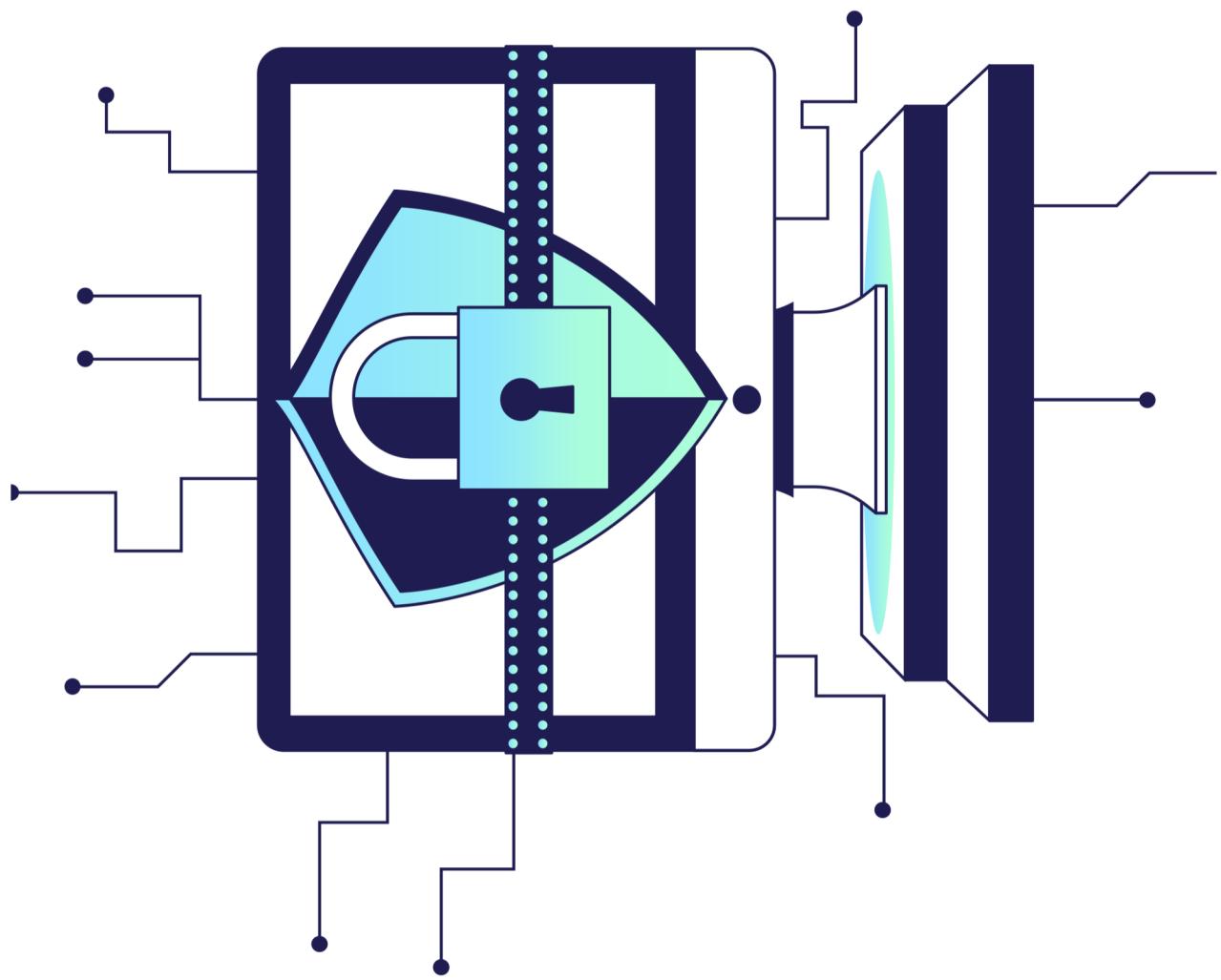


SEGURIDAD CON WAZUH

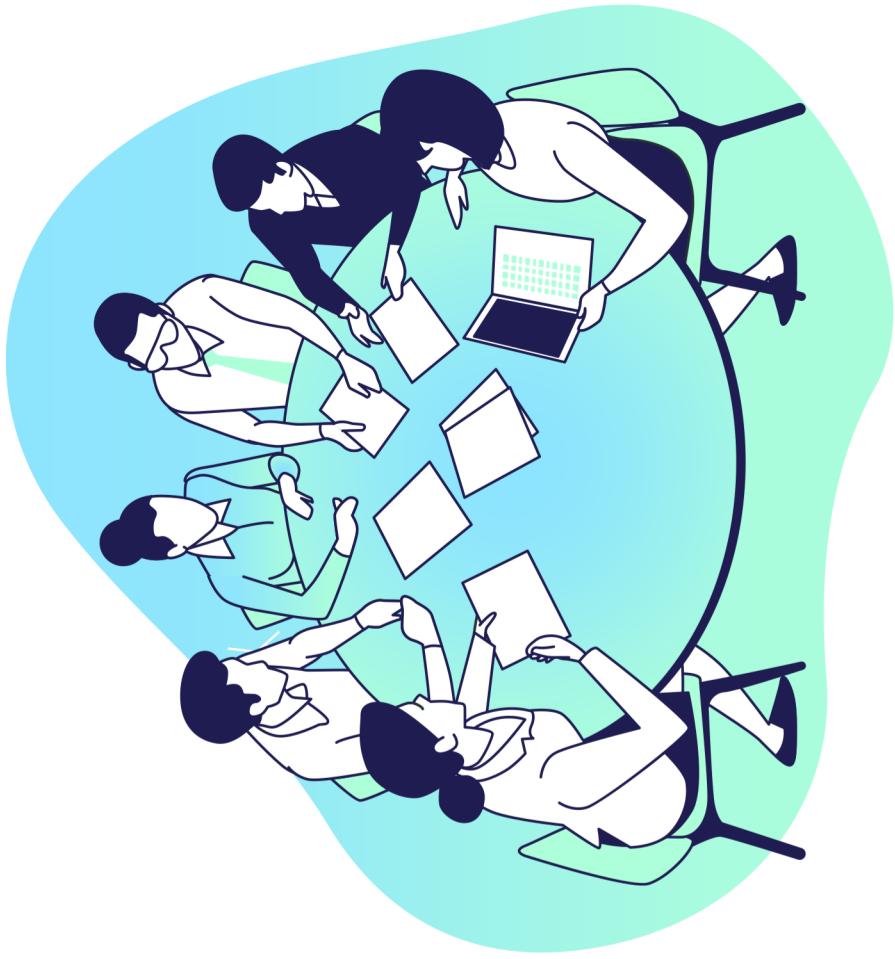
Jonathan Márquez Jiménez
IES Gonzalo Nazareno
Proyecto Fin de Ciclo



ÍNDICE

CONTENIDO

- ¿Qué es wazuh?
- Algunas capacidades de wazuh
- ¿Qué puede hacer el agente de wazuh?
- Kibana para wazuh
- Flujo de información
- Demo



QUE ES WAZUH?

Wazuh proporciona una solución de seguridad capaz de monitorear su infraestructura:

- Detectar amenazas
- Intentos de intrusión
- Anomalías del sistema
- Aplicaciones mal configuradas
- Acciones de usuarios no autorizados.

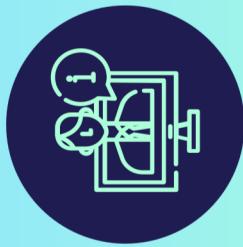


ALGUNAS CAPACIDADES DE WAZUH



Análisis de seguridad

Wazuh se utiliza para recopilar, agregar, indexar y analizar datos de seguridad



Detección de intrusiones

Wazuh escanea los datos recopilados para buscar malware, rootkits y anomalías sospechosas



Cumplimiento normativo

Wazuh proporciona algunos de los controles de seguridad necesarios para cumplir con los estándares

ALGUNAS CAPACIDADES DE WAZUH



Análisis de datos de registro

Los agentes de Wazuh leen los registros del SO y de las aplicaciones y los reenvían de forma segura al administrador



Supervisión de la integridad

Wazuh monitoriza el sistema de archivo, identificando cambios en el contenido, los permisos ...



