SIEM

Security Information and Event Management

Javier N. González

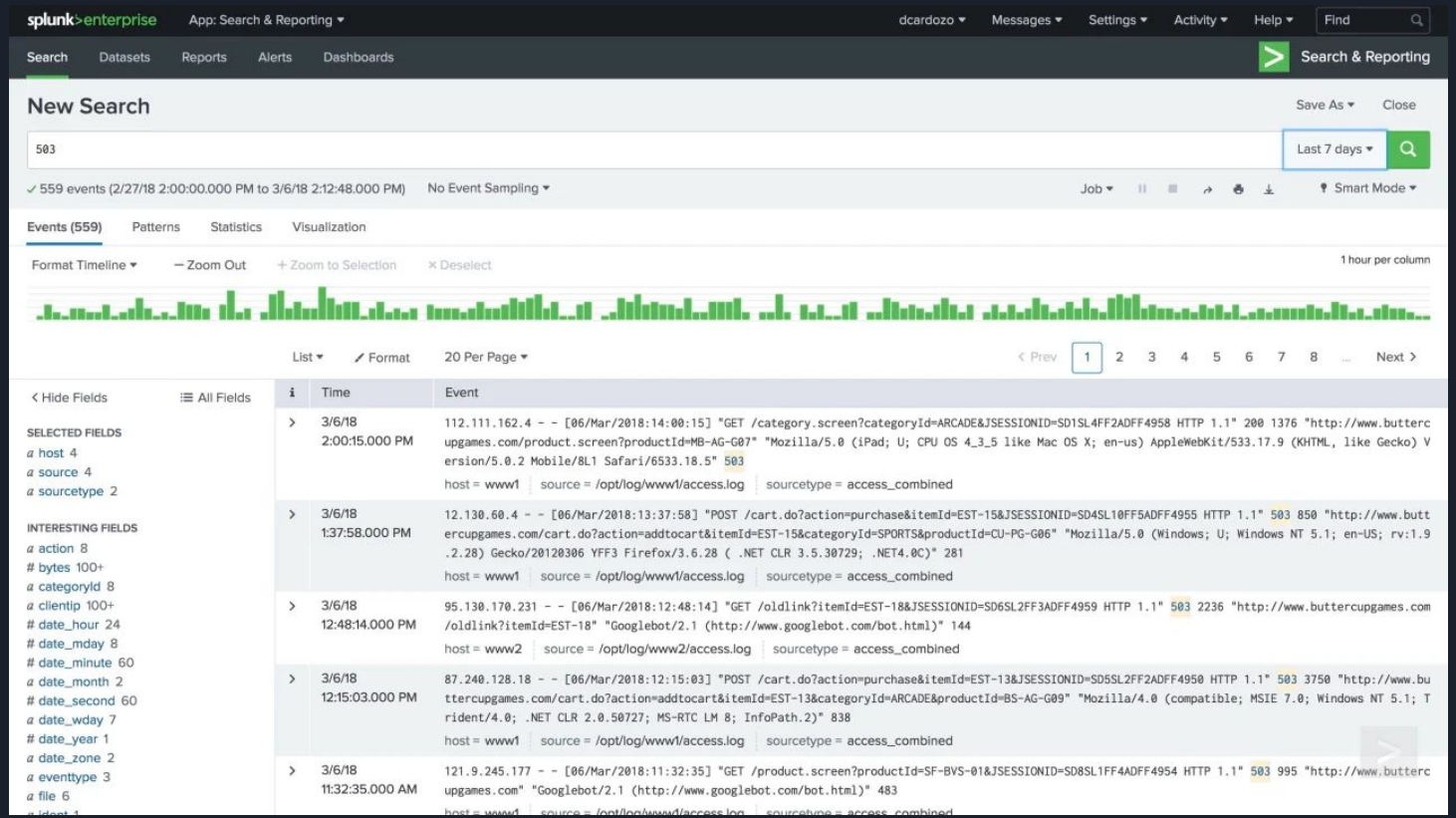
¿Qué es Splunk?

