Seguridad gestionada

Guía para el comprador

Insight

Introducción

Todo el mundo, desde los directores generales y los miembros de los consejos de administración hasta cualquier persona en su vida privada, reconoce la importancia de la ciberseguridad. Es raro que transcurra un día sin que aparezca una noticia sobre una importante marca que ha sufrido una brecha de seguridad o sobre un incidente de phishing por correo electrónico. Internet es vital para gran parte de nuestras vidas empresariales y personales, y la naturaleza global de Internet también nos expone a un conjunto de riesgos.

Si el «coste de la ciberdelincuencia» fuera un país, sería la tercera economía mundial, solo por detrás de Estados Unidos y China, con 9.000 millones de dólares en 2024$[1].

Vivimos en una época de guerras geopolíticas e híbridas. Los conflictos ya no se limitan al campo de batalla: los estados-nación y los actores alineados con los ellos utilizan regularmente la perturbación de nuestro mundo digital para promover sus objetivos en el mundo real. Los grupos de delincuencia organizada se han pasado a la alta tecnología y se han dado cuenta de que pueden hacer grandes fortunas con los ataques de ransomware, con pocas posibilidades, por desgracia, de ser llevados ante la justicia.

En aproximadamente el 45% de los casos registrados este año, los atacantes filtraron información al día siguiente del ataque[2].

El entorno normativo nunca ha sido tan estricto: la Unión Europea ha introducido leyes como NIS 2 y DORA, que obligan a las organizaciones a mejorar su ciberseguridad.

Dado que las organizaciones operan en este complejo entorno, inmersas en un panorama de amenazas cada vez peor y con requisitos normativos cada vez más estrictos, esperamos que esta guía le ayude a descifrar parte de la jerga y le proporcione una visión pragmática sobre cómo guiar a su empresa en estos tiempos turbulentos.

En 2022 y 2023, para los incidentes no relacionados con la extorsión, el tiempo medio hasta la exfiltración de datos se ha mantenido sistemáticamente por debajo de un día, lo que significa que los defensores deben reaccionar ante un ataque de rescate en menos de 24 horas[3].

Los riesgos de no hacer nada

No invertir en una ciberseguridad sólida puede acarrear graves consecuencias:

- **Pérdida económicas:** Las filtraciones de datos y los ataques de ransomware pueden dar lugar a multas, costes legales y pérdida de ingresos.
- **Daños a la reputación:** Un incidente de seguridad puede erosionar la confianza de los clientes y las partes interesadas.
- **Tiempo de inactividad operativa:** Los ciberataques suelen interrumpir los procesos empresariales, lo que provoca retrasos y la pérdida de productividad.
- **Sanciones reglamentarias:** El incumplimiento de marcos como NIS2 o GDPR puede dar lugar a multas significativas.

Aunque está claro que invertir poco en seguridad tiene riesgos obvios, invertir demasiado en seguridad o invertir en las áreas equivocadas también es malo para el negocio. Demasiada seguridad puede frustrar a empleados y clientes, por no mencionar el coste de oportunidad de utilizar ese presupuesto para hacer crecer su negocio.

La seguridad es siempre un acto de equilibrio, con el objetivo de lograr la seguridad «justa» sin causar otros impactos en su negocio.

Entendiendo lo básico

El sector utiliza una variedad desconcertante de acrónimos, y el marketing de los vendedores contribuye en gran medida a la confusión. Merece la pena conocer y comprender algunos de los más comunes para estar seguro de hablar el mismo idioma con proveedores y partners.

