MONOGRÁFICO

Gestionar la ciberseguridad con un centro de operaciones de seguridad eficaz

Descubra qué modelo de SOC se adapta mejor a las necesidades de su organización.

SOPHOS

Resumen ejecutivo

El panorama de la ciberseguridad está en constante cambio, con amenazas que se vuelven más sofisticadas y omnipresentes. En este contexto, los centros de operaciones de seguridad (SOC) son fundamentales para que las organizaciones detecten, analicen y respondan rápidamente a los ciberincidentes. Las organizaciones deben decidir qué modelo de SOC les conviene más: interno, híbrido o externalizado, y luego asegurarse de utilizar las métricas adecuadas para evaluar su rendimiento y garantizar la continuidad de la seguridad, sin perder de vista los objetivos empresariales.

63 % de las empresas

sufren ataques de ransomware debido a la falta de personal o de conocimientos técnicos.[1]

El papel de un SOC en el panorama actual de la ciberseguridad

La era digital ha traído consigo un aumento de las ciberamenazas, con ciberdelincuentes y agentes patrocinados por gobiernos que perpetran ataques sofisticados. Según las tendencias actuales, el tiempo que transcurre entre el acceso inicial y el despliegue del ransomware se ha reducido de forma preocupante, hasta alcanzar una media de solo dos días.[2] Por otra parte, el sector de la ciberseguridad sigue acusando una importante escasez de talento, lo que complica aún más la creación y el mantenimiento de un SOC interno.

Escasez de talento

El sector de la ciberseguridad sigue acusando una importante escasez de especialistas.

Un SOC es una función organizativa dedicada a gestionar procesos para identificar, investigar y remediar incidentes de seguridad. Entre sus responsabilidades más específicas se incluyen la gestión de activos, la gestión de cambios, la gestión de vulnerabilidades, la gestión de eventos de seguridad, la gestión de incidentes, así como la incorporación de información sobre amenazas y diversas actividades de DevOps, como la automatización y el control de calidad. Si bien los SOC no controlan todos los aspectos de la seguridad de una organización, desempeñan un papel fundamental en la coordinación de su respuesta ante problemas de seguridad. La misión y los objetivos específicos de un SOC pueden variar mucho, dependiendo de factores como la tolerancia al riesgo de la organización, el sector, el nivel de madurez y las herramientas y procesos que usa.

Tipos de modelos de SOC

Las organizaciones pueden elegir entre varios modelos de SOC, cada uno con sus respectivas características y ventajas:

SOC internos: suelen pertenecer a organizaciones bien financiadas que pueden mantener operaciones continuas con un equipo dedicado. Es posible que estos SOC externalicen ciertas funciones especializadas, como pruebas de penetración, búsqueda de amenazas por parte de expertos o información sobre amenazas. Las organizaciones grandes o geográficamente dispersas pueden utilizar un modelo por niveles con varios SOC que operan bajo una estructura de mando unificada.

SOC híbridos: se han vuelto cada vez más habituales, ya que combinan recursos internos con servicios externos para crear una función de seguridad personalizada en un modelo de colaboración. El proveedor de servicios de seguridad suele encargarse de la supervisión y la clasificación de alertas 24/7, la investigación de incidentes, la búsqueda de amenazas y la prestación de asistencia especializada. Esto permite al equipo interno maximizar sus recursos mediante actividades como la arquitectura y el diseño de la seguridad, la gestión de políticas y el cumplimiento normativo, la mitigación de riesgos, la formación en materia de seguridad y la ejecución de medidas de respuesta cuando la organización prefiere mantener la remediación en la empresa. Esto resulta particularmente atractivo por la flexibilidad que ofrece y la capacidad de solventar la escasez de personal cualificado y las restricciones presupuestarias.

SOC totalmente externalizados: son un servicio de terceros que proporciona funciones integrales de supervisión y respuesta en materia de ciberseguridad. Las organizaciones que necesitan montar rápidamente un SOC de base sin contar con los conocimientos técnicos necesarios a nivel interno pueden recurrir a este modelo, depositando su confianza en un proveedor consolidado de servicios de detección y respuesta gestionadas (MDR). La organización puede permitir que el proveedor externo se integre con sus tecnologías de TI y seguridad existentes para obtener una amplia visibilidad de todo el entorno y coordinar las actividades de respuesta a incidentes.

¿Sabía que...

