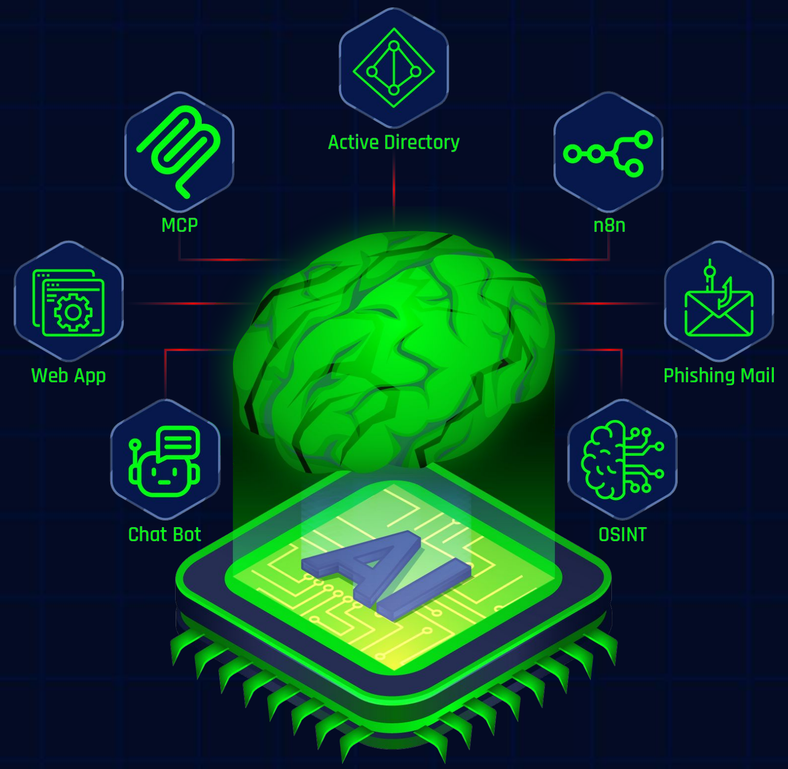
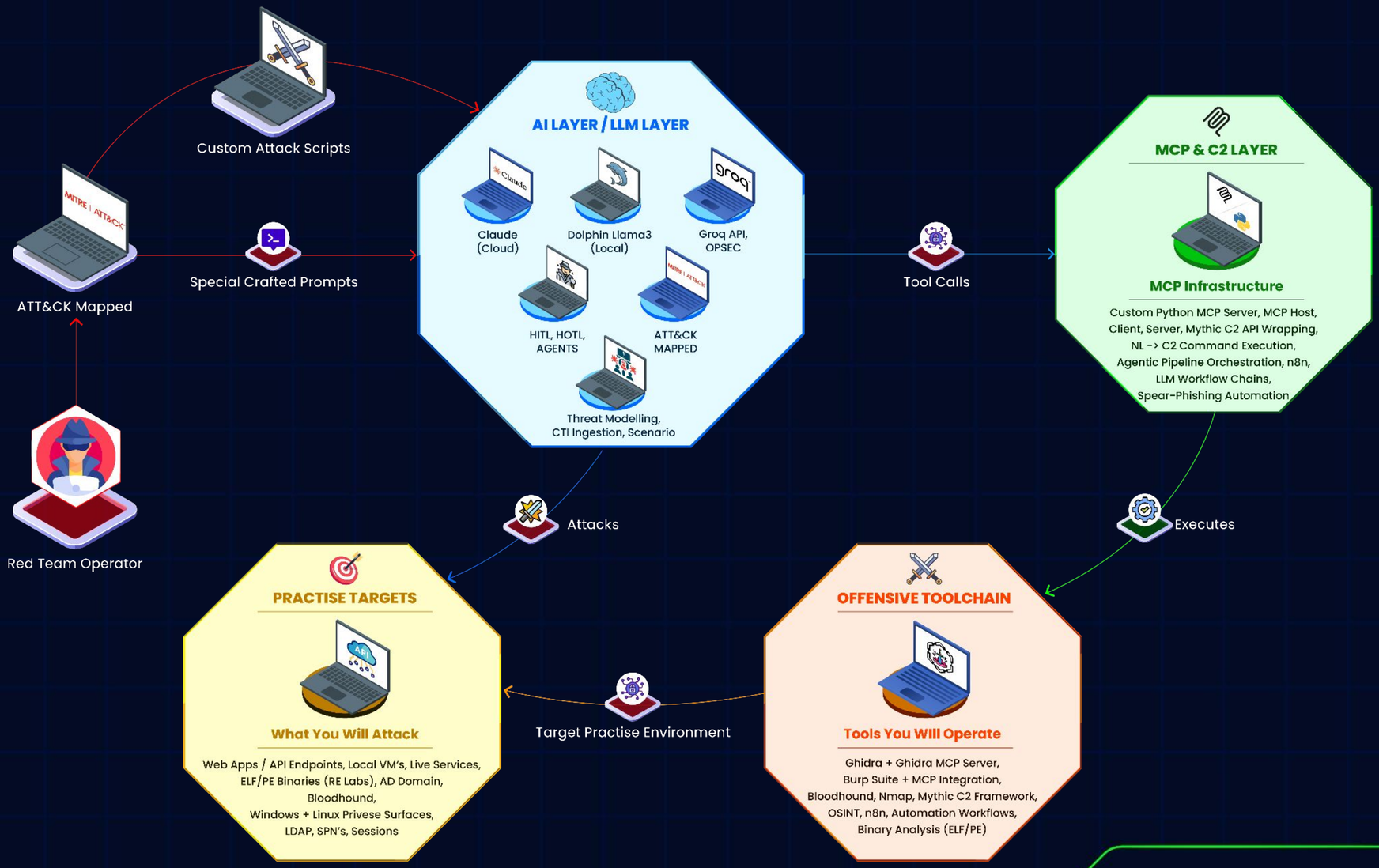
CWL
CyberWarFare Labs