Tecnología:

- **Detección y Respuesta a Endpoints (EDR):** Se centra en identificar y responder a las amenazas en los endpoints individuales (portátiles, servidores, dispositivos móviles) proporcionando datos detallados y herramientas de corrección.
- **Network Detection and Response (NDR):** es un enfoque de ciberseguridad que utiliza análisis avanzados, aprendizaje automático y detección de comportamientos para supervisar el tráfico de red en tiempo real, identificar anomalías o amenazas y proporcionar información procesable para mitigar los riesgos y mejorar los tiempos de respuesta.
- **Detección y respuesta ampliadas (XDR):** Va más allá de los puntos finales, integrando datos de múltiples fuentes (red, correo electrónico, nube) para una detección de amenazas y un contexto más amplios.
- **Gestión de información de seguridad y eventos (SIEM):** Recopila y analiza registros de toda la organización para identificar actividades sospechosas. Ideal para el cumplimiento de la normativa y la centralización de datos.
- **Consumo:** Un coche es inútil sin el tipo de combustible adecuado, y el SIEM es igual. Debe alimentarse con los registros de sus activos de TI existentes, y la cantidad de registros que ingiera repercutirá en el coste de la solución. Normalmente se mide en gigabytes al día o eventos por segundo. (EPS).
- **Orquestación, automatización y respuesta de seguridad (SOAR):** se refiere a un conjunto de herramientas y procesos que permiten a los equipos de seguridad agilizar y automatizar los flujos de trabajo de detección, investigación y respuesta ante amenazas. Al integrar sistemas de seguridad dispares y automatizar tareas repetitivas, SOAR mejora la eficacia, reduce los tiempos de respuesta y permite a los analistas centrarse en actividades de mayor valor.

Personas y procesos:

- **Detección y Respuesta Gestionadas (MDR):** Servicios de seguridad externalizados que combinan tecnología (a menudo SIEM o XDR) con un equipo de expertos que se ocupan de la detección, investigación y respuesta.
- **Centro de Operaciones de Seguridad (SOC):** Un equipo o instalación centralizada responsable de supervisar y responder a los incidentes de seguridad, ya sea internamente o gestionado por un proveedor.

¿Cómo encajan todos estos elementos?

Un servicio de seguridad gestionado consta de personas, procesos y tecnología. La tecnología es crucial para poder recopilar todos los datos necesarios para proporcionar información a las personas que gestionan el servicio. Un requisito mínimo absoluto es una herramienta EDR que proporcione datos sobre lo que ocurre en los terminales. Muchos proveedores están pasando de la EDR a la XDR, que incluye algo más que los datos de los terminales para ofrecer una visión más amplia de toda la organización.

Las herramientas XDR son excelentes para detectar incidentes «en el momento», pero suelen tener una visión más a corto plazo del mundo. Muchas organizaciones optan por complementar la XDR con una solución SIEM, que conserva los datos de registro sin procesar durante un periodo prolongado, normalmente un mínimo de 90 días, pero que puede ser de muchos años. Si su organización necesita ajustarse a los requisitos de cumplimiento de la normativa, un SIEM puede ser necesario.

El personal y los procesos suelen proceder del proveedor de servicios gestionados. Si ya ha invertido en tecnología, necesitará un partner que la domine y haya adquirido experiencia, y establecido reglas y detecciones basadas en ese proveedor, de modo que pueda aportar valor de forma inmediata. Si aún no ha invertido en tecnología, muchos partners estarán encantados de sugerirle una.

Si ha decidido recurrir a un partner para la seguridad gestionada, asegúrese de que está comprando un resultado. Si la tecnología es puntera en el mercado, es más importante seleccionar un partner por el servicio que ofrece y por lo bien que puede satisfacer sus necesidades de seguridad. Céntrese en cómo trabajarán juntos para mejorar la seguridad y deje que el partner se preocupe de la tecnología.

SIEM frente a XDR: ¿Cuál es la diferencia?

