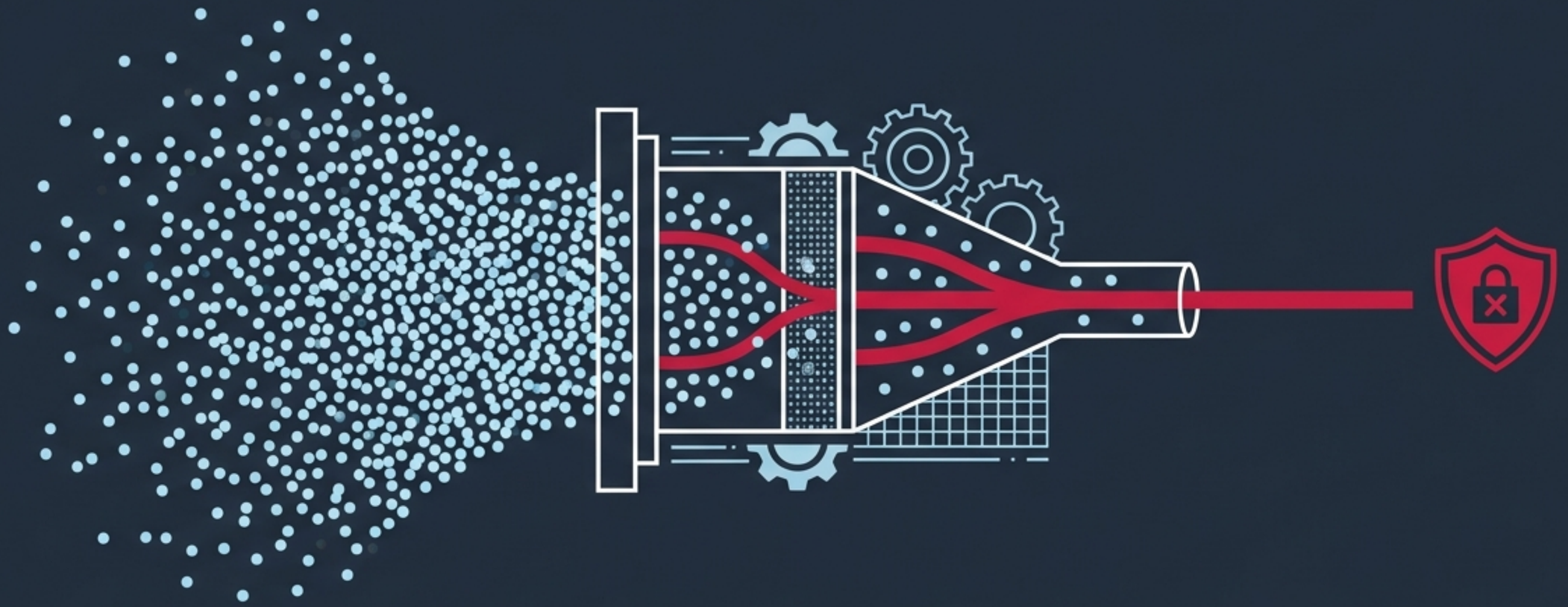
Conceptos Operativos Esenciales

El lenguaje base para analistas SOC: del ruido a la claridad.



El objetivo no es memorizar, es operar.

MISSION BRIEFING

Objetivo del módulo

Dar al alumno un lenguaje operativo preciso para distinguir evento, log, alerta e incidente, y comprender el flujo básico de respuesta de un entorno defensivo.

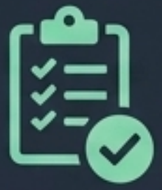
MISSION BRIEFING

Criterio pedagógico

Este módulo no busca memorizar definiciones aisladas. Busca que el alumno aprenda a clasificar correctamente lo que observa, priorizar con sentido y documentar sin confundir conceptos.

