CHECKLIST DE VISIBILIDAD SIEM

25 preguntas para identificar qué eventos de seguridad podrías estar perdiendo

Una guía práctica para CIOs, CISOs, IT Managers y responsables de infraestructura que quieren revisar fuentes críticas, brechas de monitorización, casos de uso y hoja de ruta SIEM antes de avanzar con Wazuh.

Checklist visual | **No técnico** | **25 preguntas clave**

Por qué esta checklist importa

La mayoría de organizaciones ya dispone de herramientas de seguridad: firewalls, EDR, Microsoft Defender, servidores, cloud, aplicaciones críticas, soluciones de backup y sistemas de red. El reto aparece cuando cada fuente trabaja de forma aislada y los eventos no se convierten en información accionable.

El objetivo de esta checklist es ayudarte a preparar una conversación estratégica sobre SIEM: qué fuentes conviene centralizar, qué eventos deberían correlacionarse, qué alertas necesitan priorización y qué evidencias pueden apoyar investigación, respuesta y cumplimiento.

Incluido en el Security Visibility Assessment gratuito

Usa esta checklist como preparación para la sesión con NexTReT. No es una auditoría técnica cerrada ni una certificación; es una herramienta para ordenar prioridades, detectar posibles brechas de visibilidad y decidir con más criterio.

Importante

Este documento no sustituye una auditoría técnica. Es un self-assessment inicial para detectar posibles brechas y preparar una sesión de revisión con NexTReT.

CÓMO USARLA

- Responde cada pregunta con Sí, No o No lo sé.
- Marca prioridad Alta, Media o Baja cuando la pregunta revele un punto crítico.
- Anota ejemplos concretos: herramientas, fuentes, sistemas, dolores o incidentes previos.
- Lleva tus respuestas a la sesión para revisar posibles brechas y definir una hoja de ruta SIEM realista.

FICHA DE CONTEXTO INICIAL

Completa esta ficha antes de la sesión para situar el escenario de partida.

1. Empresa	
2. Persona / cargo	
3. Sector	
4. Número aproximado de empleados	
5. Infraestructura principal	On-premise / cloud / híbrida / multisede
6. Herramientas de seguridad actuales	Firewall, EDR, Microsoft Defender, SIEM, backup, monitorización, etc.
7. Principal prioridad	Detección / cumplimiento / centralización / reducción de ruido / respuesta / otro
8. Existe SIEM actualmente?	No / Wazuh / otra solución / no lo sé
9. Comentarios iniciales	

CHECKLIST DE VISIBILIDAD SIEM

BLOQUE 1 – FUENTES DE INFORMACIÓN

Identifica qué sistemas generan eventos relevantes y cuáles deberían formar parte de una visión centralizada de seguridad.

1. Tenéis identificadas las fuentes críticas que deberían enviar eventos al SIEM?

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas: _____

2. Están incluidos firewalls, VPN, servidores, endpoints, cloud, Directorio Activo y aplicaciones críticas?

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas: _____

3. Sabéis qué fuentes generan más eventos y cuáles generan señales realmente útiles?

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas: _____

4. Existen sistemas relevantes que hoy no estén integrados en ninguna plataforma centralizada?

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas: _____

5. Tenéis un criterio claro para priorizar qué fuentes integrar primero?

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas: _____

BLOQUE 2
CASOS DE USO Y CORRELACIÓN

Revisa si los eventos se interpretan de forma aislada
o si existen reglas para conectar señales y detectar patrones.

6. **Tenéis definidos los principales casos de uso que el SIEM debería detectar?**

☐ Sí ☐ No ☐ No lo sé | **Prioridad:** ☐ Alta ☐ Media ☐ Baja

Notas: _____

7. **Existen reglas para identificar accesos indebidos, cambios críticos o comportamientos anómalos?**

☐ Sí ☐ No ☐ No lo sé | **Prioridad:** ☐ Alta ☐ Media ☐ Baja

Notas: _____

8. **Las alertas se analizan de forma aislada o se correlacionan con otras señales?**

☐ Sí ☐ No ☐ No lo sé | **Prioridad:** ☐ Alta ☐ Media ☐ Baja

Notas: _____

9. **Hay eventos que hoy generan ruido pero poco valor operativo?**

☐ Sí ☐ No ☐ No lo sé | **Prioridad:** ☐ Alta ☐ Media ☐ Baja

Notas: _____

10. **Tenéis reglas diferenciadas por criticidad, tipo de activo o riesgo?**

☐ Sí ☐ No ☐ No lo sé | **Prioridad:** ☐ Alta ☐ Media ☐ Baja

Notas: _____

BLOQUE 3
ALERTAS, RESPUESTA Y OPERACIÓN

Evalúa si las alertas se convierten en acción,
con responsables, prioridades y ciclos de mejora.