Es la herramienta SIEM (Security Information and Event Management) por excelencia para las empresas.

El Ciclo de Vida del Dato:

1. **Recolectar:** Obtener logs de endpoints, servidores y red.
2. **Normalizar:** Transformar datos crudos en pares `Campo = Valor`.
3. **Analizar:** Búsqueda y correlación.
4. **Alertar:** Notificar en base a reglas.

Así se ve Splunk



Arquitectura de Splunk

1. Forwarder (El Agente):

- Se instala en el Endpoint (Windows, Linux).
- Solo recolecta y envía logs (Sysmon, Apache, Event Viewer).

2. Indexer (El Cerebro):

- Recibe los datos del Forwarder.
- Procesa, normaliza y almacena la información en disco.

3. Search Head (La Interfaz):

- Donde el usuario realiza las consultas (SPL).
- Visualiza los datos procesados por el Indexer.

Análisis de Datos: SPL y Campos

SPL (Search Processing Language):

- Lenguaje propio para filtrar y operar con los datos.
- Uso de operadores lógicos (ej. `NOT France` para excluir tráfico).

Normalización automática:

- Splunk detecta formatos (ej. JSON) automáticamente.
- Crea "Campos Interesantes" en la barra lateral (User, Source_IP, Country).

Ejemplo real:

- Subir logs de VPN -> Filtrar por IP -> Identificar usuario sospechoso.

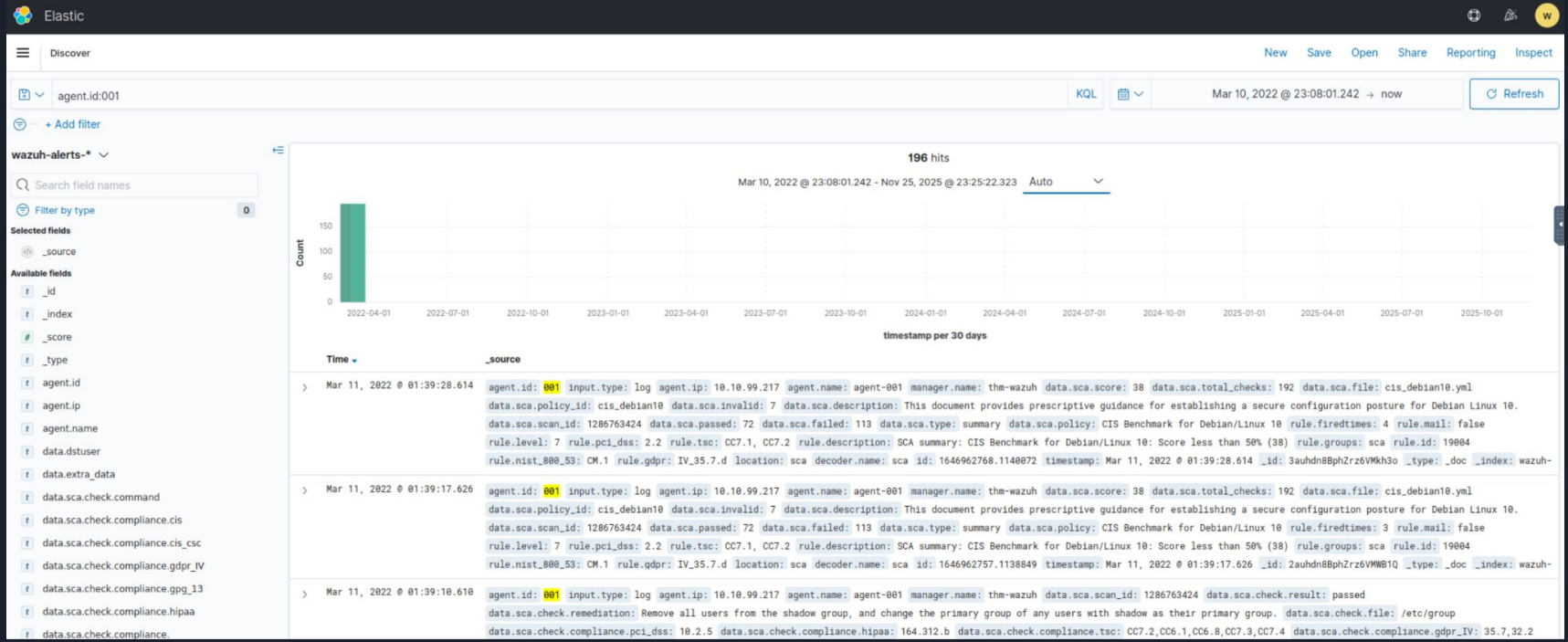
¿Qué es Wazuh?

