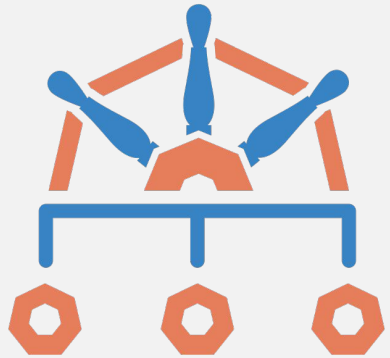
Plataforma de seguridad para kubernetes con Kyverno + Wazuh + Falco + Virustotal

Francisco Javier Doblado Alonso

INDICE

1. ¿QUE ES KYVERNOS?
2. ¿QUE ES WAZUH?
3. ¿QUE ES FALCO?
4. INFRAESTRUCTURA
5. ¿QUÉ GANAMOS JUNTÁNDOSE TODO?

¿QUE ES KYVERNOS?



- Es un motor de políticas para Kubernetes. Su función principal es **validar, modificar y generar configuraciones** de recursos de Kubernetes basándose en políticas de seguridad que definimos. En resumen, se asegura de que todo lo que se despliegue en el clúster cumpla con nuestras reglas de seguridad desde el principio. *Por ejemplo, podemos prohibir que se creen contenedores con privilegios de administrador.*

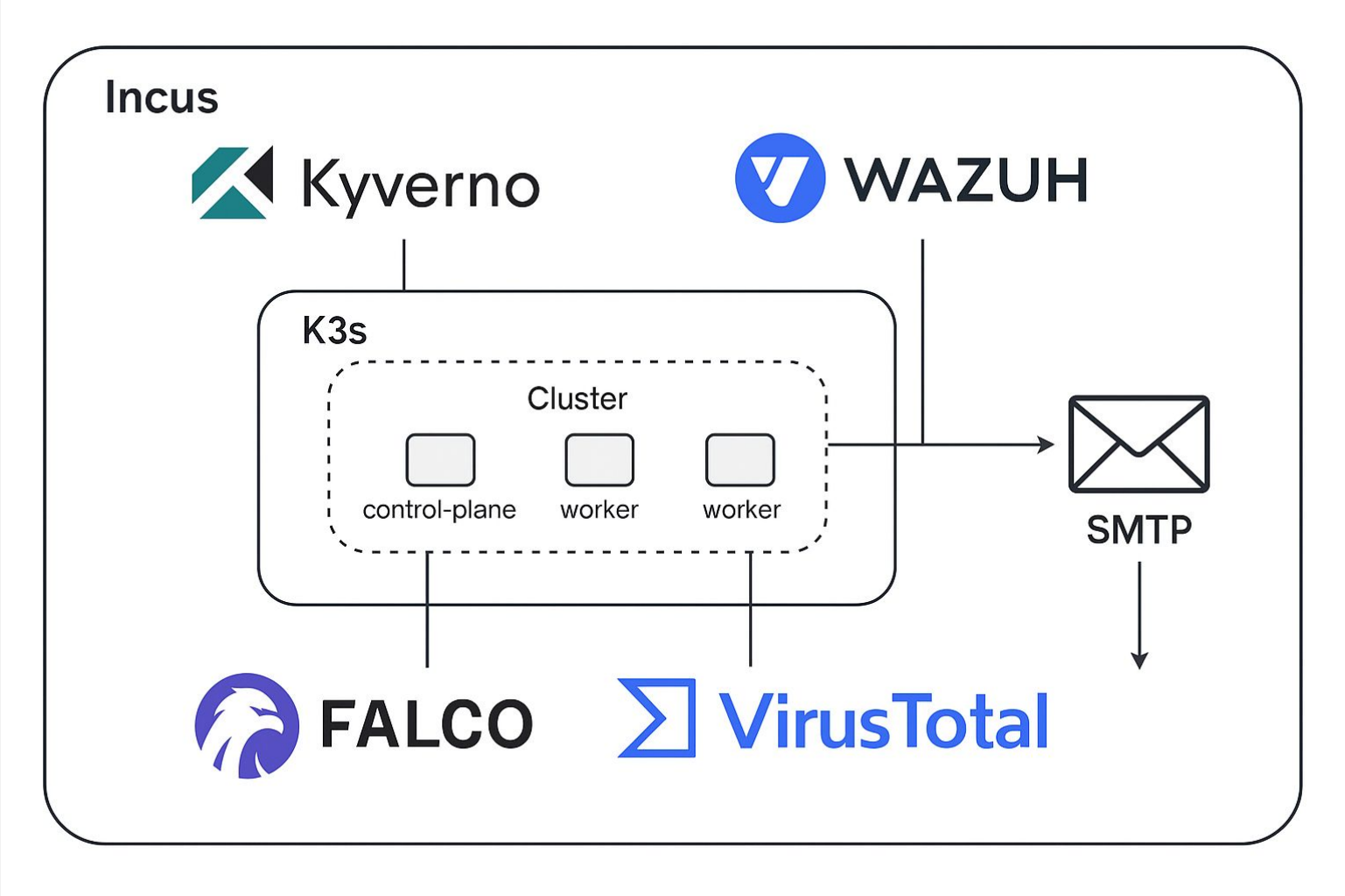
¿QUE ES WAZUH?

- Este actúa como nuestro centro de operaciones de seguridad. Es una plataforma de **SIEM** (Security Information and Event Management) y **XDR** (Extended Detection and Response). Recopila, analiza y correlaciona datos de seguridad de múltiples de diferentes bases de datos. En este proyecto, Wazuh centraliza todas las alertas generadas por las demás herramientas, permitiéndonos gestionar la seguridad desde un único punto.

¿QUE ES FALCO?

- Es una la herramienta de seguridad en tiempo de ejecución. Se engancha al kernel de Linux para **observar el comportamiento anómalo** de las aplicaciones dentro de los contenedores. Si un proceso hace algo inesperado o sospechoso (cómo escribir en un directorio sensible o abrir una conexión de red inusual), Falco lo detecta y lanza una alerta inmediata.

INFRAESTRUCTURA



¿QUÉ GANAMOS JUNTÁNDOSE TODO?

- **Seguridad Multicapa:** Protegemos antes con Kyverno (seguridad "shift-left"), durante con Falco y después con Wazuh de un ataque, creando una defensa completa en todas las fases.
- **Alertas Inteligentes:** En lugar de avisos aislados, generamos alertas enriquecidas que conectan la causa (configuración insegura), la acción (proceso anómalo) y la reputación del archivo (VirusTotal) para entender la amenaza al instante.
- **Control Centralizado:** Gestionamos toda la seguridad desde una única consola (Wazuh). Una sola vista para supervisar, investigar y responder a todo, sin cambiar de herramienta.

Gracias por su atención.