Este proyecto tiene un potencial enorme y, con ese concepto de “toquens de antesala”, aporta un enfoque diferencial muy interesante. Vamos a desglosarlo para que podamos empezar a trabajar en una base sólida y clara. Aquí tienes una propuesta de estructura inicial del proyecto:

**🧠 Nombre Tentativo del Proyecto**

**"SentinelCore"**  
*(o algo en esa línea que evoque vigilancia, núcleo, protección centralizada… podemos debatirlo si quieres)*

**🔍 Objetivo General**

Desarrollar una plataforma modular y extensible que integre herramientas de análisis de vulnerabilidades en sitios web y entornos cloud, proporcionando también guías de mitigación adaptadas a cada hallazgo. Como elemento innovador clave, incorpora un sistema de “toquens de antesala” que actúan como filtros inteligentes y activos antes del almacenamiento local de archivos potencialmente inseguros.

**🧬 Características Clave**

1. **Centralización de Herramientas**
   * Integración con herramientas como:
     + OWASP ZAP
     + Nikto
     + Wapiti
     + Nmap/Netcat para pentesting
     + OpenVAS o Nessus (si se puede enlazar APIs)
     + Detectores de malware cloud (VirusTotal API, ClamAV…)
2. **Sistema de “Toquens de Antesala” (Innovación Propia)**
   * Analizador pre-escritura de archivos.
   * Clasificador de archivos (binarios, scripts, docx/pdf, etc.).
   * Encaminamiento a “toquens especializados” según tipo:
     + Análisis estático (YARA, ClamAV)
     + Sandboxing ligero (por ejemplo, integración con Firejail)
     + Desempaquetado e inspección (UPX, binwalk, etc.)
   * Inoculación o rechazo antes de escritura final en disco.
3. **Informes y Mitigación Automática**
   * Generación de informes en HTML/PDF.
   * Consejos de mitigación basados en bases como OWASP, MITRE ATT&CK.
   * Integración con LLMs locales o cloud para generar textos explicativos sobre vulnerabilidades detectadas.
4. **Arquitectura Modular**
   * Cada “toquen” se instala como módulo.
   * Sistema de dependencias cruzadas entre toquens.
   * Cada toquen puede delegar tareas a otros (comunicación segura entre módulos).
5. **Panel de Control**
   * GUI web o escritorio (Electron o GTK+).
   * Registro de escaneos.
   * Control de toquens, logs, amenazas procesadas.
   * Alertas y eventos críticos.

**🧠 Valor Añadido Frente a la Competencia**

* **Prevención antes del almacenamiento**: no solo detecta, sino que intercepta antes de que la amenaza exista realmente en disco.
* **Modularidad basada en toquens**: microservicios cooperativos que permiten adaptabilidad y extensibilidad.
* **Foco en Mitigación Activa**: no solo reporta, también actúa, orienta o ejecuta scripts para reducir riesgos.
* **Diseño agnóstico**: puede ejecutarse tanto en entornos on-premise como cloud/híbridos.
* **Capacidad educativa**: ideal para Blue Teams, SOCs pequeños y entornos de formación.

**🧱 Próximos Pasos**

1. **Definir stack tecnológico preferido** (¿Python con Flask/FastAPI + Docker? ¿Rust para los toquens críticos?).
2. **Prototipo básico de toquen de antesala**: interceptar un archivo, clasificarlo, redirigirlo.
3. **Diseñar arquitectura general del sistema** (diagrama).
4. **Crear estructura de proyecto modular** (plantilla base con directorios de toquens, configuraciones, etc.).
5. **Benchmark del mercado actual**: qué hacen otros (OpenVAS, Nessus, Rapid7, etc.) y qué no hacen.