Aunque tanto SIEM como XDR son tecnologías fundamentales en ciberseguridad, sirven para fines diferentes::

CARACTERÍSTICAS	SIEM	XDR
Función principal	Agrega y analiza registros para el cumplimiento de normativas y la detección de amenazas.	Detección unificada de amenazas en múltiples vectores con respuestas automatizadas.
Modelo de implantación	Normalmente requiere configuración y mantenimiento internos.	Se entrega como un servicio gestionado o una plataforma de software.
Alcance	Amplio y flexible, compatible con integraciones personalizadas.	Menor alcance pero mayor integración entre las herramientas compatibles.
Casos de uso	Ideal para organizaciones centradas en el cumplimiento normativo y con experiencia.	Ideal para organizaciones que buscan una detección y respuesta simplificadas e integradas.

Ambos tienen sus puntos fuertes. Muchas organizaciones combinan las capacidades de cumplimiento normativo de un SIEM con la detección de amenazas avanzadas de XDR para cubrir todas las bases.

El caso de negocio de la seguridad gestionada

Hace un par de décadas, muchas organizaciones no consideraban la seguridad en absoluto. A medida que se producían las primeras ciberamenazas, las organizaciones empezaron a invertir en antivirus, cortafuegos y otros controles de seguridad básicos para mantenerse a salvo. El "encargado de seguridad" gestionaba estos controles y las cosas eran sencillas. Sin embargo, el aumento de las amenazas supuso una mayor inversión en nuevos controles. El «encargado de seguridad» se convierte en un equipo de seguridad; cada miembro con un conjunto diferente de habilidades. Proteger los datos, las aplicaciones, la infraestructura, la nube y los sistemas de IA requiere un conjunto de habilidades diferentes, y todos estos conjuntos de habilidades diferentes deben gestionarse de forma cohesionada para garantizar una cobertura de seguridad integral.

El coste y la complejidad de gestionar la seguridad internamente es una barrera de entrada para muchos. La alternativa es asociarse con un proveedor de servicios de seguridad gestionados.

ASPECTO	SOC interno	Partner MSSP
Coste	Altos costes iniciales de infraestructura, herramientas y contratación.	Menos costes iniciales y costes de servicio continuos gracias al pago de ETC fraccionados.
Experiencia	Requiere contratar y retener a profesionales altamente cualificados.	Acceso a una amplia gama de conocimientos sin necesidad de contratación.
Escalabilidad	La extensión requiere una inversión adicional en recursos, personal e infraestructura.	Fácilmente escalable con la infraestructura existente del MSSP.
Cobertura 24/7	Caro y complejo de conseguir con personal interno. Necesidad de al menos 12 personas para cubrir todo el día.	Normalmente incluido como parte del servicio.

ASPECTO	SOC interno	Partner MSSP
Control	Control total de las operaciones, personalizaciones y priorización del SOC.	Control limitado, con cierta dependencia de los procesos y la priorización del MSSP.
Plan de implementación	Más tiempo debido a la instalación, alquiler y configuración.	Configuración más rápida, ya que los MSSP a menudo tienen soluciones y procesos preconfigurados.
Actualizaciones de tecnología	La organización es responsable de mantenerse al día con las herramientas y tecnologías.	Los MSSP proporcionan acceso a las últimas herramientas y tecnologías como parte del servicio.
Gobernanza y cumplimiento	Plena responsabilidad en el cumplimiento de los requisitos normativos y de conformidad.	Los MSSP suelen prestar servicios acordes con los requisitos de cumplimiento, pero puede que no cubran los matices específicos de la organización.
Inteligencia sobre amenazas	Requiere la creación o suscripción independiente a fuentes de información sobre amenazas.	Acceso a información agregada sobre amenazas desde múltiples clientes.
Personalización	Muy adaptable a las necesidades y flujos de trabajo específicos de cada organización.	Es posible que las ofertas estandarizadas no se ajusten plenamente a las necesidades específicas.
Conocimiento del contexto empresarial	Conocimiento profundo de la estructura, las prioridades y el contexto de la organización.	Conocimiento limitado del entorno específico de la organización.
Colaboración interna	Alineación más sencilla de las operaciones del SOC con los equipos internos de TI y seguridad.	Requiere una mayor coordinación entre la organización y el MSSP.

