Documento de Arquitectura Modular - SentinelCore

# 1. Identificación de Módulos Funcionales

A continuación se describen los módulos principales del sistema SentinelCore, con su propósito y ejemplos de tecnologías asociadas.

|  |  |  |
| --- | --- | --- |
| Módulo | Descripción | Tecnologías Sugeridas |
| Escáner Web | Detecta vulnerabilidades en sitios web. | OWASP ZAP, Wapiti |
| Toquen de Antesala | Intercepta y clasifica archivos antes del almacenamiento. | Python, Watchdog |
| Toquens Especializados | Analizan archivos según su tipo para identificar amenazas. | ClamAV, YARA, PyMuPDF |
| Dispatcher / Orquestador | Gestiona el flujo entre módulos. | Python, colas de tareas |
| Base de Datos | Almacena resultados y trazabilidad. | SQLite, PostgreSQL |
| Interfaz | Permite la interacción con el sistema. | CLI, Flask, GTK |
| Módulo de Mitigación | Muestra recomendaciones específicas. | MITRE ATT&CK, OWASP |
| Generador de Informes | Exporta escaneos e informes en HTML/PDF. | ReportLab, Jinja2 |

# 2. Definición de Interfaces y Protocolos de Comunicación

Todos los módulos se comunicarán mediante JSON como formato estándar, facilitando el intercambio de datos y la interoperabilidad. Se empleará comunicación directa a través de funciones, archivos temporales o colas de mensajes.

Ejemplo de estructura JSON:

{  
 "filename": "documento.pdf",  
 "filetype": "pdf",  
 "from": "toquen\_antesala",  
 "to": "pdf\_sanitizer",  
 "hash": "sha256:abc123...",  
 "timestamp": "2025-06-29T10:45:00"  
}

# 3. Asignación de Responsables

La siguiente tabla asigna a cada miembro del equipo módulos específicos, buscando balancear la carga y especialización.

|  |  |  |
| --- | --- | --- |
| Persona | Módulos Asignados | Justificación |
| Dev A | Escáner Web + Mitigación | Conocimiento de herramientas de análisis y gestión de riesgos |
| Dev B | Toquen de Antesala + Clasificador | Desarrollo del núcleo innovador y detección proactiva |
| Dev C | Toquens Especializados | Análisis profundo de archivos específicos |
| Dev D | Interfaz + Dispatcher + Base de Datos | Conecta módulos y diseña experiencia de usuario |

# 4. Diagrama de Arquitectura General

El siguiente esquema representa los principales componentes y el flujo de información entre ellos:

Frontend Dashboard --> API REST --> Backend  
Backend --> Dispatcher --> Toquen de Antesala --> Toquens Especializados --> Mitigación --> Informe  
Backend --> Escáner Web / Cloud Connectors / DB / Auth

# 5. Validación con el Equipo

Antes del inicio del desarrollo, se realizará una reunión para revisar cada módulo, confirmar entendimiento de funciones, posibles dependencias y definir criterios de éxito. Cada miembro debe validar sus módulos y estar de acuerdo con los protocolos definidos.

Checklist de validación:

* • ¿Están claras las funciones y límites de cada módulo?
* • ¿La comunicación entre módulos está definida y es comprensible?
* • ¿Todos los miembros están cómodos con sus asignaciones?
* • ¿Hay un mecanismo claro de integración?
* • ¿Están identificadas las dependencias técnicas?