**Herramientas necesarias para ejecutar PlatSentinel**

A continuación se presenta una lista detallada de las herramientas esenciales para el desarrollo, despliegue y operación del proyecto PlatSentinel, junto con su función general y su papel específico dentro del proyecto.

**1. Docker**

* **Función general:** Plataforma de contenedores que permite empaquetar aplicaciones y sus dependencias en entornos aislados y portables.
* **Función en PlatSentinel:** Cada “token” (módulo funcional, como escaneo web o análisis de archivos) se ejecuta en su propio contenedor Docker, garantizando independencia, escalabilidad y fácil despliegue en cualquier entorno[1](https://www.hiberus.com/crecemos-contigo/docker-y-microservicios/)[2](https://appmaster.io/es/blog/arquitectura-de-microservicios-docker).

**2. Docker Compose**

* **Función general:** Herramienta para definir y gestionar aplicaciones multicontenedor.
* **Función en PlatSentinel:** Orquesta el despliegue simultáneo de todos los servicios y tokens, facilitando la gestión y el escalado del sistema[1](https://www.hiberus.com/crecemos-contigo/docker-y-microservicios/).

**3. FastAPI**

* **Función general:** Framework web moderno para construir APIs rápidas y seguras en Python.
* **Función en PlatSentinel:** Implementa la API central que conecta el dashboard, los tokens y las integraciones externas, gestionando autenticación y comunicación entre módulos.

**4. RabbitMQ**

* **Función general:** Sistema de mensajería para la comunicación asíncrona entre servicios.
* **Función en PlatSentinel:** Facilita la transmisión de tareas y resultados entre el backend y los tokens, asegurando la escalabilidad y desacoplamiento de procesos.

**5. ClamAV**

* **Función general:** Antivirus open source para el análisis y detección de malware en archivos.
* **Función en PlatSentinel:** Utilizado por el “toquen de antesala” para analizar archivos antes de su almacenamiento, bloqueando amenazas antes de que ingresen al sistema[3](https://blog.hackmetrix.com/10-herramientas-de-seguridad-informatica-y-como-usarlas/).

**6. OWASP ZAP / OpenVAS / Nessus**

* **Función general:** Escáneres de vulnerabilidades para aplicaciones web y sistemas.
* **Función en PlatSentinel:** Analizan páginas web y recursos cloud en busca de vulnerabilidades, generando informes para la mitigación de riesgos[4](https://www.tokioschool.com/noticias/herramientas-ciberseguridad/)[5](https://www.guru99.com/es/vulnerability-scanning-tools.html)[6](https://www.revistacloudcomputing.com/2024/02/4-herramientas-gratuitas-para-el-analisis-de-vulnerabilidades/).

**7. API de WhatsApp Business (Twilio o Meta Cloud API)**

* **Función general:** Permite la integración de WhatsApp con sistemas externos para enviar y recibir mensajes automatizados.
* **Función en PlatSentinel:** Facilita la comunicación directa con usuarios y técnicos, permitiendo alertas, gestión remota y activación de servicios a través de WhatsApp[7](https://es.chatarchitect.com/news/official-whatsapp-api-improve-data-security-in-customer-communications)[8](https://getitsms.com/es/blogs/whatsapp-business-api-for-cybersecurity-services/)[9](https://itsit.es/la-seguridad-en-whatsapp-business-proteccion-avanzada-para-la-comunicacion-empresarial/).

**8. React.js o Vue.js**

* **Función general:** Frameworks para construir interfaces web interactivas y modernas.
* **Función en PlatSentinel:** Implementan el dashboard web donde se visualizan resultados, se gestionan tokens y se configuran servicios.

**9. D3.js / Sigma.js**

* **Función general:** Bibliotecas de visualización de datos.
* **Función en PlatSentinel:** Permiten mostrar gráficas, mapas de servicios gestionados y visualizaciones dinámicas de vulnerabilidades y estado del sistema.

**10. PostgreSQL o Redis**

* **Función general:** Sistemas de gestión de bases de datos relacionales (PostgreSQL) o en memoria (Redis).
* **Función en PlatSentinel:** Almacenan resultados de análisis, logs, usuarios y configuraciones del sistema.

**11. Terraform**

* **Función general:** Infraestructura como código para aprovisionar y gestionar recursos cloud.
* **Función en PlatSentinel:** Automatiza el despliegue de la infraestructura (servidores, redes, almacenamiento) en AWS u otros proveedores cloud.

**12. GitHub Actions**

* **Función general:** Plataforma de CI/CD para automatizar pruebas, builds y despliegues.
* **Función en PlatSentinel:** Automatiza el ciclo de vida del desarrollo, asegurando calidad y despliegues consistentes.