El Problema

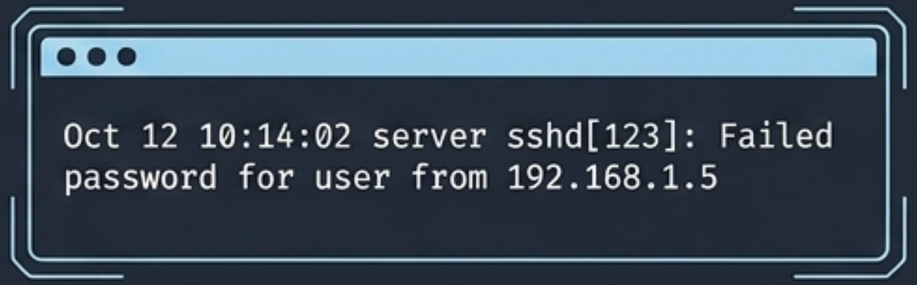
Un analista sin una base léxica clara mira datos, pero no sabe priorizarlos ni documentarlos.



La Solución

Adquirir un lenguaje operativo preciso para distinguir eventos, alertas e incidentes.

La Fundación: Eventos y Logs



Evento (La Acción)

Cualquier cambio o acción observable.
Es la unidad mínima de análisis.

Ejemplo: Un inicio de sesión fallido.

Log (El Registro)

La evidencia técnica escrita de ese evento.
Responde al qué, cuándo, dónde y quién.

Sin logs no hay trazabilidad. El SOC investiga evidencias, no suposiciones.

La Señal: ¿Cuándo prestamos atención?

¿Qué es una alerta?

Una notificación generada porque una regla considera que uno o varios eventos merecen revisión.

Concepto Clave

Una alerta NO es un ataque confirmado. Es un punto de partida, una señal accionable para el analista.

Ejemplo

1 fallo de autenticación = Evento.
10 fallos desde la misma IP en 2 minutos = Alerta (Fuerza bruta).

El Incidente: De la sospecha a la confirmación

¿Qué es un incidente?

Una situación con afectación real (o muy probable) a la confidencialidad, integridad o disponibilidad que exige gestión formal.

Regla de Oro

Llamar incidente a todo genera caos; no llamarlo cuando lo es retrasa la respuesta.