Detección de vulnerabilidades

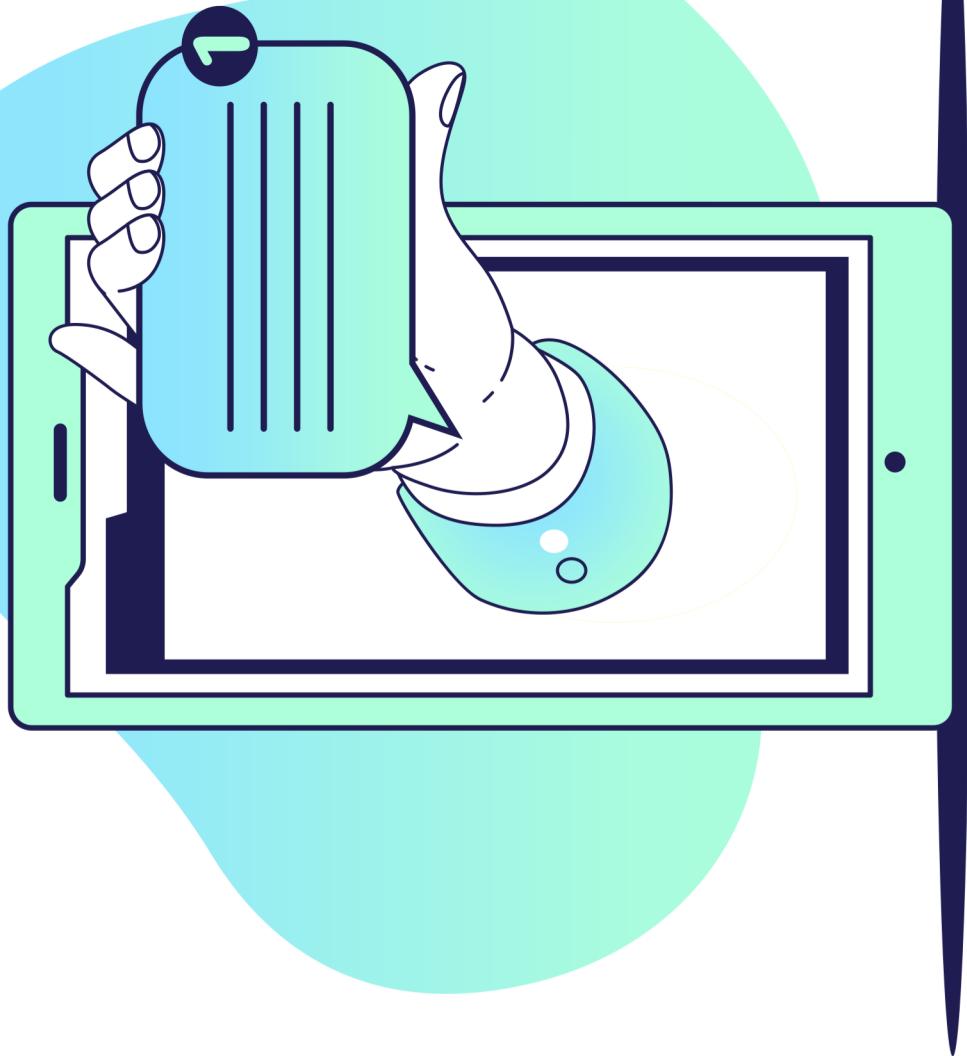
Los agentes de Wazuh extraen datos de software y envían esta información al servidor para correlacionar con la base de datos CVE

