CyberSentinel-AI Academy: Guia Rapida

Portada

* **Título:** CyberSentinel-AI Academy: El Futuro de la Ciberseguridad
* **Subtítulo:** Guía Ejecutiva y Hoja de Ruta
* **Versión:** 1.0

Índice Visual

Introducción y Metodología

* **Visión:** "No formamos técnicos; formamos Cazadores de Amenazas potenciados por IA."
* **Enfoque:** 70% Práctico (Python, Labs) / 30% Teórico (Estrategia, Normativas).
* **Herramientas:** Python, LLMs, Firewalls, SIEM, Wireshark.

Capítulo 1: Fundamentos de Ciberseguridad

* **Objetivos:**
* Comprender el panorama de amenazas actual.
* Dominar el modelado de amenazas (STRIDE).
* Entender los vectores de ataque a la identidad.
* **Contenido:**
* Conceptos base: CIA Triad, Risk Management.
* Escenario Banco Digital: Análisis de vulnerabilidades.
* Ataques: Phishing, Credential Stuffing, SQL Injection.
* **Prácticas:**
* `lab01_bank_heist.py`: Simulación de vulnerabilidades bancarias.
* `lab02_credential_stuffing.py`: Ataque y defensa de autenticación.

Capítulo 2: Arquitectura y Defensa

* **Objetivos:**
* Diseñar redes seguras.
* Implementar defensas perimetrales.
* Monitorizar tráfico de red.
* **Contenido:**
* Firewalls: Tipos, reglas y configuración.
* IDS/IPS: Detección vs Prevención.
* SIEM: Centralización de logs y correlación.
* **Prácticas:**
* Configuración de reglas de firewall (iptables/ufw).
* Análisis de tráfico con Wireshark.

CyberSentinel-AI Academy: Guia Rapida

Capítulo 3: Seguridad Moderna con IA

* **Objetivos:**
* Superar las limitaciones de las firmas estáticas.
* Aplicar Machine Learning para detección.
* Realizar Threat Hunting proactivo.
* **Contenido:**
* De firmas a comportamiento.
* Detección de anomalías con ML.
* Threat Hunting: Hipótesis y búsqueda.
* **Prácticas:**
* `lab01_behavior_vs_rules.py`: Comparativa Reglas vs ML.
* `hipotesis_caza.md`: Creación de escenarios de caza.

Capítulo 4: IA Ofensiva y Defensiva

* **Objetivos:**
* Utilizar LLMs para seguridad.
* Automatizar tareas de Red/Blue Team.
* Entender los riesgos de la IA adversarial.
* **Contenido:**
* Prompt Engineering para seguridad.
* Generación de exploits y reglas de defensa con IA.
* Defensa contra ataques a modelos de IA.
* **Prácticas:**
* Laboratorios de IA Applied Security.
* Simulación de ataques generados por IA.

Capítulo 5: Operaciones Avanzadas (SCADA/DFIR)

* **Objetivos:**
* Proteger infraestructuras críticas (OT).
* Gestionar incidentes de seguridad (DFIR).
* Recuperación ante desastres.
* **Contenido:**
* Seguridad en sistemas industriales (SCADA/ICS).
* Forense digital: Adquisición y análisis.
* Playbooks de respuesta a incidentes.
* **Prácticas:**
* Simulación de defensa de Power Grid.
* Análisis forense de disco y memoria.

Capítulo 6: Profesionalización y Carrera

* **Objetivos:**
* Conocer el marco legal y ético.
* Desarrollar habilidades de comunicación.
* Prepararse para el mercado laboral.
* **Contenido:**
* GRC: Gobernanza, Riesgo y Cumplimiento (ISO 27001).
* Ética Hacker: White vs Black Hat.
* Carrera: Roles, certificaciones y soft skills.

* **Prácticas:**
* Redacción de informes ejecutivos.
* Simulación de entrevista técnica.

Equipo y Contacto

* **Director:** Usuario (Visión Estratégica).
* **Copiloto IA:** Trae (Soporte Técnico).
* **Contacto:** academia@cybersentinel.ai
* **Web:** www.cybersentinel.ai