Un SOAR (por sus siglas en inglés: Security Orchestration, Automation and Response) es una plataforma de ciberseguridad que permite a los equipos de seguridad gestionar amenazas y responder a incidentes de forma más eficiente mediante:

1. Orquestación (Orchestration): Integra diversas herramientas y sistemas de seguridad (firewalls, antivirus, SIEM, etc.) para que trabajen en conjunto desde un único panel de control.
2. Automatización (Automation): Ejecuta tareas repetitivas y procesos definidos automáticamente, como bloquear una IP sospechosa o generar tickets de incidentes.
3. Respuesta (Response): Ayuda a gestionar y ejecutar respuestas ante incidentes con procedimientos estandarizados, conocidos como *playbooks*.

Implementar una plataforma SOAR (Security Orchestration, Automation and Response) en una empresa ofrece una serie de ventajas clave que pueden transformar significativamente la forma en que se gestionan la seguridad y la respuesta ante incidentes. A continuación, se detallan sus principales beneficios:

## 1. Mejora de la eficiencia operativa

Una de las principales ventajas del SOAR es su capacidad para automatizar tareas repetitivas y manuales, como:

- Clasificar alertas de seguridad.
- Correlacionar datos de amenazas.
- Generar tickets y notificaciones.
- Realizar bloqueos de IPs o usuarios automáticamente.

Esto libera a los analistas de seguridad de cargas operativas innecesarias, permitiéndoles concentrarse en actividades más críticas y complejas. Además, al reducir la intervención humana, se disminuyen los errores operativos.

## ⚡ 2. Respuesta más rápida ante incidentes

Con SOAR, las respuestas ante amenazas pueden ejecutarse en segundos en lugar de horas. Esto es crucial, ya que el tiempo de respuesta es un factor determinante para minimizar el impacto de un ataque. Por ejemplo:

- Un playbook puede detectar automáticamente un comportamiento sospechoso en un endpoint y aislarlo de la red sin intervención humana.
- Se pueden ejecutar análisis de malware automatizados y compartir los resultados con otras herramientas.

## □ Estándar en la gestión de incidentes

SOAR permite crear y aplicar playbooks (guiones de respuesta) que aseguran que todos los incidentes se gestionen de forma consistente, siguiendo las mejores prácticas. Esto es esencial para:

- Asegurar el cumplimiento de normativas (como ISO 27001, GDPR, etc.).
- Facilitar auditorías y generación de reportes detallados.
- Reducir la dependencia del conocimiento individual de los analistas.

## □ Integración de herramientas de seguridad

Un SOAR puede conectarse con múltiples herramientas y sistemas de seguridad existentes, como:

- Firewalls, antivirus, EDR, SIEMs, sistemas de ticketing, etc.

Esto crea un ecosistema centralizado donde todas las herramientas trabajan de manera coordinada, lo que mejora la visibilidad y la capacidad de reacción.

## Mejora continua mediante inteligencia de amenazas

Muchos SOAR permiten integrarse con fuentes de Threat Intelligence, lo que permite:

- Enriquecer automáticamente las alertas con información contextual (por ejemplo, si una IP ya es conocida por actividades maliciosas).
- Tomar decisiones automatizadas basadas en inteligencia actualizada.

## Escalabilidad del equipo de seguridad

Al automatizar procesos y estandarizar la respuesta, las empresas pueden escalar sus capacidades de ciberseguridad sin necesidad de aumentar proporcionalmente el número de analistas. Esto es especialmente valioso para organizaciones con recursos limitados o en crecimiento.

## Reducción de la fatiga por alertas (alert fatigue)

Al filtrar, correlacionar y clasificar las alertas antes de presentarlas al equipo, un SOAR reduce significativamente la sobrecarga de información, permitiendo que los analistas se enfoquen en los incidentes más relevantes.

## Resumen de ventajas

| Ventaja | Beneficio concreto |
|---|---|
| Automatización de tareas | Ahorro de tiempo y reducción de errores |
| Respuesta rápida | Menor impacto ante ataques |
| Estandarización con playbooks | Procesos más predecibles y auditables |
| Integración de herramientas | Mayor coordinación y eficiencia |
| Inteligencia de amenazas integrada | Respuesta más informada y proactiva |
| Escalabilidad del equipo | Más capacidad sin más personal |
| Reducción de alert fatigue | Mayor concentración en incidentes prioritarios |

Implementar un SOAR es una inversión estratégica en ciberseguridad que no solo mejora la protección, sino que también permite a las empresas responder con agilidad, coherencia y eficacia frente a amenazas cada vez más sofisticadas.

# ¿Cuál es la diferencia entre un SOAR y un SIEM?

La diferencia entre un SOAR y un SIEM radica en su propósito principal y la forma en que gestionan la información de seguridad. Aunque pueden integrarse y trabajar juntos, cada uno cumple funciones distintas dentro del ecosistema de ciberseguridad:

## 1. Objetivo principal

| Plataforma | Objetivo principal |
|---|---|
| SIEM | Recopilar, correlacionar y centralizar logs y eventos de seguridad para detectar amenazas. |
| SOAR | Orquestar, automatizar y responder ante incidentes de seguridad de forma eficiente. |

## 2. Funcionalidades clave

| Función | SIEM | SOAR |
|---|---|---|
| Recolección de logs | Sí | No (aunque puede consultarlos) |
| Correlación de eventos | Sí | Depende del SIEM o fuente externa |
| Alertas de seguridad | Genera y clasifica | Actúa sobre ellas |
| Automatización de tareas | Limitada o inexistente | Sí, con playbooks automatizados |
| Orquestación de herramientas | No o muy limitada | Integra múltiples sistemas de seguridad |
| Respuesta a incidentes | Manual (o requiere integración extra) | Automática o semiautomática |

## ⚙ 3. ¿Cómo trabajan juntos?

- El SIEM detecta.
    - Por ejemplo, una correlación de eventos indica que una cuenta fue comprometida.
- El SOAR responde.
    - Detecta esa alerta desde el SIEM y lanza un *playbook* que puede:
        - Bloquear al usuario comprometido.
        - Notificar al equipo.
        - Abrir un ticket en el sistema de IT.
        - Iniciar un análisis forense automáticamente.

## 4. ¿Cuál necesitas?

| Necesitas… | Entonces usa… |
|---|---|
| Visibilidad centralizada de logs y eventos | SIEM |
| Reglas de correlación para detectar amenazas | SIEM |
| Automatizar respuestas a alertas | SOAR |
| Integrar herramientas y ejecutar playbooks | SOAR |
| Todo lo anterior | Ambos |

- El SIEM es como un centro de monitoreo: reúne datos, detecta anomalías y genera alertas.
- El SOAR es como un sistema de respuesta automatizado: recibe esas alertas y toma decisiones (según reglas o IA) para actuar de forma inmediata y coordinada.