El 88 % de los ataques de ransomware se producen fuera del horario laboral habitual.[2]

¿Qué modelo es el adecuado para su organización?

Determinar el modelo de SOC adecuado para su organización depende de varios factores, incluido su perfil de riesgo general. Debe sopesar el nivel de riesgo aceptable de su empresa frente al presupuesto que está dispuesto a destinar a la ciberseguridad. Hay varios aspectos clave que deben tenerse en cuenta, entre ellos:

1. Las limitaciones en cuanto a recursos internos (la disponibilidad de conocimientos especializados o de personal/capacidad)
2. El equilibrio entre lo que debe gestionarse internamente y lo que debe externalizarse
3. El grado de madurez actual de sus operaciones de seguridad
4. El reto de contratar, formar y retener a los mejores talentos con competencias especializadas
5. La necesidad de trabajar continuamente con tecnologías emergentes y mantenerse a la vanguardia de las amenazas en constante evolución y las técnicas de los adversarios activos
6. La dependencia entre los departamentos de TI, jurídico, de riesgos, de cumplimiento normativo y otros

Sea cual sea el modelo que elija, es importante desarrollar un argumento comercial que justifique el modelo y los recursos necesarios para garantizar la sostenibilidad a largo plazo. También es fundamental evaluar periódicamente las capacidades del SOC para asegurarse de que se ajusta al diseño previsto y a los objetivos operativos.

La mayoría de las organizaciones adolecen de una escasez de personal cualificado en ciberseguridad, y muchos presupuestos impiden crear y mantener un SOC interno 24/7 con todo el personal necesario. Los CISO con más experiencia también comprenden el valor de mantener el control estratégico sobre sus operaciones de ciberseguridad y, por extensión, la sostenibilidad a largo plazo de su organización, mediante la supervisión y el control.

Ventajas del modelo de SOC híbrido

El modelo de SOC híbrido es la combinación perfecta de las ventajas del enfoque interno y externalizado. Permite a las organizaciones beneficiarse de la experiencia y la eficiencia de un proveedor externo, sin renunciar a la personalización y el control de sus operaciones de seguridad.

Una de las principales ventajas de un SOC híbrido es el acceso y el alcance a expertos en seguridad y a información validada sobre amenazas. Estos profesionales forman parte de un grupo más amplio de talentos que están continuamente expuestos a una gran variedad de amenazas, lo que les permite estar al día de las últimas novedades en el campo de la ciberseguridad. Esta exposición normalmente no la podría igualar un equipo interno independiente, dada la rápida evolución del panorama de amenazas.

Además, colaborar con un proveedor externo garantiza una cobertura continua 24/7/365, incluyendo noches, fines de semana y días festivos, cuando los equipos internos quizá no estén disponibles.

Un SOC híbrido puede reducir significativamente la fatiga por alertas al ayudar a las organizaciones a ajustar sus sistemas de detección, lo que reduce el tiempo medio de respuesta (MTTR) a incidentes. Las organizaciones también pueden ahorrarse los elevados costes que conlleva la investigación sobre amenazas dedicada, ya que sus Partners externos se encargarán de realizarla en su nombre, añadiendo continuamente funcionalidades de detección a medida que se desarrollan.

Otra ventaja es poder destinar los recursos internos a cuestiones clave de TI, tecnología y cumplimiento normativo, mientras que el proveedor del SOC se centra en los incidentes de seguridad. Esta división del trabajo permite asignar los recursos y conocimientos especializados de forma más eficiente. También permite que otros departamentos se centren en sus responsabilidades adicionales relacionadas con la seguridad.

En un modelo híbrido, se optimiza la formación en ciberseguridad, que puede resultar costosa y requerir mucho tiempo. El proveedor externo vela por que su personal esté al día en todos los aspectos de la ciberseguridad, desde el análisis forense y de malware hasta la respuesta a incidentes y la seguridad en la nube. De este modo, el equipo interno se libera de la carga que supone mantener conocimientos especializados en todos los aspectos de la ciberseguridad, lo que le permite centrarse en las áreas más relevantes para su negocio.

El modelo de SOC híbrido también ofrece flexibilidad para clasificar las operaciones en función de la propensión al riesgo de la organización y ajustar las metodologías de respuesta en consecuencia. Esto puede dar lugar a medidas de seguridad más eficaces y específicas. Además, el ahorro de costes asociado a un SOC híbrido lo convierte en una atractiva opción no solo para las pymes, sino también para las organizaciones grandes que desean externalizar determinadas funciones de seguridad.