¿Cuáles son los costes de crear un equipo interno?

La creación de un centro de operaciones de seguridad (SOC) interno requiere una planificación financiera cuidadosa, ya que hay múltiples factores de coste que deben tenerse en cuenta:

1. Costes de personal

- **Analistas de SOC:** Asuma un mínimo absoluto de dos analistas por turno para mantener una cobertura 24 horas al día, 7 días a la semana, teniendo en cuenta las bajas por enfermedad, las vacaciones y la prevención del agotamiento.
- **Ingenieros de seguridad:** Al menos dos ingenieros dedicados a crear, gestionar y actualizar las herramientas del SOC e infraestructura.
- **Funciones especializadas:** Considere la posibilidad de añadir agentes de respuesta a incidentes, detectores de amenazas y un gestor de SOC para garantizar que el equipo opere de forma eficaz.
- **Formación y certificación:** Formación continua para mantener al equipo al día de la evolución de las amenazas, las herramientas y los requisitos de cumplimiento.

2. Costes de SIEM (gestión de información de seguridad y eventos)

- **Tarifas de licenciamiento y suscripción:** Los costes suelen basarse en el volumen de datos de registro consumidos.
- **Infraestructura:** Alojar el SIEM in situ o en la nube puede suponer costes adicionales en servidores, almacenamiento y ancho de banda.
- **Alternativas de código abierto:** Aunque existen plataformas gratuitas, pueden requerir una inversión sustancial en personal cualificado o consultoría externa para su configuración, mantenimiento y puesta a punto.

3. Costes de la inteligencia sobre amenazas

- **Suscripciones:** Acceso de pago a fuentes de información sobre amenazas para enriquecer los datos y contextualizar las alertas.
- **Integración:** Costes adicionales para integrar las plataformas de inteligencia sobre amenazas en su ecosistema actual.

4. Costes de detección y respuesta para endpoints (EDR/XDR)

- **Licencias de herramientas:** Licencias para detectar y responder a amenazas en endpoints, redes y otros activos.
- **Costes de escalado:** Los costes varían en función del número de dispositivos o activos supervisados.

5. Costes de infraestructura

- **Hardware y software:** Servidores, dispositivos de almacenamiento y software para la recopilación, el análisis y el almacenamiento de registros.
- **Redundancia y recuperación ante desastres:** Sistemas de copia de seguridad y planes de recuperación ante desastres para operaciones de SOC.
- **Espacio físico:** Espacio de oficinas seguro o una sala de operaciones específica con los controles ambientales adecuados.

6. Herramientas de supervisión y detección

- Herramientas de supervisión del tráfico de red, análisis del comportamiento y sistemas de detección de intrusiones (IDS/IPS).
- Actualizaciones y ajustes periódicos para garantizar la eficacia frente a las amenazas cambiantes.

7. Costes de respuesta a incidentes

- **Desarrollo de la guía práctica:** Tiempo y recursos para desarrollar procesos y flujos de trabajo detallados de respuesta a incidentes.
- **Herramientas forenses:** Herramientas especializadas para la investigación en profundidad de infracciones o actividades sospechosas.

8. Costes de cumplimiento y reglamentación

- Garantizar el cumplimiento de las normas del sector. (por ejemplo, ISO27001, NIS2, PCI DSS) pueden requerir inversiones adicionales en herramientas, auditorías y conocimientos especializados.
- Evaluaciones y auditorías periódicas para verificar el cumplimiento.

9. Costes de gestión de vulnerabilidades

- Herramientas para la exploración y gestión de vulnerabilidades en todo su entorno de TI.
- Tiempo del personal o consultoría para la gestión de parches y los esfuerzos de reparación.

