoara 26Z, București 061331, Romania

---