

# Generative AI & Cybersecurity Professional Certification Program

TOOLS & PROJECTS

OPEN-SOURCE · HANDS-ON · INDUSTRY-GRADE

The definitive certification for cybersecurity professionals ready to operate at the enterprise level. Built on a 100% open-source stack, this program delivers rigorous, scenario-based training across every critical security domain — from offensive operations to AI-driven threat detection and post-quantum cryptography.

# Toolkit

No licensing barriers. No vendor lock-in. Every tool in this curriculum is battle-tested in the real world and trusted by security teams at Fortune 500 companies. You will graduate with hands-on proficiency across the full security spectrum.



## Offensive Security

- Kali Linux & Parrot OS
- Nmap, Metasploit Framework
- BloodHound, Hydra, Responder
- SQLmap



## Blue Team & SOC

- ELK Stack (Elasticsearch, Logstash, Kibana)
- Wazuh EDR/XDR
- Wireshark, Zeek, Suricata
- MISP Threat Intelligence



## Digital Forensics (DFIR)

- Autopsy & Sleuth Kit
- Volatility Framework
- FTK Imager Lite
- Wireshark



## Cloud & DevSecOps

- Docker & Kubernetes (K3s)
- GitLab CI/CD
- Snyk Open Source, Checkov
- OWASP ZAP



## AI & Data Science

- TensorFlow & Scikit-Learn
- Jupyter Notebooks
- Python Security Libraries



## Advanced Cryptography

- Qiskit (Quantum-Ready Simulations)
- OpenSSL
- Hashcat

# Real-World Implementation

Participants apply theoretical mastery through five rigorous, scenario-based labs that faithfully replicate enterprise environments. Each project builds a verifiable, portfolio-ready artifact that demonstrates your capability to security hiring managers and CISOs.

1

## Automated Vulnerability Management Pipeline

Build a continuous security scanning engine using **Nmap** and **OpenVAS** to automate asset discovery. Generate CVSS-based risk reports and prioritize remediation across a simulated enterprise network.

2

## Active Directory Exploitation & Hardening

Execute **Kerberos abuse** and **Pass-the-Hash** attacks using Mimikatz and BloodHound, then pivot to defense — implementing GPO-based hardening to secure the organization's primary identity provider.

3

## AI-Driven Network Anomaly Detection

Train a machine learning model using **Scikit-Learn** and Jupyter on Zeek network logs to identify zero-day malware traffic patterns and enable proactive, intelligence-driven threat hunting.

4

## Securing the CI/CD Pipeline (DevSecOps)

Configure a **GitLab CI pipeline** that automatically executes SAST/DAST scans and container security checks using Docker and Snyk — embedding security directly into the software development lifecycle.

5

## Digital Forensics & Ransomware Incident Response

Investigate a post-compromise scenario using **Volatility** for memory acquisition and analysis. Recover command history and identify malicious processes from a ransomware-infected host image.

# Capstone Project: The Portfolio Builder

The final **24 hours** of the program are dedicated to a high-stakes capstone that consolidates every skill acquired. Choose one elite track and produce a flagship portfolio artifact that speaks for itself in any enterprise interview.

## Track 1: The AI-Powered SOC

Build a functional Security Operations Center using the ELK Stack and Wazuh enhanced with AI to automatically triage alerts and generate mitigation playbooks. Demonstrate the future of autonomous defense operations.

## Track 2: Full-Chain Red Team Engagement

Conduct a comprehensive penetration test on a simulated corporate network — including Active Directory exploitation, lateral movement, and privilege escalation — culminating in an executive-level remediation report.

## Track 3: Post-Quantum Secure Architecture

Implement Zero Trust principles alongside quantum-resistant cryptographic protocols using Qiskit and OpenSSL. Architect a cloud environment that is hardened against both today's threats and tomorrow's adversaries.



**Your GitHub Portfolio:** Upon completion, you will possess documented, deployable evidence of your ability to solve complex enterprise security problems — a living portfolio that sets you apart in a competitive market.