10. Licenciamiento para plataformas de seguridad

- Costes adicionales de licencias para DLP (Prevención de Pérdida de Datos), herramientas de seguridad en la nube o cortafuegos integrados con operaciones SOC.

11. Costes de pruebas y optimización

- **Pruebas de intrusión:** Pruebas periódicas de los procesos y defensas del SOC para detectar lagunas.
- **Ejercicios de Equipo Rojo/Equipo Azul:** Ejercicios de formación para mejorar la preparación del SOC y perfeccionar las capacidades de respuesta a incidentes.

12. Integración con los sistemas de TI existentes

- Costes de integración de las herramientas SOC con los sistemas de gestión de TI, como Active Directory, sistemas de tickets y plataformas ITSM.

13. Mantenimiento y actualizaciones

- Actualizaciones periódicas de software, parches y ajustes de configuración.
- Sustitución del hardware o software obsoleto con el paso del tiempo.

14. Consultorías y asociaciones de terceros

- Costes a corto plazo de consultores especializados que ayuden en la configuración inicial o en tareas complejas.
- Posibles asociaciones con proveedores para el apoyo y la cogestión durante las primeras fases operativas.

15. Costes ocultos e indirectos

- **Inversión de tiempo:** Se necesita mucho tiempo para configurar, ajustar y optimizar el SOC antes de que esté plenamente operativo.
- **Costes de oportunidad:** Tiempo y recursos desviados de otros proyectos informáticos y de seguridad.

¿Cuáles son los costes de asociarse con un MSSP?

Como el proveedor ya ha invertido en todas las partidas anteriores, usted pagará una parte de estos costes, normalmente en función de su consumo. La ventaja para usted es que no pagará por un equipo entero que estará infrautilizado, sino que tendrá acceso a un equipo entero cuando lo necesite.

Los proveedores habituales de servicios de seguridad gestionada fijarán el precio de un servicio en función de una combinación de los siguientes factores:

- **Número de usuarios:** por supuesto, cuantos más usuarios, más incidentes habrá que gestionar.
- **Número de endpoints:** hoy en día, los usuarios suelen tener varios puntos finales, y también es fundamental supervisar los servidores.
- **Volumen de datos de registro:** algunas organizaciones pequeñas generan muchos datos, mientras que otras grandes pueden tener una infraestructura bastante sencilla. Al analizar la cantidad de datos de registro que su empresa genera, los MSSP pueden estimar el nivel de respuesta a incidentes que será necesario.

Aunque probablemente usted conozca el número de usuarios y endpoints, a menos que ya disponga de un SIEM o SOC, es posible que desconozca el volumen de datos de registro. Un buen partner le ayudará a hacer una estimación en función de la cantidad y los tipos de dispositivos que tenga en su patrimonio; este trabajo suele ser gratuito como parte del compromiso de preventa.

El proveedor puede ofrecer un pago inicial para cubrir el trabajo de consultoría necesario para poner en marcha el servicio, seguido de una cuota mensual, o puede combinar ambos en una única cuota mensual. Lo ideal es que puedan trabajar con cualquiera de las dos, según sus preferencias.

Puede haber costes asociados a la licencia de la propia plataforma SIEM. Esto puede estar incluido en la cuota mensual o pagarse por separado a un proveedor de SaaS como Microsoft o Cisco. El partner debe indicar claramente si hay que pagar honorarios adicionales a terceros y debe calcularlos para que usted disponga de un precio total.

SLA e informes: La base del servicio

Un acuerdo de nivel de servicio (SLA) define las expectativas, responsabilidades y métricas de rendimiento entre usted y su proveedor de seguridad gestionada. Un SLA sólido garantiza la claridad, la responsabilidad y la alineación con las necesidades de su empresa, pero no todos los acuerdos de nivel de servicio son iguales.