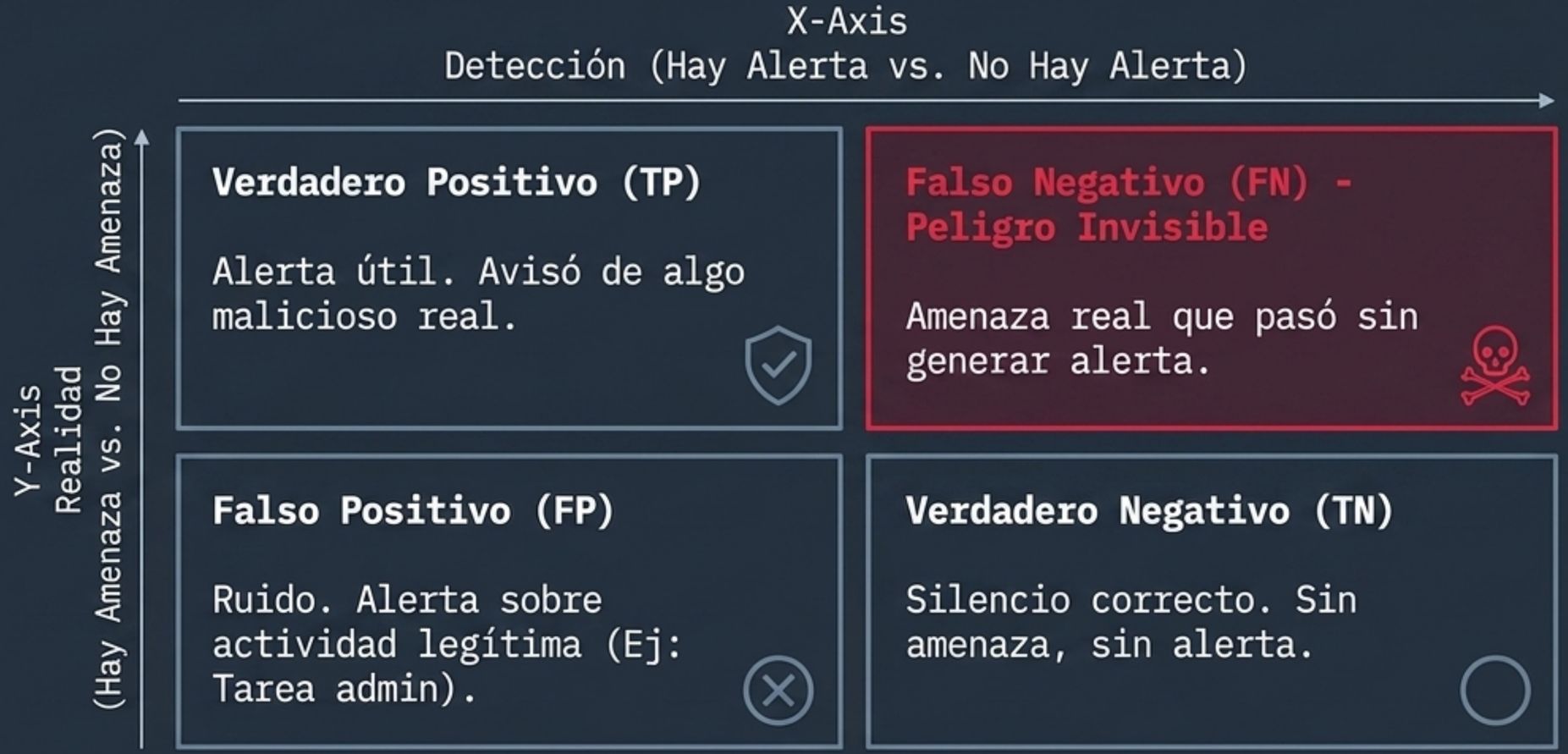
Ejemplo

Acceso no autorizado confirmado con uso de credenciales válidas.

Matriz de Jerarquía Operativa

Término	Naturaleza	Rol en el SOC	Ejemplo
Evento	Acción observada	Unidad mínima	Usuario intenta login
Log	Registro técnico	Evidencia base	Línea en /var/log/auth.log
Alerta	Señal accionable	Foco de revisión inicial	Regla detecta 10 fallos
Incidente	Problema confirmado	Detona respuesta formal	Brecha de datos confirmada

Evaluando la Detección: La Matriz de Calidad



El ‘Tuning’ busca reducir FP sin crear FN (que dan falsa sensación de seguridad).