**13. Herramientas de Seguridad y Monitoreo**

* **Ejemplos:** Suricata (IPS), Prometheus (monitorización), Grafana (visualización de métricas), Trivy (escaneo de vulnerabilidades en contenedores).
* **Función en PlatSentinel:** Refuerzan la seguridad, monitorizan el estado del sistema y detectan amenazas en tiempo real[4](https://www.tokioschool.com/noticias/herramientas-ciberseguridad/)[10](https://www.campusmvp.es/recursos/post/las-10-herramientas-mas-importantes-para-orquestacion-de-contenedores-docker.aspx).

**14. Vault (HashiCorp)**

* **Función general:** Gestión segura de secretos y credenciales.
* **Función en PlatSentinel:** Protege claves, tokens y contraseñas utilizadas por los distintos módulos y servicios.

**15. Ory Hydra (OIDC)**

* **Función general:** Servidor de autenticación y autorización basado en OpenID Connect.
* **Función en PlatSentinel:** Gestiona el acceso seguro de usuarios al dashboard y a la API central.

**Tabla Resumen**

| **Herramienta** | **Función General** | **Función en PlatSentinel** |
| --- | --- | --- |
| Docker | Contenedores y despliegue | Ejecutar tokens y microservicios independientes |
| Docker Compose | Orquestación multicontenedor | Gestionar despliegue conjunto de todos los servicios |
| FastAPI | API web rápida y segura | Backend central del sistema |
| RabbitMQ | Mensajería asíncrona | Comunicación entre backend y tokens |
| ClamAV | Antivirus open source | Análisis de archivos en toquen de antesala |
| OWASP ZAP/OpenVAS/Nessus | Escaneo de vulnerabilidades | Análisis de web y cloud, generación de informes |
| API WhatsApp Business | Mensajería segura | Alertas y gestión remota vía WhatsApp |
| React.js / Vue.js | Frontend web | Dashboard para clientes y técnicos |
| D3.js / Sigma.js | Visualización de datos | Gráficas y mapas de servicios |
| PostgreSQL / Redis | Base de datos | Almacenamiento de resultados y configuraciones |
| Terraform | Infraestructura como código | Despliegue automatizado en la nube |
| GitHub Actions | CI/CD | Automatización de pruebas y despliegues |
| Suricata / Prometheus / Grafana | Seguridad y monitorización | Detección de intrusos y visualización de métricas |
| Vault | Gestión de secretos | Protección de credenciales y claves |
| Ory Hydra (OIDC) | Autenticación/autorización | Acceso seguro al dashboard y API |

**Esta combinación de herramientas garantiza que PlatSentinel sea modular, seguro, escalable y fácil de mantener, cubriendo tanto las necesidades técnicas del desarrollo como la operación y la experiencia del usuario final.**

1. <https://www.hiberus.com/crecemos-contigo/docker-y-microservicios/>
2. <https://appmaster.io/es/blog/arquitectura-de-microservicios-docker>
3. <https://blog.hackmetrix.com/10-herramientas-de-seguridad-informatica-y-como-usarlas/>
4. <https://www.tokioschool.com/noticias/herramientas-ciberseguridad/>
5. <https://www.guru99.com/es/vulnerability-scanning-tools.html>
6. <https://www.revistacloudcomputing.com/2024/02/4-herramientas-gratuitas-para-el-analisis-de-vulnerabilidades/>
7. <https://es.chatarchitect.com/news/official-whatsapp-api-improve-data-security-in-customer-communications>
8. <https://getitsms.com/es/blogs/whatsapp-business-api-for-cybersecurity-services/>
9. <https://itsit.es/la-seguridad-en-whatsapp-business-proteccion-avanzada-para-la-comunicacion-empresarial/>
10. <https://www.campusmvp.es/recursos/post/las-10-herramientas-mas-importantes-para-orquestacion-de-contenedores-docker.aspx>
11. <https://www.deltaprotect.com/blog/herramientas-seguridad-informatica>
12. <https://www.ambit-iberia.com/blog/herramientas-y-tecnologias-seguridad-it>
13. <https://www.fortinet.com/lat/resources/cyberglossary/smb-cybersecurity-tools>
14. <https://www.genetec.com/es/blog/productos/optimiza-la-seguridad-y-las-operaciones-con-dashboards-personalizados>
15. <https://www.incibe.es/ciudadania/herramientas>
16. <https://xygeni.io/es/blog/top-vulnerability-scanning-tools/>
17. <https://choam.net/analitica/mejores-herramientas-para-crear-dashboards/>
18. <https://es.linkedin.com/pulse/herramientas-esenciales-de-software-para-la-seguridad-seijas-5yyoc>
19. <https://datascope.io/es/blog/las-mejores-herramientas-para-hacer-un-dashboard-en-2022/>
20. <https://www.captio.net/blog/herramientas-seguridad-informatica>