- **Tiempo medio de detección:** Cuánto tiempo transcurre entre que se produce un incidente y es detectado por el SOC? Con las plataformas SIEM modernas, la detección debería ser casi en tiempo real; sin embargo, detectar un incidente depende de lo bien configurada que esté la plataforma, de las fuentes de registro que se ingieran y de la calidad de las reglas. Es difícil comparar directamente los SLA a este nivel.

- **Tiempo medio de respuesta:** Una vez detectado un incidente, ¿con qué rapidez responde el SOC? Aunque esta medida suele ser la más importante, no es tan sencillo como buscar al partner con el tiempo más rápido... (vea el apartado «Cómo es un buen SLA»).

- **Tiempo medio de reparación:** ¿Cuánto tiempo transcurre entre la respuesta y la resolución del problema? Hay una amplia gama de tipos y complejidades de incidentes, por lo que, una vez más, es difícil comparar estas cifras. Además, algunas actividades de reparación pueden requerir que su equipo de TI interno o un tercero las resuelva; los MSSP excluyen estos tiempos de este SLA.

Cómo es un buen SLA

Un SLA bien elaborado equilibra el rendimiento con la practicidad. Busque lo siguiente:

- **Priorización basada en el riesgo:** Mayor urgencia para incidencias críticas y menor prioridad para cuestiones menores.

- **Métricas transparentes:** Definiciones claras de tiempos de respuesta y resolución con resultados medibles.

- **Plazos realistas:** A primera vista, un tiempo de respuesta de 5 minutos puede parecer mejor que uno de 30 minutos. Pero, ¿cuál es el contenido de una «respuesta»? ¿De verdad quiere que le llamen a las 3 de la madrugada todas las noches porque un partner está dando prioridad a su SLA frente a la eliminación de falsos positivos? Pagará al partner para que clasifique y confirme los verdaderos positivos, no sólo para que le reenvíe directamente todas las alertas del SIEM.

Los SLA son la base de la confianza entre usted y su proveedor. Un buen SLA no sólo promete rapidez, sino que garantiza calidad, responsabilidad y alineación con sus objetivos empresariales.

Informes

Por lo general, encontrará dos tipos de informes: informes rutinarios e informes "ad-hoc" que se generan cuando se detecta un incidente y se le notifican. Tienen por objeto comunicar rápidamente un problema, por lo general algo que requiere su intervención o una notificación a tiempo.
Sin embargo, el MSSP no solo debe intervenir cuando hay un problema. Debe haber una cadencia regular de reuniones, tanto con las partes interesadas técnicas como con las empresariales, en las que se traten temas como:

- **Cobertura de fuentes de registro:** El servicio es tan bueno como los registros a los que tiene acceso. ¿Utiliza el proveedor un marco como MITRE ATT&CK para asesorarle sobre fuentes de registro adicionales que podrían añadir valor?
- **Rendimiento respecto al SLA:** Una oportunidad para analizar el rendimiento del servicio en relación con el SLA y poner en marcha planes correctivos en caso necesario.
- **Revisión de incidentes anteriores:** Una mirada retrospectiva a algunos de los incidentes más graves: ¿Qué salió bien y qué podría mejorarse?
- **Una visión más amplia:** el mundo no se detiene, su organización cambiará con el tiempo, al igual que lo hará el panorama de las amenazas. Debe existir la posibilidad de informar periódicamente al proveedor de cualquier cambio en la empresa (por ejemplo, fusiones y adquisiciones) que pueda afectar al servicio, y de que el proveedor ofrezca información sobre nuevas amenazas y soluciones.

Capacidades que debe buscar en un partner de seguridad gestionada

Automatización e IA

Las amenazas modernas requieren una detección y respuesta rápidas. Los proveedores deben aprovechar la automatización y la IA para:

- Identificar anomalías en tiempo real, reduciendo la dependencia del análisis manual.
- Agilizar los flujos de trabajo de respuesta a incidentes, garantizando una rápida contención.
- Automatizar acciones comunes como aislar un dispositivo o bloquear una cuenta comprometida. Esto es especialmente importante si desea que el partner pueda actuar en su nombre fuera del horario laboral.

