Guía para comprender los Centros Globales de Operaciones de Seguridad

Por: Greg Newman, Vicepresidente de operaciones, HiveWatch

Muchas organizaciones grandes con amplia presencia en mercados regionales o globales necesitan supervisar la seguridad física de sus activos, personal y clientes desde una ubicación centralizada. Ahí es donde entra en juego un Centro Global de Operaciones de Seguridad (GSOC). Y, ya sea que trabajes para un integrador, fabricante, usuario final o algo intermedio, es muy probable que te encuentres con un GSOC mientras trabajes en esta industria. Así que, veamos en qué consiste esta pieza clave de la infraestructura de seguridad.

¿Qué es un GSOC?

Antes que nada, ¿qué es un GSOC? Con frecuencia utilizamos el término GSOC cuando una organización tiene una amplia presencia global y administra múltiples instalaciones en todo el mundo desde una ubicación central. Del mismo modo, también es posible encontrar el término Centro de Operaciones de Seguridad (SOC), que suele asociarse a un alcance más regional.

De cualquier manera, un GSOC es una instalación encargada de monitorear y responder a eventos de seguridad a escala global.

¿Cuál es la función de un GSOC?

El papel que juega un GSOC dentro de una organización es la de actuar como un punto central donde se recopilan, analizan y procesan los datos de seguridad entrantes para tomar las medidas correspondientes. En concreto, un GSOC integra información de inteligencia procedente de distintas fuentes para facilitar una respuesta más eficaz ante un incidente de seguridad o una emergencia. Los GSOC cumplen una función fundamental en la mitigación de riesgos a los que se enfrenta una organización, ya que ayudan a proteger a las personas y los activos frente a posibles daños y mantener la conciencia situacional de múltiples ubicaciones y de los riesgos a los que están expuestas.

Los GSOC desempeñan una gran variedad de funciones, entre las que se incluyen:

- Monitorear el desempeño de cámaras y soluciones de puntos de control de acceso para garantizar la disponibilidad y el flujo continuo de datos.
- Comunicarse con los equipos internos y personal de seguridad externo (recursos de vigilancia, equipos de seguridad u operaciones comerciales y autoridades locales) en caso de una emergencia o incidente.
- Facilitar los protocolos de respuesta ante emergencias.

- Garantizar la seguridad y protección de las personas, la marca y los bienes.
- Proporcionar información de valor sobre el desempeño del programa de seguridad de una organización mediante información analizada que facilite la toma de decisiones.
- Recopilar datos de múltiples fuentes para mejorar la capacidad de respuesta mediante decisiones fundamentadas en información analizada.

¿Quiénes trabajan en un GSOC?

Los GSOC están compuestos principalmente por operadores de seguridad y analistas de inteligencia, quienes se encargan de gestionar las alertas que se reciben, desde su identificación hasta su escalamiento y respuesta.

¿Qué es un GSOC virtual?

Para algunas organizaciones, crear un GSOC puede resultar demasiado costoso o incluso puede no tener sentido para la empresa a corto plazo. En estos casos, las empresas pueden beneficiarse de un GSOC virtual externo (vGSOC o GSOC como servicio), el cual consiste en recursos externos disponibles para supervisar y responder a incidentes de seguridad física en tiempo real desde una ubicación centralizada. Por lo general, se trata de una solución personalizada diseñada en función de las necesidades específicas de la operación de la empresa, pero administrada por expertos externos. Estos componentes del vGSOC utilizan la tecnología que el cliente ha implementado, junto con procedimientos operativos estándar (SOP) específicos para sus necesidades.

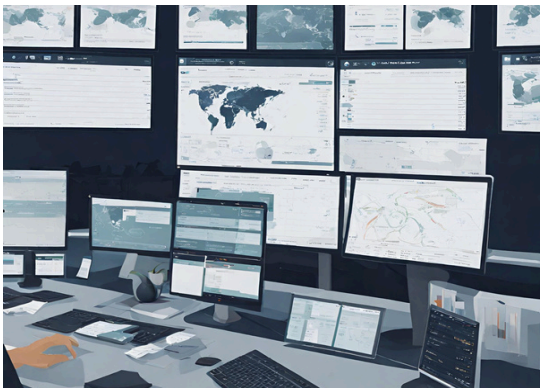
En algunos casos, las empresas pueden recurrir a un vGSOC mientras construyen su propia infraestructura con el objetivo de realizar cambios o la transición de su programa de seguridad existente hacia un modelo interno. Utilizar un vGSOC le permite a una organización ahorrar dinero al reducir los recursos internos y la capacitación necesaria para poner en marcha dicha operación.

¿Qué tipo de tecnología se encuentra en un GSOC?

Si bien los datos procedentes de soluciones tradicionales de punto final, como los sistemas de control de acceso y cámaras de videovigilancia, pueden canalizarse al GSOC para que los operadores los analicen, también existen otras herramientas que pueden emplearse, tales como:

Un *video wall o estación de trabajo* (*Workstation*)*:* Puede que no se vea exactamente como una escena de "*Minority Report: sentencia previa*", pero un GSOC normalmente sí cuenta con pantallas grandes que muestran una gran cantidad de fuentes de información, como transmisiones de noticias en vivo, actualizaciones de redes sociales, transmisiones de video y más.

Dashboard operativo: No es raro que los operadores de un GSOC tengan que navegar entre múltiples pantallas y soluciones para obtener la información que necesitan para un incidente en específico. Sin embargo, un GSOC moderno debe estar bien equipado con dashboards operativos y una plataforma de fusión diseñada para integrar datos de múltiples fuentes y agregar la información para los operadores. El resultado es una respuesta más eficiente que puede ahorrar tiempo y dinero.



Inteligencia artificial (IA): Aunque pueda parecer una palabra de moda, la IA se utiliza de muchas maneras en un GSOC moderno a través de detección de amenazas, detección de anomalías y optimización de procesos para los operadores y la protección de los recursos.

Soluciones de inteligencia sobre amenazas: El software capaz de procesar los datos que llegan al GSOC desde diversas fuentes, determinar los niveles de riesgo y ofrecer recomendaciones basadas en los hallazgos está transformando la forma en que las organizaciones perciben los GSOC. La reducción de riesgos es el principal objetivo del uso de este tipo de tecnología.

¿Cuáles son algunos de los desafíos a los que se enfrenta un GSOC moderno?

Si bien los GSOC se enfrentan a retos relacionados con los recursos, como la falta de personal de vigilancia, la alta rotación de personal y las elevadas tasas de *burnout* (síndrome del trabajador agotado), también existe una cantidad abrumadora de datos entrantes que dificulta identificar lo que es importante. Para muchos GSOC, no ha sido un problema generar datos, lo que sí ha sido un verdadero desafío es la capacidad de analizar los datos entrantes y convertirlos en información útil para las partes interesadas pertinentes. En concreto, es un reto utilizar esos datos para demostrar el retorno de la inversión (ROI) del capital gastado en seguridad, así como demostrar que el programa de seguridad de una empresa es beneficioso y no solo un centro de costos.

A medida que los operadores aprovechen plataformas más inteligentes para agregar flujos de datos que ingresan al GSOC, el resultado será una mejor comprensión de los puntos débiles dentro de un programa de seguridad, mejores tiempos de respuesta, así como la reducción del ruido y de falsas alarmas, lo que, en última instancia, puede abordar algunas de las causas del *burnout*.