Triage: El Primer Filtro Humano

Misión

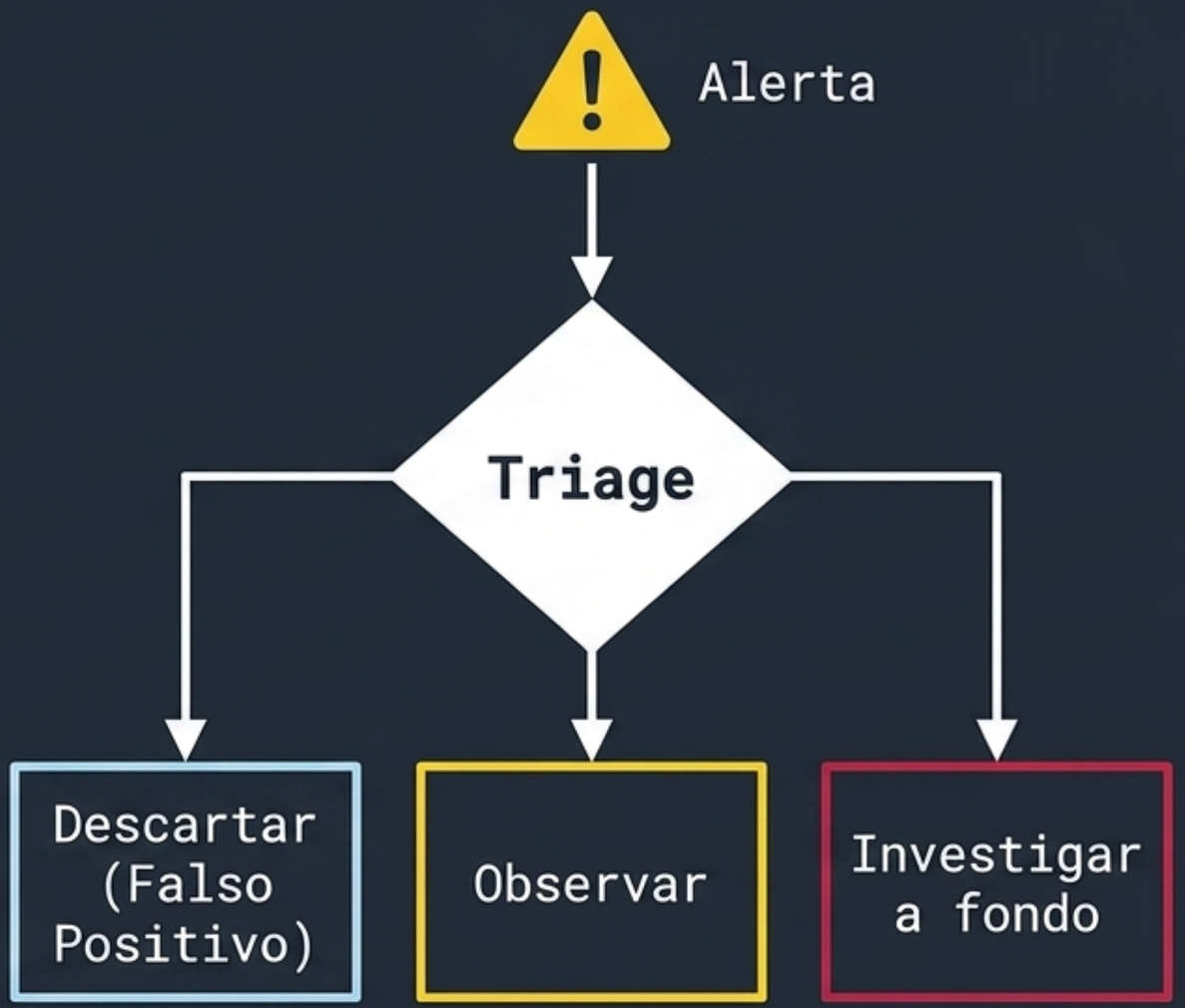
Valoración inicial para decidir la relevancia, prioridad y el siguiente paso de una alerta.

No es

Una investigación completa ni un cierre rápido ciego.

Qué miramos

Hora, IP origen, activo afectado, criticidad, historial.



El analista N1 es el maestro del Triage. Protege el tiempo del SOC filtrando con criterio.

Investigación: Construyendo el Contexto

Misión
Transformar una señal en entendimiento operativo mediante evidencias (logs en el SIEM).

El Proceso
Ampliar contexto, contrastar hipótesis, buscar la causa.

Preguntas a responder
¿Qué pasó? ¿Cuándo? ¿Cómo? ¿A quién afectó? ¿Cuál es el alcance?

Error Común
Buscar solo confirmar la primera hipótesis o cerrar por falta de tiempo.

Mitigación: Torniquete vs. Cura

Contención (Frenar)

- Limitar la expansión del daño temporalmente.
- Gana tiempo.
- Ejemplo: Aislar un host de la red, bloquear una IP.

Erradicación (Eliminar)

- Retirar la causa raíz y la persistencia.
- Resuelve el problema.
- Ejemplo: Borrar el malware, cambiar credenciales.

Takeaway: Contener sin erradicar solo aplaza el problema.