Inteligencia sobre amenazas

La información procesable sobre amenazas le ayudará a anticiparse a los riesgos cambiantes. Busque proveedores que:

- Mantengan actualizados los feeds de amenazas y los integren en sus servicios.
- Compartan ideas sobre nuevas tendencias de ataque relevantes para su sector.
- Utilicen la inteligencia para mejorar la detección y priorizar las amenazas críticas.

Búsqueda de amenazas:

La búsqueda proactiva de amenazas garantiza que éstas no pasen desapercibidas. Evalúe si el proveedor:

- Ofrece actividades regulares y manuales de detección de amenazas.
- Utiliza herramientas avanzadas para identificar riesgos ocultos.
- Proporciona informes detallados sobre las conclusiones y las medidas paliativas.

Remediación

Las alertas son solo una parte de la ecuación: la remediación eficaz es crítica. Asegúrese de que el proveedor:

- Ofrece una orientación clara sobre las estrategias de contención.
- Tiene capacidad de consultoría para ayudarle a poner en marcha proyectos de mayor envergadura para mejorar la madurez de la seguridad.

Consideraciones prácticas

Certificaciones

Cualquier partner podrá mostrarle materiales de marketing atractivos, pero ¿qué validación externa puede aportar para respaldar la eficacia de su servicio

- Busque una validación externa e imparcial de fuentes como MSSP Alert: www.msspalert.com/top-250

- Compruebe si están acreditados en el proveedor que elija. Usted querrá asegurarse de que son expertos en sus herramientas y de que su servicio ha sido verificado por el proveedor. Esto también indica que colaborarán estrechamente con el proveedor en las mejoras y tendrán una buena relación con su equipo de ingenieros.

- Compruebe si existen marcos de cumplimiento pertinentes en su región o sector. Certificados como Cyber Essentials+ e ISO27001 indican que la organización se toma en serio su propia seguridad y deberían ser un requisito mínimo para un proveedor de seguridad.

Proceso de onboarding

Es de esperar que un buen partner le guíe a través del proceso de integración. En el cuadro que figura a continuación se indican las etapas principales. Aunque el partner debe hacer el trabajo pesado, es importante ser consciente de cualquier dependencia de su personal para poder planificarla.

¿Qué?	Participación
Alcance y detección: Para poder ofrecer una solución adecuada, el partner tendrá que hacerle muchas preguntas sobre sus aspiraciones para el servicio y su conjunto tecnológico actual.	Debe contar con la participación de varias partes interesadas para poder ofrecer una visión general de la composición y el tamaño de su patrimonio. Conocer aspectos como el número de dispositivos de punto final y la marca, modelo y cantidad de cortafuegos, servicios en la nube y otros activos ayudará a garantizar que el diseño se adapte a sus necesidades.
Construcción de la plataforma: Si es necesario desplegar una herramienta SIEM o XDR en todo su parque, querrá participar en ello para garantizar que se minimizan las molestias a los usuarios.	Es posible que su equipo de TI tenga que proporcionar acceso a su entorno de nube para que el partner despliegue el SIEM. Debe colaborar con el partner para crear un plan conjunto sobre cómo y cuándo se desplegarán los agentes para endpoints.
Personalización: Cualquier buen partner tendrá un conjunto de reglas por defecto que funcionarán para detectar incidentes en la mayoría de las organizaciones. Pero, si necesita personalizaciones específicas, tendrá que trabajar con el partner para asegurarse de que se tienen en cuenta sus necesidades.	Si ya dispone de reglas en un sistema heredado que deben reescribirse, proporcionarlas puede agilizar el onboarding en lugar de empezar desde cero. Si se trata de requisitos nuevos, documentarlos en lenguaje natural puede ayudar a comunicar sus necesidades al partner.
Soporte vital temprano: Una vez que el servicio entre en funcionamiento, habrá un periodo de ajuste adicional para reducir los falsos positivos y ajustar el sistema a su entorno específico.	Será necesaria una estrecha colaboración entre su equipo de TI y el partner. Aunque para el partner será fácil clasificar muchos incidentes como falsos o verdaderos positivos, querrá trabajar con usted en la «zona gris» para asegurarse de que se pueden redactar artículos en la base de conocimientos y personalizar las reglas para minimizar los falsos positivos en la operación.
Operaciones en directo: Una vez completado el soporte vital inicial, la solución pasará a un estado estable. El trabajo de personalización del partner no se detiene en este punto, pero debería ralentizarse considerablemente a medida que la atención se centre en la detección de incidentes.	Deberá proporcionar un mapa de contactos para saber a quién se debe notificar cuando se produzca un incidente de seguridad. Podría tratarse de una única lista de distribución para organizaciones más pequeñas, pero también podría tener una complejidad añadida, como diferentes vías de escalado dentro o fuera del horario laboral, o grupos de resolución específicos para problemas con determinada tecnología. Incluso podría incluir a terceros si ha subcontratado algunas operaciones.