Definición: Plataforma de seguridad Open Source que combina SIEM y protección de Endpoints (XDR).

Diferencia en el Ciclo:

- Incluye **Respuesta Activa** (Bloqueo automático de ataques).
- Enfoque en cumplimiento normativo predefinido.

Así se ve Wazuh



Arquitectura de Wazuh

1. Wazuh Agent (El Sensor):

- Más avanzado que un simple "Forwarder".
- Ejecuta escaneos de vulnerabilidades y FIM (Integridad de Ficheros) localmente.

2. Wazuh Server (El Analista):

- Decodifica los logs y los compara con miles de reglas predefinidas.
- Orquesta la Respuesta Activa.

3. Indexer & Dashboard:

- Basado en OpenSearch/Elasticsearch.
- Almacena y visualiza las alertas generadas.

Resumen

Características	Splunk	Wazuh
Ingesta de datos	Tolera todo tipo de dato (Logs, metricas, IoT).	Estructurada (Logs y eventos de seguridad).
Procesamiento	**Schema on Read:** Estructura el dato al buscarlo.	**Reglas y Decodificadores:** Analiza el dato al recibirlo.
Lenguaje	**SPL:** Muy flexible y potente para investigar.	**Reglas XML:** Más rígido, basado en matching.
Agente	Pasivo (Envío de logs).	Activo (Detección de vulnerabilidades, FIM).
Costo	Licencia por volumen (GB/día).	Gratuito, open source

¿Cúal es mejor?

Wazuh es mejor IDS/XDR. Splunk es mejor plataforma de Big Data Analytics. Son herramientas distintas que a menudo conviven.

Caso real: Trabajas en un SOC y tú cliente principal es un banco…
Imaginad que trabajáis en un banco.

- Si quieres saber si ha entrado un hacker en el servidor de nóminas -> **Wazuh**: gratis y al instante.
- Pero si el CISO te pide un gráfico cruzando *'Tiempos de respuesta del servidor'* con *'Dinero perdido en transacciones fallidas'* y *'Usuarios afectados por región'* en tiempo real... **Wazuh no puede hacer eso fácilmente.** Splunk lo hace en 5 minutos."

Cómo crear reglas en Wazuh

Wazuh no usa un lenguaje de búsqueda para crear reglas (como Splunk), usa **XML**.

Estructura básica:

- Definir un ID de regla (ej. 100001).
- Definir el nivel de alerta (0 a 15).
- Definir qué buscamos (ej. un string en el log).

El Flujo: Editar fichero `/var/ossec/etc/rules/local_rules.xml` -> Reiniciar servicio.

```
<rule id="100002" level="10">
  <if_sid>5716</if_sid>
  <match>refused</match>
  <description>Conexión rechazada detectada</description>
</rule>
```

Ejemplo realista de regla

Regla detecta: "Intento de fuerza bruta SSH desde IP 1.2.3.4".

Active Response dispara: `firewall-drop.sh`.

Resultado: La IP queda bloqueada en el firewall inmediatamente.

Si detecta un ataque, puede ejecutar un script que bloquee la IP en el firewall al instante. Pasa de la detección a la protección.