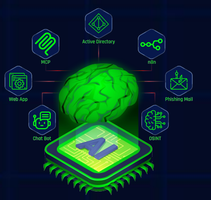
Offensive Cyber Operations with AI (OCO-AI)



Offensive Cyber Operations with AI (OCO-AI) Architecture



I. Introduction to OCO-AI



1.1 Course orientation, learning objectives, and certification roadmap.

1.2 Certification process, exam structure, and attempt policy.

1.3 Lab architecture walkthrough, required tooling setup, and exam environment orientation.

II. Offensive AI Foundations

2.1 The offensive AI mindset : operationalizing LLMs across every phase of the cyber kill chain.

2.2 Human-in-the-Loop vs Human-on-the-Loop: Understanding AI operational control models for adversarial workflows.

2.3 Local vs cloud LLMs: navigating privacy exposure, censorship boundaries, and OPSEC considerations for offensive deployments.

III. AI-Driven Threat Modeling & Attack Planning

3.1 Structuring AI-assisted threat models for realistic attack surface analysis and adversary simulation.

3.2 Automated ingestion and analysis of CTI and DFIR reports to extract actionable offensive intelligence.

3.3 MITRE ATT&CK technique mapping and AI-synthesized attack scenario generation for red team planning.

IV. AI-Assisted Infrastructure & MCP Integration

4.1 Model Context Protocol (MCP) architecture: deep dive into host, client, and server components.

4.2 Agentic tooling concepts: designing autonomous pipelines that interact with live security infrastructure.

4.3 Integrating AI with offensive security tooling and command-and-control frameworks via MCP server interfaces.

4.4 Natural language to C2 command execution: operationalizing LLMs as a direct interface to C2 infrastructure.

CWL
CyberWarFare Labs

V. AI-Powered Reconnaissance Operations

5.1 AI-assisted OSINT collection: autonomous target profiling and phishing-focused intelligence enrichment.

5.2 Context-aware reconnaissance: building LLM pipelines that adapt targeting based on discovered intelligence.

5.3 Automated network scanning, AI-interpreted service analysis, and CVE surface mapping against live targets.

VI. Web Pentesting with AI

6.1 AI-assisted web reconnaissance: attack surface discovery, subdomain enumeration, and technology fingerprinting.

6.2 Automated endpoint and parameter discovery at scale using LLM-augmented tooling.

6.3 Hidden API surface enumeration and AI-guided HTTP request analysis via integrated proxy workflows.

VII. Reverse Engineering with AI

7.1 LLM-augmented binary analysis: decompilation interpretation and AI-assisted behavioral understanding.

7.2 AI-driven script generation and source code reconstruction from decompiled output.

7.3 Vulnerability identification and exploitation opportunity mapping within compiled binaries.

7.4 Custom exploitation path development leveraging trusted system binaries and LOLBIN abuse vectors.

VIII. Red Team Operations with AI

8.1 AI-assisted privilege escalation analysis across Windows and Linux attack surfaces.

8.2 Active Directory enumeration and BloodHound-driven pathfinding augmented with LLM interpretation.

8.3 AI-guided lateral movement planning and OPSEC-safe operational decision-making for multi-stage red team engagements.

CWL
CyberWarFare Labs

THANK YOU

Cyberwarfare.live