, ¿cuánto tiempo tardarías en detectar una brecha de seguridad en tu infraestructura?

Como en su organización, probablemente has invertido en múltiples herramientas de seguridad. Pero hay una pregunta crítica: ¿tienes visibilidad continua de lo que realmente está pasando en tu entorno?

El costo oculto de la detección tardía

El tiempo promedio para detectar una brecha de seguridad es de **277 días** (IBM Security). Durante ese tiempo, los atacantes pueden moverse lateralmente, exfiltrar datos críticos y establecer persistencia. El costo promedio de una violación de datos: **USD $4.45 millones**.

La paradoja de las herramientas de seguridad

Más herramientas no equivalen a más seguridad. De hecho, el 67% de las organizaciones reportan "fatiga de alertas": reciben tantas notificaciones que es imposible distinguir las amenazas reales del ruido de fondo.

El resultado: eventos críticos pasan desapercibidos mientras tu equipo de TI se ahoga en falsos positivos. No es falta de tecnología. Es falta de capacidad de análisis continuo y correlación inteligente.

La verdadera seguridad no es tener más herramientas. Es tener visibilidad continua, análisis experto y capacidad de respuesta inmediata.

Las organizaciones con mayor madurez en ciberseguridad no son las que tienen más presupuesto. Son las que han implementado **monitoreo 24/7 con análisis experto y respuesta automatizada** para detectar y contener amenazas antes de que se conviertan en incidentes.

Señales de que necesitas visibilidad continua:

- Tu equipo de TI no tiene capacidad para monitorear eventos de seguridad 24/7
- Recibes alertas de seguridad pero no tienes claridad sobre su criticidad real
- No cuentas con un proceso definido de respuesta a incidentes
- Dependes de herramientas aisladas sin correlación entre eventos
- No tienes visibilidad de lo que pasa fuera del horario laboral

CyberSOC as a Service: Detección, protección y respuesta continuas

No es solo monitoreo. Es un equipo de analistas expertos trabajando para tu organización sin la necesidad de contratar personal interno.

Nuestro CyberSOC basado en la nube proporciona supervisión de eventos y gestión de incidentes las 24 horas del día desde nuestra red global de centros de operaciones. Utilizamos tecnologías líderes como **Elastic Security, SIEM y XDR** para correlacionar eventos, detectar amenazas y generar respuestas automatizadas.

Capacidades clave de nuestro CyberSOC

🔍 Monitorización Continua

Análisis 24/7 de eventos de seguridad en toda tu infraestructura: endpoints, servidores, cloud, red perimetral.

🎯 Detección de Amenazas

Correlación inteligente de eventos para identificar patrones de ataque y comportamientos anómalos en tiempo real.

⚡ Respuesta Activa

Contramedidas automatizadas para contener amenazas: bloqueo de IPs, aislamiento de endpoints, escalamiento a equipos.

🧠 Inteligencia de Amenazas

Integración con feeds globales de threat intelligence para anticipar vectores de ataque emergentes.

📊 Análisis Forense

Investigación profunda de incidentes para entender alcance, impacto y vectores de compromiso.

📋 Cumplimiento Normativo

Reportes y dashboards para demostrar cumplimiento con PCI DSS, GDPR, ISO 27001 y otros estándares.

Stack tecnológico de clase mundial

Elastic Security | Wazuh SIEM | XDR | SOAR | Threat Intelligence | EDR

Impacto medible en tu postura de seguridad:

- **Reducción de 85%** en tiempo de detección de amenazas
- **Contención en menos de 1 hora** para incidentes críticos
- **Visibilidad de 100%** de eventos de seguridad
- **Reducción de 60%** en falsos positivos
- **Ahorro de 70%** vs. construir un SOC interno

Esto no es un servicio de alertas. Es **un equipo de analistas de seguridad trabajando como extensión de tu organización**, con capacidad de respuesta inmediata y mejora continua basada en threat intelligence global.

”Detectamos y contuvimos un ransomware antes de que cifrara información crítica”

Caso real de respuesta a incidente en empresa de servicios financieros

DIRECTOR DE TI | EMPRESA DE SERVICIOS FINANCIEROS | 180 EMPLEADOS

Situación inicial:

"Teníamos antivirus en endpoints y firewall perimetral, pero sin capacidad de monitoreo continuo. Nuestro equipo de TI (3 personas) se enfocaba en operaciones diarias. Los fines de semana y horarios nocturnos eran puntos ciegos totales. Sabíamos que era un riesgo, pero contratar un equipo de seguridad 24/7 estaba fuera de nuestro presupuesto."

El incidente:

"Un viernes a las 22:30 hrs, el CyberSOC de THE detectó actividad anómala: un endpoint ejecutando comandos de reconocimiento de red y movimiento lateral. Las alertas llegaron inmediatamente al equipo de analistas, quienes identificaron el patrón como ransomware en fase inicial. En **menos de 45 minutos**, aislaron el endpoint comprometido, bloquearon las IPs de comando y control, y nos contactaron con el análisis completo."

Respuesta coordinada:

"El equipo de THE no solo detectó la amenaza. Nos guió en la respuesta: análisis forense del endpoint, verificación de backups, escaneo de toda la red para confirmar que no había otros sistemas comprometidos. El lunes en la mañana, teníamos un informe completo del incidente, recomendaciones de remediación y un plan de fortalecimiento."

Impacto evitado:

"Si ese ransomware hubiera cifrado nuestros sistemas, el costo estimado era de **USD $850,000** (rescate + tiempo de inactividad + pérdida de confianza de clientes + remediación). El CyberSOC de THE nos costó una fracción de eso y nos dio algo que no teníamos: **tranquilidad de que alguien está vigilando 24/7**."

Resultado medible:

"Desde la implementación del CyberSOC, hemos detectado y contenido **12 intentos de intrusión** en 8 meses. Ninguno llegó a convertirse en incidente. Nuestro board directivo ahora ve la ciberseguridad como una inversión estratégica, no como un gasto."

Su transformación no fue sobre comprar más herramientas. Fue sobre tener un equipo de expertos monitoreando, analizando y respondiendo en tiempo real.

Evaluación de madurez para su organización

Si reconoces que tu organización tiene puntos ciegos en monitoreo de seguridad o falta de capacidad de respuesta 24/7, ya estás listo para el siguiente paso.

Servicios complementarios

☁️ Seguridad Cloud	🔐 Identidades	🛡️ Seg. Aplicativa
🏭 Seguridad OT	🤖 Gobierno IA	📊 Consultoría

Qué incluye nuestra evaluación:

- **Mapeo de activos:** Sistemas prioritarios
- **Análisis de gaps:** Puntos ciegos actuales
- **Capacidad de respuesta:** Tiempo de detección
- **Roadmap:** Plan según presupuesto
- **Cumplimiento:** Brechas regulatorias

La realidad de la ciberseguridad

No se trata de si serás atacado, sino de cuándo. Tu capacidad de respuesta marcará la diferencia.

¿Listo para visibilidad continua?

Evaluación de 45 minutos sin costo donde analizamos tu postura actual.

Agendar Evaluación Gratuita

Sin compromiso. Basado en tu infraestructura real.