Recuperación: Regreso Seguro a la Normalidad

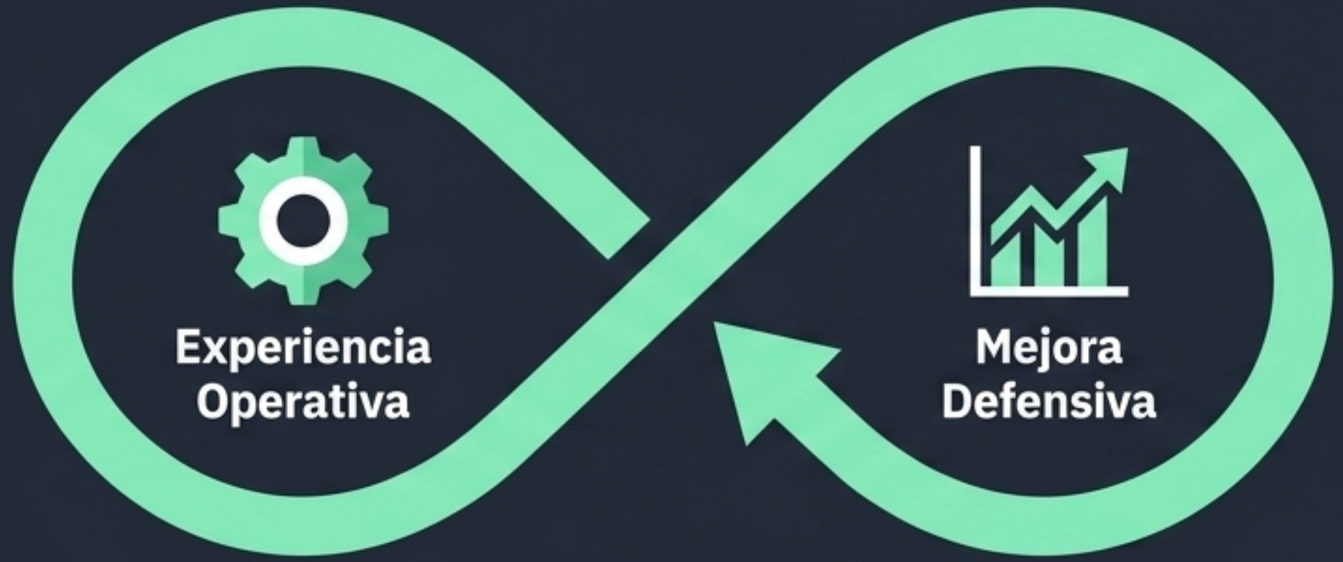
Concepto
Restaurar sistemas o servicios bajo vigilancia reforzada.

Requisito Vital
Garantías razonables de que el problema técnico y la causa han sido controlados.

Acciones
Validar accesos, comprobar funcionamiento normal y monitorizar si reaparecen indicadores en los logs.

⚠ **Error Común** Encender el servicio y olvidarse sin validación posterior.

Lecciones Aprendidas: El Motor de Madurez



Propósito

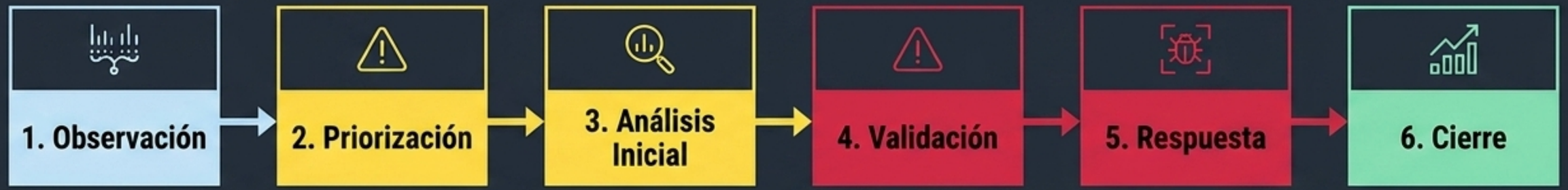
Entender qué falló y qué funcionó para no repetir errores. No es burocracia, es evolución.

Resultados Prácticos

Ajustar umbrales (Tuning), crear mejores reglas SIEM, documentar excepciones, mejorar procesos.

Un SOC estático pierde. Un SOC que convierte casos reales en cambios medibles mejora.

El Flujo Operativo del SOC (Ciclo de Vida)



(Eventos -> Logs)

(Regla SIEM -> Alerta)

(Triage)

(Investigación -> Incidente)

(Contención -> Erradicación)

(Recuperación -> Lecciones)

Ideas Clave para Recordar

Datos vs Señales: Eventos y Logs son observaciones; **Alertas** son peticiones de revisión; **Incidentes** son problemas confirmados.

El Silencio Engaña: Los **Falsos Negativos** son más peligrosos que los **Falsos Positivos** porque dan falsa seguridad.

Triage vs Investigación: El Triage filtra y orienta rápidamente; la **Investigación** profundiza y concluye con evidencias.

El Cierre Exige Aprendizaje: Un incidente termina cuando se erradica la causa y se ajustan las defensas (Lecciones aprendidas).