**Presentación: SentinelCore - Plataforma Modular de Seguridad como Servicio**

**1. Visión General**

**Objetivo**:  
Desarrollar una plataforma centralizada de seguridad como servicio (SaaS) que:  
✅ Integre herramientas de análisis web/cloud bajo una API única.  
✅ Implemente "toquens" en contenedores Docker para sanitización proactiva de archivos.  
✅ Ofrezca gestión remota mediante dashboard web y WhatsApp como canal de comunicación.  
✅ Sea escalable para técnicos y PYMEs con necesidades específicas.

**Innovación clave**:

* **Toquens Dockerizados**: Microservicios independientes para análisis de archivos.
* **Comunicación multimodal**: Alertas y acciones vía WhatsApp + dashboard web.
* **Arquitectura 100% en la nube**: Sin instalación en cliente, solo API remota.

**2. Diagrama de Arquitectura (Evolución Continua)**

Diagram

Code

Mermaid rendering failed.

**Flujo de trabajo**:

1. Usuario envía archivo/URL vía web o WhatsApp.
2. API Gateway redirige a Dispatcher.
3. Toquens o escáneres procesan en contenedores aislados.
4. Resultados se almacenan y generan informes.
5. Alertas/acciones se envían por WhatsApp o dashboard.

**3. Estructura de Carpetas (Evolutiva)**

plaintext

sentinelcore/

├── api/ # API Gateway

│ ├── main.py # FastAPI

│ ├── whatsapp\_adapter.py # Integración WhatsApp

├── core/ # Núcleo del sistema

│ ├── dispatcher.py # Orquestador

│ ├── config/ # Configuraciones

├── toquens/ # Contenedores Docker

│ ├── maestro/ # Toquen Maestro

│ │ ├── app.py # Lógica de enrutamiento

│ │ ├── Dockerfile # Config contenedor

│ ├── pdf/ # Toquen PDF

│ │ ├── sanitizer.py # Sanitización con PyMuPDF

│ │ ├── Dockerfile

├── web\_scanner/ # Escaneo web

│ ├── zap\_docker/ # OWASP ZAP en Docker

│ │ ├── docker-compose.yml

│ ├── results\_parser.py # Procesamiento JSON

├── partners/ # Integración partners

│ ├── aws\_security.py # AWS Security Hub

│ ├── clamav\_api.py # ClamAV como servicio

├── frontend/ # Dashboard web

│ ├── public/ # Vue.js/React

│ ├── src/

│ │ ├── views/ # Vistas principales

├── docs/ # Documentación

│ ├── architecture.md # Evolución arquitectura

│ ├── api\_specs/ # OpenAPI/Swagger

**Características clave**:

* Cada toquen es un contenedor Docker autónomo (toquens/\*/Dockerfile).
* Integración con partners en carpeta dedicada (partners/).
* Documentación viva en docs/.

**4. Comunicación Multimodal (WhatsApp + Dashboard)**

**Integración con WhatsApp Business API**

python

# Ejemplo: whatsapp\_adapter.py

from fastapi import APIRouter

from twilio.rest import Client

router = APIRouter()

@router.post("/whatsapp/alert")

async def send\_alert(to: str, message: str):

client = Client(account\_sid, auth\_token)

client.messages.create(

body=f"🔒 SentinelCore Alert: {message}",

from\_="whatsapp:+14155238886",

to=f"whatsapp:{to}"

)

**Casos de uso**:

* Alertas de vulnerabilidades críticas.
* Confirmación de acciones (ej: "¿Ejecutar mitigación automática? Responda SI/NO").
* Soporte técnico en tiempo real.

**Dashboard Web**

* **Tecnologías**: Vue.js + Tailwind CSS.
* **Funcionalidades**:
  + Visualización unificada de resultados.
  + Activación remota de herramientas (OWASP ZAP, ClamAV).
  + Gestión de partners externos (ej: Qualys, CrowdStrike).

**5. Toquens Dockerizados (Ejemplo: Toquen PDF)**

dockerfile

# toquens/pdf/Dockerfile

FROM python:3.9-slim

WORKDIR /app

COPY requirements.txt .

RUN pip install -r requirements.txt # PyMuPDF, python-magic

COPY pdf\_sanitizer.py .

CMD ["python", "pdf\_sanitizer.py"]

**Ventajas**:

* **Aislamiento**: Si un toquen falla, no afecta al sistema.
* **Escalabilidad**: Se pueden añadir más instancias bajo demanda.
* **Portabilidad**: Fácil despliegue en cualquier cloud.

**6. Mapeo de Servicios Gestionados**

Diagram

Code

**Ejemplo de flujo con partners**:

1. SentinelCore detecta vulnerabilidad crítica en AWS.
2. Automáticamente activa una solución de CrowdStrike vía API.
3. El técnico recibe confirmación por WhatsApp.

**7. Ventajas Competitivas**

| **Característica** | **Competencia** | **SentinelCore** |
| --- | --- | --- |
| Implementación | Local/SaaS | 100% Cloud (API remota) |
| Comunicación | Email/Web | WhatsApp + Dashboard |
| Toquens | No existe | Dockerizados y especializados |
| Integración Partners | Limitada | API abierta para fabricantes |
| Target | Empresas grandes | PYMEs y equipos técnicos |

**Propuesta de valor**:

* **Para técnicos**: Control centralizado de múltiples herramientas.
* **Para PYMEs**: Seguridad "sin instalación" con soporte accesible.

**8. Próximos Pasos (Roadmap)**

1. **Fase Alpha (2 meses)**:
   * Dockerizar toquens básicos (PDF, Office).
   * Integración OWASP ZAP + WhatsApp API.
2. **Fase Beta (3 meses)**:
   * Dashboard web con autenticación.
   * Onboarding de partners (ClamAV, AWS Security Hub).
3. **Lanzamiento**:
   * Documentación para desarrolladores.
   * Soporte multiidioma en alertas.

**9. Checklist de Validación**

* Pruebas de comunicación WhatsApp con API Gateway.
* Despliegue de toquens en Docker Swarm/Kubernetes.
* Integración con al menos 1 partner (ej: ClamAV Cloud).
* Documentar esquema de carpetas en docs/architecture.md.

**Conclusión**

SentinelCore redefine la gestión de seguridad para PYMEs y técnicos con:  
🚀 **Toquens proactivos** en contenedores.  
📱 **Interacción multimodal** (Web + WhatsApp).  
☁️ **Arquitectura cloud-first** sin instalación local.  
🤝 **Ecosistema abierto** para partners.

**¿Preguntas clave para el equipo?**

1. ¿Priorizar más integraciones con partners en la Fase 1?
2. ¿Incluir Telegram como canal adicional además de WhatsApp?

**Anexos**:

* [Prototipo Figma del Dashboard](https://link_figma/).
* [Repositorio GitHub con Dockerfiles](https://link_github/).