Medir la eficacia del SOC

Sea cual sea el modelo más adecuado para su organización, para evaluar la efectividad de un SOC es esencial usar un conjunto de métricas que reflejen el panorama de seguridad y la eficacia de los recursos del SOC. Las métricas sugeridas a continuación, entre otras, pueden resumirse en un panel de control para mostrar recuentos en tiempo real, además de estadísticas semanales, mensuales y trimestrales para hacer un seguimiento de las tendencias a lo largo del tiempo, centrándose en la capacidad de respuesta del SOC y la calidad de la investigación.

En lo que respecta al panorama de seguridad, las métricas deben proporcionar información sobre el alcance y el volumen de las posibles amenazas, los puntos vulnerables de la organización y la exposición general al riesgo. Ejemplos de ello son el volumen de correos sospechosos o maliciosos recibidos, el número de intentos de escaneado y explotación contra sistemas externos y el número de incidentes de seguridad por origen.

Al evaluar la eficacia del SOC, las métricas deben registrar el rendimiento en relación con los objetivos establecidos en materia de políticas y postura, que están vinculados a resultados empresariales como la reducción del riesgo y el cumplimiento normativo. Esto incluye la capacidad de respuesta y la calidad de la investigación, el desglose del tiempo dedicado por el personal de seguridad a diversas actividades, el número de incidentes por categoría de cumplimiento y la cantidad de trabajo de ingeniería relacionado con la reducción de la superficie de ataque. Las métricas clave también incluyen el tiempo de clasificación de las investigaciones, el número de investigaciones con medidas correctivas adoptadas, el número de medidas correctivas basadas en la búsqueda proactiva de amenazas y el número de vulnerabilidades parcheadas clasificadas por gravedad.

Mediante la supervisión periódica de estas métricas, las organizaciones pueden garantizar que su SOC no solo funciona de manera eficiente, sino que también contribuye a la postura de seguridad general y a los objetivos de la empresa.

Las métricas deben:

- Ofrecer información sobre el alcance y el volumen de las posibles amenazas
- Detectar los puntos vulnerables de una organización
- Mostrar la exposición global al riesgo
- Hacer un seguimiento del rendimiento en relación con los objetivos establecidos en materia de políticas y postura

Métricas clave:

- Tiempo de clasificación de investigaciones
- Número de investigaciones con medidas correctivas adoptadas
- Número de medidas correctivas basadas en la búsqueda proactiva de amenazas
- Número de vulnerabilidades parcheadas clasificadas por gravedad

Encuentre una solución de SOC avanzada

Cada empresa es diferente y tiene distintos niveles de madurez en materia de seguridad. Con un panorama de amenazas en constante evolución, el acceso a un SOC competente es necesario para cualquier organización que se tome en serio su ciberseguridad. Tanto si las organizaciones optan por desarrollar internamente sus capacidades, trabajar con un proveedor externo o adoptar un enfoque híbrido, la colaboración adecuada puede garantizar una defensa eficaz y la alineación con los objetivos empresariales.

Muchas organizaciones están adoptando modelos de SOC híbridos o totalmente gestionados para abordar la falta de talento, las limitaciones presupuestarias y la creciente complejidad de las ciberamenazas. Estos modelos proporcionan flexibilidad, conocimientos especializados y cobertura 24/7, lo que permite a los equipos internos centrarse en iniciativas estratégicas al tiempo que Partners de confianza ofrecen operaciones de seguridad escalables.

Sophos MDR es un ejemplo del poder de este enfoque. Con ofertas por niveles diseñadas para satisfacer las necesidades de las organizaciones en su andadura en ciberseguridad, Sophos ofrece funciones avanzadas de detección, investigación y respuesta. Ya sea prestando apoyo a un equipo SOC interno u operando de forma totalmente externalizada, Sophos MDR mejora la visibilidad y la respuesta a amenazas, con lo que ayuda a las organizaciones a reforzar sus defensas y proteger lo que más importa.

[1] Sophos, informe El estado del ransomware 2025
[2] Sophos, Informe sobre adversarios activos 2025

SOPHOS

Más información sobre nuestros servicios de detección y respuesta gestionadas en es.sophos.com/mdr.

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com