AI-Augmented Cybersecurity: Low-Code AI Edition

What You Will Learn

* **Learn** the fundamentals of building AI-powered workflows without extensive coding.
* **Discover** how to use platforms like Make.com and N8N to automate critical cybersecurity tasks.
* **Gain hands-on practice** creating AI agents for security analysis, alert triage, and incident response.

Course Overview

In today's threat landscape, security teams are often overwhelmed by a high volume of alerts and repetitive tasks. This course will teach you how to leverage low-code platforms and AI to build powerful automations and autonomous agents, acting as a force multiplier for your security operations. You will learn to automate previously time-consuming workflows, enabling you to focus on the most critical threats. We will cover practical, hands-on applications for a variety of cybersecurity use cases, including:

* **Phishing Analysis:** Build workflows to analyze suspicious emails and/or attachments.
* **Vulnerability Management:** Automate the process of creating pentest findings from vulnerability data.
* **Bug Fixes:** Utilize AI to suggest and implement fixes for simple bugs in scripts and automations.

Course Outline

Module 1: Fundamentals of Low-Code AI Automation

* Introduction to AI Workflow Fundamentals (Triggers, Actions, Logic).
* The Power of Low-Code/No-Code (LCNC) for Cybersecurity.
* Setting up your environment in Make.com.
* AI in Make.com: Integrating OpenAI to build a simple workflow that analyzes text for malicious intent.

Module 2: Building Autonomous AI Agents

* AI Agents Fundamentals: How they differ from simple workflows (autonomy, planning, tool use).
* Introduction to N8N as an Agent-Building Platform.
* Building an N8N agent to create pentest findings from vulnerability data.
* Agentic Workflows: Designing multi-step processes for complex security tasks.

Module 3: AI-Assisted Development and Debugging

* Introduction to OpenAI's Codex for Low-Code Environments.
* Using Natural Language to Generate and Understand Code Snippets.
* Using an AI assistant to identify and fix a bug in a broken code (e.g. scripts, web apps, etc.)
* Course Wrap-up: Recap, Q&A, and discussion on productionizing AI automations.

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

---