1. Una empresa de desarrollo tiene una aplicación 'legacy' hecha a medida que genera logs con un formato caótico y no estándar. El director quiere poder buscar en esos logs sin gastar horas de ingeniería en crear 'parsers' o decodificadores previos. ¿Qué herramienta es la más adecuada?

A. Wazuh, por su capacidad de normalización automática.

B. Ambas son igualmente efectivas para datos no estructurados.

C. Ninguna, se necesita una base de datos SQL.

D. Splunk, debido a su filosofía 'Schema on Read'.

1. Una empresa de desarrollo tiene una aplicación 'legacy' hecha a medida que genera logs con un formato caótico y no estándar. El director quiere poder buscar en esos logs sin gastar horas de ingeniería en crear 'parsers' o decodificadores previos. ¿Qué herramienta es la más adecuada?

D. Splunk, debido a su filosofía 'Schema on Read'.

✓ **¡Exacto!**

Splunk ingesta el dato crudo y permite estructurarlo en el momento de la búsqueda, ideal para logs 'sucios' o desconocidos.

2.Estás analizando una regla personalizada de Wazuh y te encuentras con la etiqueta `<if_sid>5716</if_sid>`. ¿Qué función cumple exactamente esta etiqueta dentro de la lógica de detección?

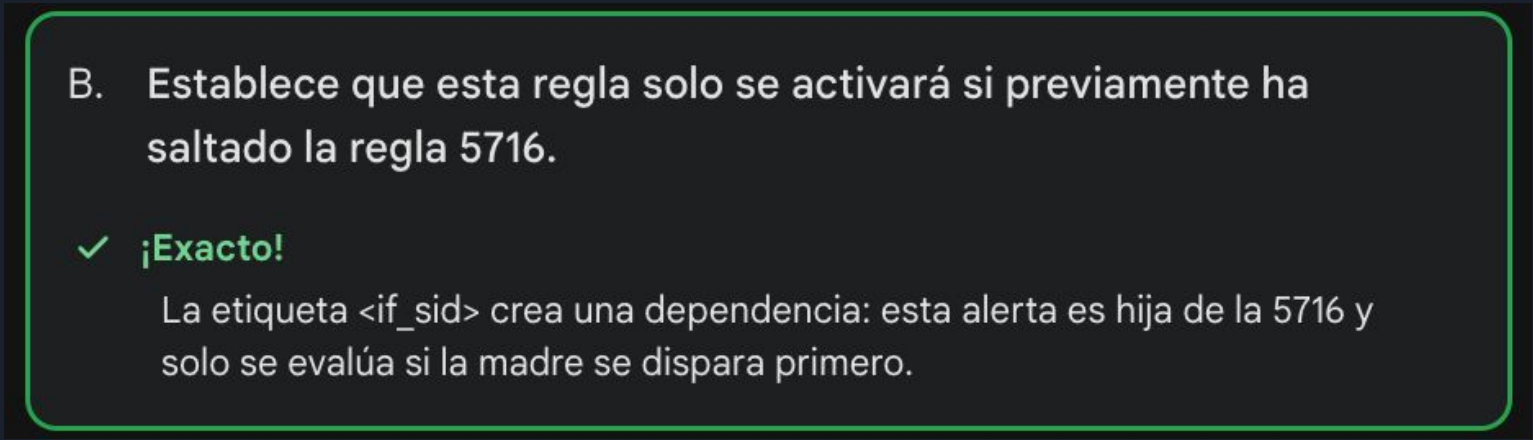
A. Asigna el nivel de gravedad 5716 a la alerta.

B. Establece que esta regla solo se activará si previamente ha saltado la regla 5716.

C. Define el ID único de la nueva regla que estamos creando.

D. Filtra los logs que contengan el texto '5716'.

2.Estás analizando una regla personalizada de Wazuh y te encuentras con la etiqueta `<if_sid>5716</if_sid>`. ¿Qué función cumple exactamente esta etiqueta dentro de la lógica de detección?