11. **Quién revisa las alertas y con qué frecuencia?**

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas / Evidencias: _____

12. **Existe una clasificación clara de alertas críticas, altas, medias y bajas?**

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas / Evidencias: _____

13. **Hay responsables definidos para investigar y escalar incidentes?**

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas / Evidencias: _____

14. **Tenéis procedimientos básicos para actuar ante actividad sospechosa?**

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas / Evidencias: _____

15. **Existe seguimiento de alertas recurrentes, falsos positivos y reglas que necesitan ajuste?**

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas / Evidencias: _____

BLOQUE 4 - CUMPLIMIENTO Y EVIDENCIAS

Identifica si la información disponible ayuda a demostrar control, trazabilidad y capacidad de respuesta.

16. ¿Sabéis qué eventos pueden servir como evidencia para auditorías o marcos normativos?

☐ Sí ☐ No ☐ No lo sé | **Prioridad:** ☐ Alta ☐ Media ☐ Baja

Notas: .....

17. ¿Tenéis trazabilidad suficiente sobre accesos, cambios, actividad administrativa y eventos críticos?

☐ Sí ☐ No ☐ No lo sé | **Prioridad:** ☐ Alta ☐ Media ☐ Baja

Notas: .....

18. ¿Podéis generar informes ejecutivos o técnicos de forma recurrente?

☐ Sí ☐ No ☐ No lo sé | **Prioridad:** ☐ Alta ☐ Media ☐ Baja

Notas: .....

19. ¿La información está centralizada o depende de revisiones manuales en varias herramientas?

☐ Sí ☐ No ☐ No lo sé | **Prioridad:** ☐ Alta ☐ Media ☐ Baja

Notas: .....

20. ¿El modelo actual ayuda a demostrar control o solo a reaccionar ante incidencias?

☐ Sí ☐ No ☐ No lo sé | **Prioridad:** ☐ Alta ☐ Media ☐ Baja

Notas: .....

BLOQUE 5 - HOJA DE RUTA SIEM

Ordena el punto de partida para definir una implantación progresiva y operable.

21. Tenéis definido qué problema debe resolver primero el SIEM?

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas: _____

22. La prioridad es detección, cumplimiento, reducción de ruido, respuesta o centralización?

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas: _____

23. Tenéis claro qué fases debería seguir la implantación?

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas: _____

24. Sabéis qué recursos técnicos y operativos necesitaría el proyecto?

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas: _____

25. Tenéis un modelo para operar, mantener y optimizar el SIEM después del despliegue?

☐ Sí ☐ No ☐ No lo sé

Prioridad: ☐ Alta ☐ Media ☐ Baja

Notas: _____

CÓMO INTERPRETAR TUS RESPUESTAS

No buscamos una puntuación numérica. El objetivo es detectar patrones de riesgo, áreas sin suficiente visibilidad y prioridades para una hoja de ruta SIEM.

Si predominan los “No”

Probablemente existen brechas visibles de cobertura, correlación, respuesta o evidencia. Conviene priorizar fuentes críticas y casos de uso.

Si predominan los “No lo sé”

Existe incertidumbre operativa. Antes de implantar o evolucionar un SIEM, conviene mapear fuentes, responsables, eventos y criterios de prioridad.

Si predominan los “Sí”

Hay una base inicial de control. El siguiente paso suele ser optimizar reglas, reducir ruido, mejorar dashboards y formalizar operación.

PRIORIDADES PARA REVISAR CON NEXTRET

- Qué fuentes deberían integrarse primero y por qué.
- Qué casos de uso aportarían más valor en detección, respuesta o cumplimiento.
- Qué reglas o alertas podrían generar ruido si no se diseñan correctamente.
- Qué evidencias necesita la organización para auditorías, controles internos o marcos normativos.
- Qué fases tendría sentido seguir para implantar, evolucionar u operar un SIEM basado en Wazuh.

ANTES DE LA SESIÓN, TEN A MANO:

- Un listado aproximado de herramientas actuales: firewall, EDR, Microsoft Defender, cloud, servidores, aplicaciones y monitorización.
- Las fuentes que hoy ya generan eventos y aquellas que no están integradas.
- Los principales dolores: exceso de alertas, falta de contexto, cumplimiento, respuesta o visibilidad limitada.
- Cualquier objetivo prioritario: implantación SIEM, evolución de una solución existente, reducción de ruido o evidencias para auditoría.

SIGUIENTE PASO

Reserva tu Security Visibility Assessment gratuito y revisa tus respuestas con un especialista de NexTReT para obtener una primera orientación sobre fuentes, brechas y hoja de ruta SIEM.

La finalidad del Security Visibility Assessment es convertir esta checklist en una conversación práctica: qué revisar primero, qué fuentes priorizar y qué hoja de ruta SIEM tendría más sentido para tu organización.