Servicios de valor añadido

Aunque su principal preocupación a la hora de buscar un proveedor de seguridad gestionada será ayudarle a detectar y solucionar incidentes de seguridad, a menudo hay otros servicios que encajan de forma natural con un proveedor de seguridad gestionada, y merece la pena considerar si alguno de ellos podría serle útil, y podría incluirse al mismo tiempo. A menudo resulta beneficioso contar con varios servicios prestados por el mismo partner, ya que tendrá una mayor visibilidad de su seguridad y a menudo podrá tomar decisiones más informadas.

La gestión de vulnerabilidades es el complemento natural de un SOC, ya que identifica, evalúa y prioriza de forma proactiva los fallos de seguridad en todo el entorno digital de una organización. Al integrar este servicio, las organizaciones se benefician de una supervisión continua de las vulnerabilidades y de planes de corrección procesables que se alinean con las capacidades de detección de amenazas del SOC. Esto reduce el riesgo de explotación al cerrar las brechas de seguridad antes de que los atacantes puedan explotarlas.

Los servicios de protección de riesgos digitales (DRPS) ofrecen otra adición estratégica, ampliando el alcance del SOC más allá de la red corporativa al panorama digital más amplio. DRPS supervisa las amenazas en entornos externos, como la Web oscura, las redes sociales y los sistemas externos. Al identificar suplantaciones de marca, fugas de credenciales o datos sensibles expuestos, las organizaciones pueden obtener alertas tempranas de posibles amenazas, lo que permite al SOC responder rápidamente y mitigar los riesgos.

Para las organizaciones que se enfrentan a amenazas activas o infracciones, la combinación **de análisis forense digital y respuesta a incidentes (DFIR)** con la seguridad gestionada garantiza una rápida contención y un análisis detallado posterior al incidente. Los equipos de DFIR pueden aprovechar la telemetría y los registros del SOC para investigar las causas, determinar el alcance de la brecha y recomendar medidas de recuperación. Este enfoque holístico permite a las empresas responder de forma decisiva y, al mismo tiempo, obtener información para evitar la recurrencia. La agrupación de estos servicios crea una solución de seguridad integral sin fisuras, que ofrece a las organizaciones confianza tanto tanto en materia de prevención como de resiliencia.

Próximos pasos

Las amenazas a la ciberseguridad van en aumento, y el coste de no hacer nada es muy alto. No espere a que se produzca esa brecha, póngase en contacto con Insight, uno de los principales MSSP, y descubra cómo nuestros servicios de seguridad gestionada pueden ser la forma más rentable de ayudarle a proteger su empresa.

- **es.insight.com**
- **91 384 07 90**

[1] fuente: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

[2] fuente: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

[3] fuente: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report