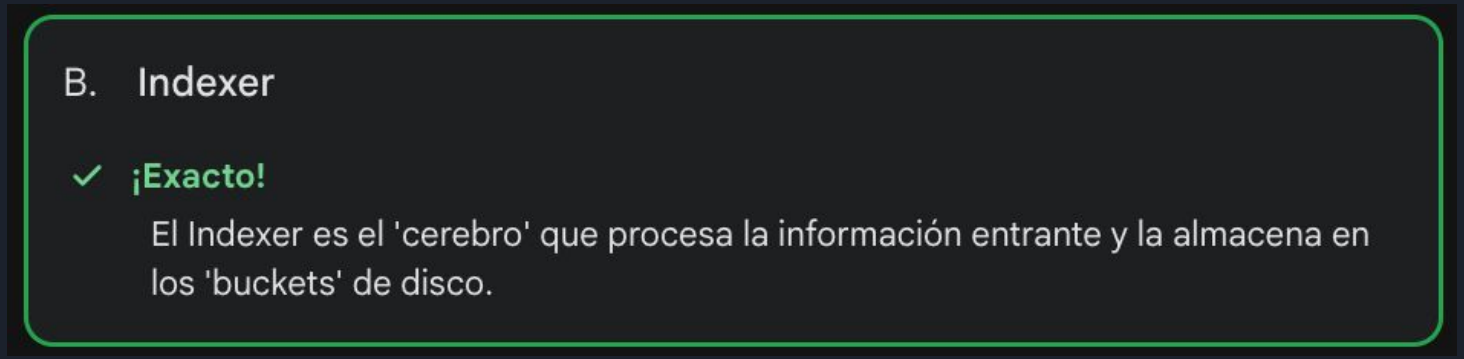


Es una regla de dependencia (Padre-Hijo). Significa que si el Signature ID (sid) 5716 ha saltado, entonces comprueba esta regla. Es vital para evitar falsos positivos.

3.En la arquitectura de Splunk, ¿qué componente es el encargado principal de recibir los datos, procesarlos, normalizarlos y escribirlos en el disco?

A. Universal Forwarder
B. Indexer
C. Deployment Server
D. Search Head

3.En la arquitectura de Splunk, ¿qué componente es el encargado principal de recibir los datos, procesarlos, normalizarlos y escribirlos en el disco?



4.Un administrador de sistemas intenta crear una regla personalizada en Wazuh editando un archivo en `/var/ossec/etc/rules/` dentro de un Agente (Agent-001). Al reiniciar, la regla no funciona. ¿Cuál es la causa más probable?

A. Ha olvidado la etiqueta `<group>` en el XML.

B. No ha usado el comando `logger` para probarla.

C. Los Agentes de Wazuh no procesan reglas localmente; las reglas deben estar en el Manager.

D. El nivel de la regla es demasiado bajo (menor a 3).

4.Un administrador de sistemas intenta crear una regla personalizada en Wazuh editando un archivo en `/var/ossec/etc/rules/` dentro de un Agente (Agent-001). Al reiniciar, la regla no funciona. ¿Cuál es la causa más probable?

C. Los Agentes de Wazuh no procesan reglas localmente; las reglas deben estar en el Manager.

✓ **Respuesta correcta**

Correcto. El Agente solo recolecta y envía. El cerebro que correlaciona y tiene las reglas es el Wazuh Manager.

5.Queremos configurar una respuesta automática (Active Response) en Wazuh para que bloquee una IP en el firewall cuando detecte un ataque de fuerza bruta. ¿Qué dos elementos son imprescindibles definir?

A. Un 'Command' (qué script ejecutar) y una 'Active Response' (cuándo ejecutarlo).

B. Una regla de Splunk y un script de Python.

C. El ID del evento de Windows y el nombre del usuario.

D. Un decodificador XML y un índice de OpenSearch.

5.Queremos configurar una respuesta automática (Active Response) en Wazuh para que bloquee una IP en el firewall cuando detecte un ataque de fuerza bruta. ¿Qué dos elementos son imprescindibles definir?