QUE PUEDEN HACER EL AGENTE DE WAZUH

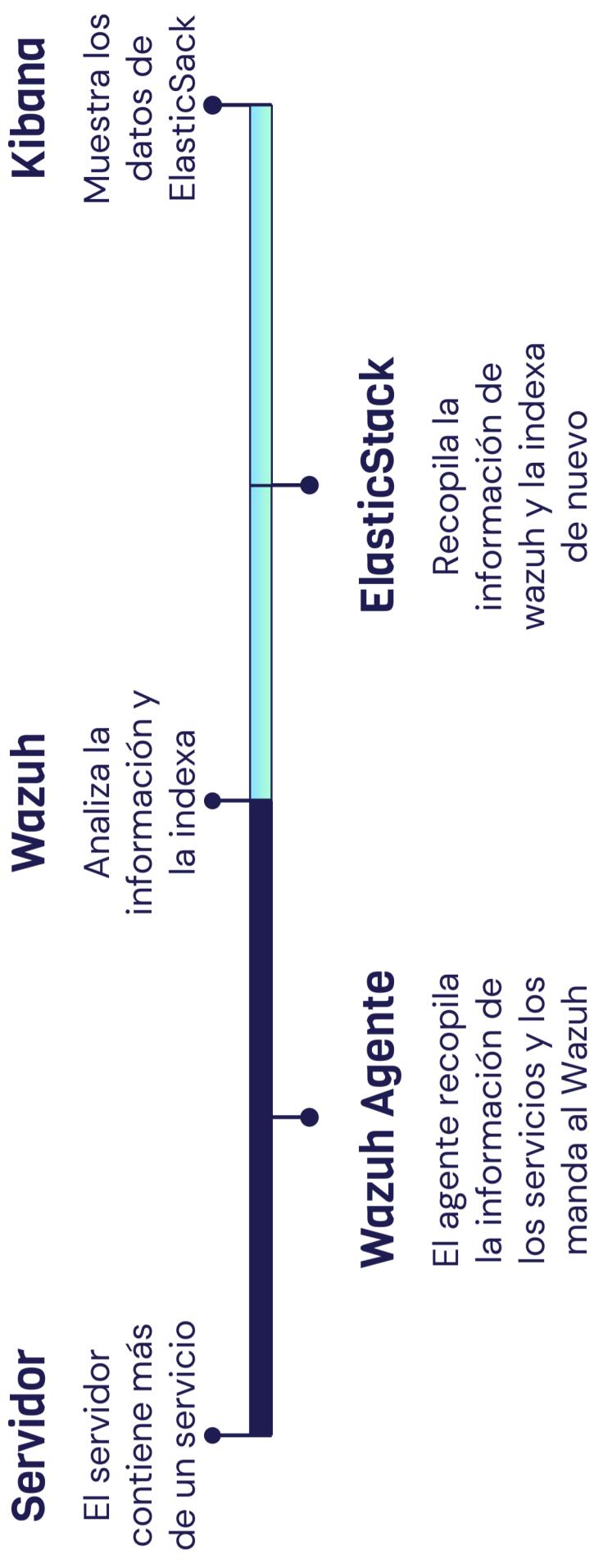


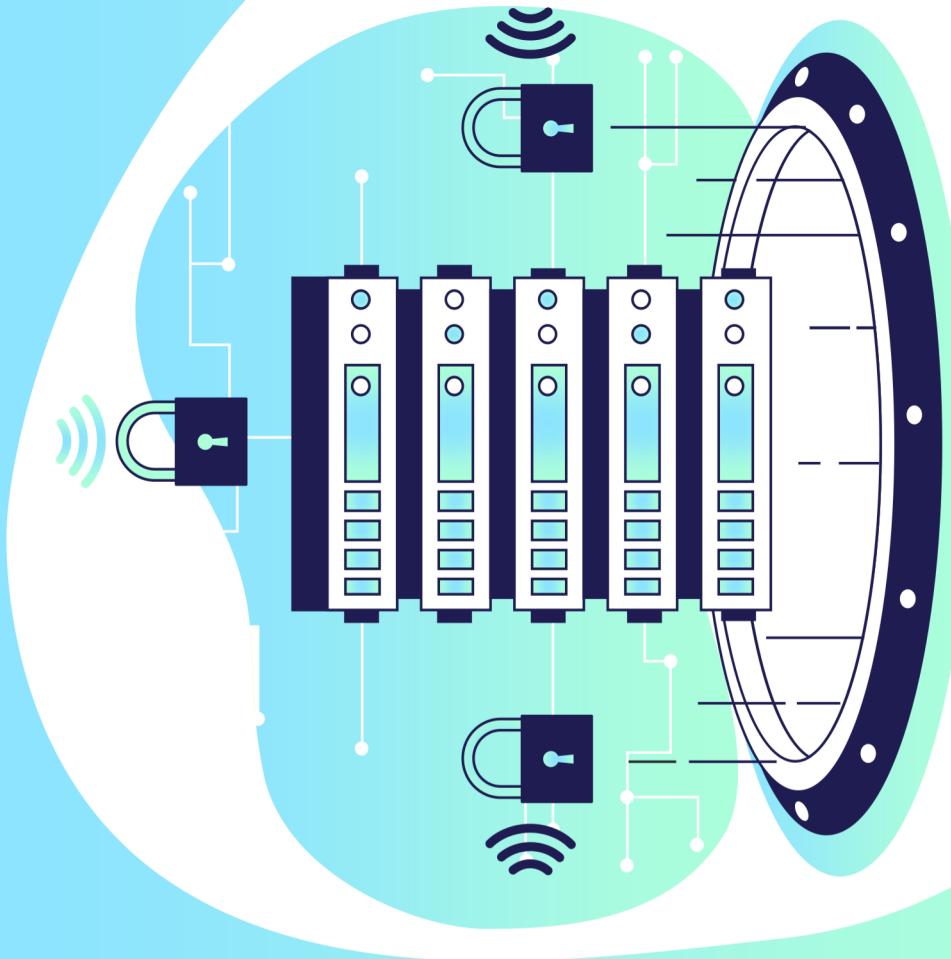
KIBANA

Gracias a kibana y a su API de wazu, podremos gestionar mucho mejor los datos recibidos de wazuh, nos da la posibilidad de crear alertas y tendremos un dashboard para una mejor visualización de los datos



FLUJO DE LA INFORMACIÓN





DEMO