A. Un 'Command' (qué script ejecutar) y una 'Active Response' (cuándo ejecutarlo).

✓ **¡Exacto!**

Necesitas definir el comando (ej. firewall-drop) y la configuración de respuesta que lo vincula a una regla o nivel de alerta.

6.En Splunk, si ejecuto la búsqueda `index=main error | stats count by host`, ¿qué estoy solicitando exactamente?

A. Ver todos los logs del índice principal que contengan la palabra 'error', ordenados por fecha.

B. Borrar todos los eventos que contengan 'error' del host principal.

C. Crear una alerta si el contador de errores supera un umbral.

D. Una tabla estadística que muestra cuántos eventos contienen la palabra 'error' agrupados por cada máquina (host).

6.En Splunk, si ejecuto la búsqueda `index=main error | stats count by host`, ¿qué estoy solicitando exactamente?

D. Una tabla estadística que muestra cuántos eventos contienen la palabra 'error' agrupados por cada máquina (host).

✓ **¡Exacto!**

El comando 'stats count by host' transforma los eventos individuales en una tabla resumen numérica.

7.Al crear una regla personalizada en Wazuh para detectar una 'palabra mágica' en los logs, hemos usado un ID alto como `100005`. ¿Por qué no usamos un ID bajo como `100` o `500`?

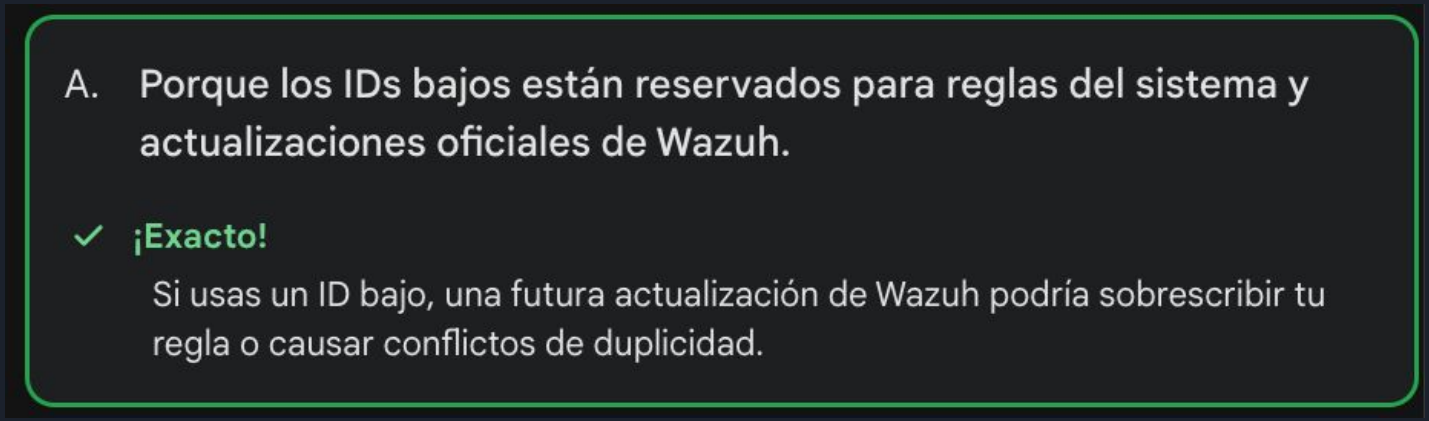
A. Porque los IDs bajos están reservados para reglas del sistema y actualizaciones oficiales de Wazuh.

B. Es una convención estética, técnicamente da igual.

C. Porque Wazuh solo acepta números de 6 dígitos.

D. Porque el ID debe coincidir con el PID del proceso Linux.

7.Al crear una regla personalizada en Wazuh para detectar una 'palabra mágica' en los logs, hemos usado un ID alto como `100005`. ¿Por qué no usamos un ID bajo como `100` o `500`?



Normalmente las reglas del 1 al 99.999 son territorio de Wazuh. Si usamos el ID 100, mañana Wazuh puede sacar una actualización que use el ID 100 y nuestra regla deja de funcionar.

8.Un analista de seguridad necesita investigar un incidente ocurrido hace 6 meses. Necesita realizar correlaciones complejas entre logs de acceso físico, logs de VPN y transacciones de base de datos. ¿Qué herramienta facilita más esta tarea de investigación histórica 'forense'?

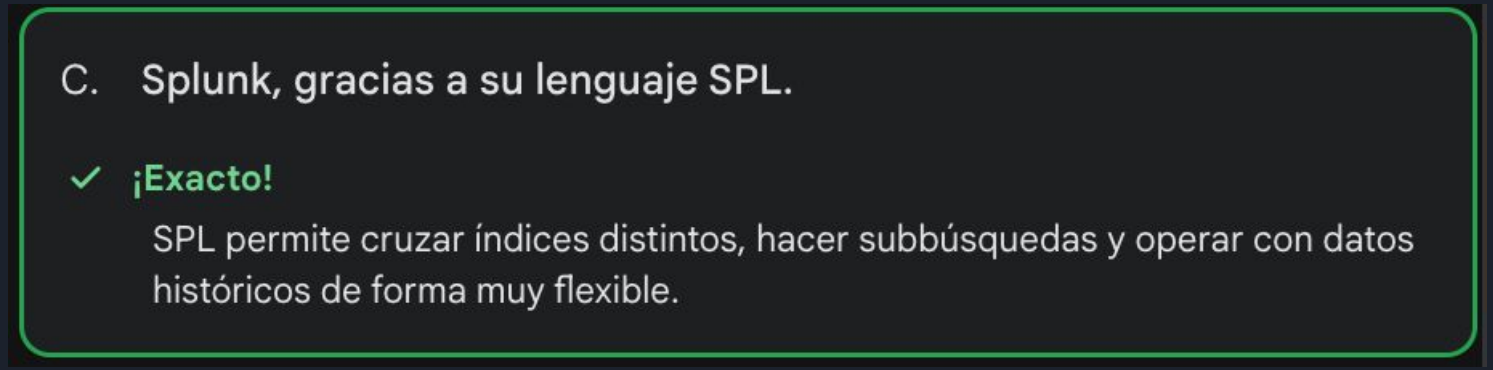
A. Wazuh, usando Active Response.

B. Ninguna, se necesitan logs en papel.

C. Splunk, gracias a su lenguaje SPL.

D. Wazuh, gracias a sus reglas XML.

8.Un analista de seguridad necesita investigar un incidente ocurrido hace 6 meses. Necesita realizar correlaciones complejas entre logs de acceso físico, logs de VPN y transacciones de base de datos. ¿Qué herramienta facilita más esta tarea de investigación histórica 'forense'?



9.Si en un archivo de reglas de Wazuh encuentras el error: `Invalid root element 'rule'. Only 'group' is allowed`, ¿qué falta en tu archivo XML?

A. El archivo debe llamarse obligatoriamente `ossec.conf`.

B. Falta definir el `<if_sid>`.

C. Falta la etiqueta de cierre `</rule>`.

D. Las reglas no pueden estar sueltas; deben estar envueltas en etiquetas `<group>` y `</group>`.

9.Si en un archivo de reglas de Wazuh encuentras el error: `Invalid root element 'rule'. Only 'group' is allowed`, ¿qué falta en tu archivo XML?

D. Las reglas no pueden estar sueltas; deben estar envueltas en etiquetas `<group>` y `</group>`.

✓ **¡Exacto!**

Wazuh exige que todas las reglas pertenezcan a un grupo lógico definido en la raíz del archivo.