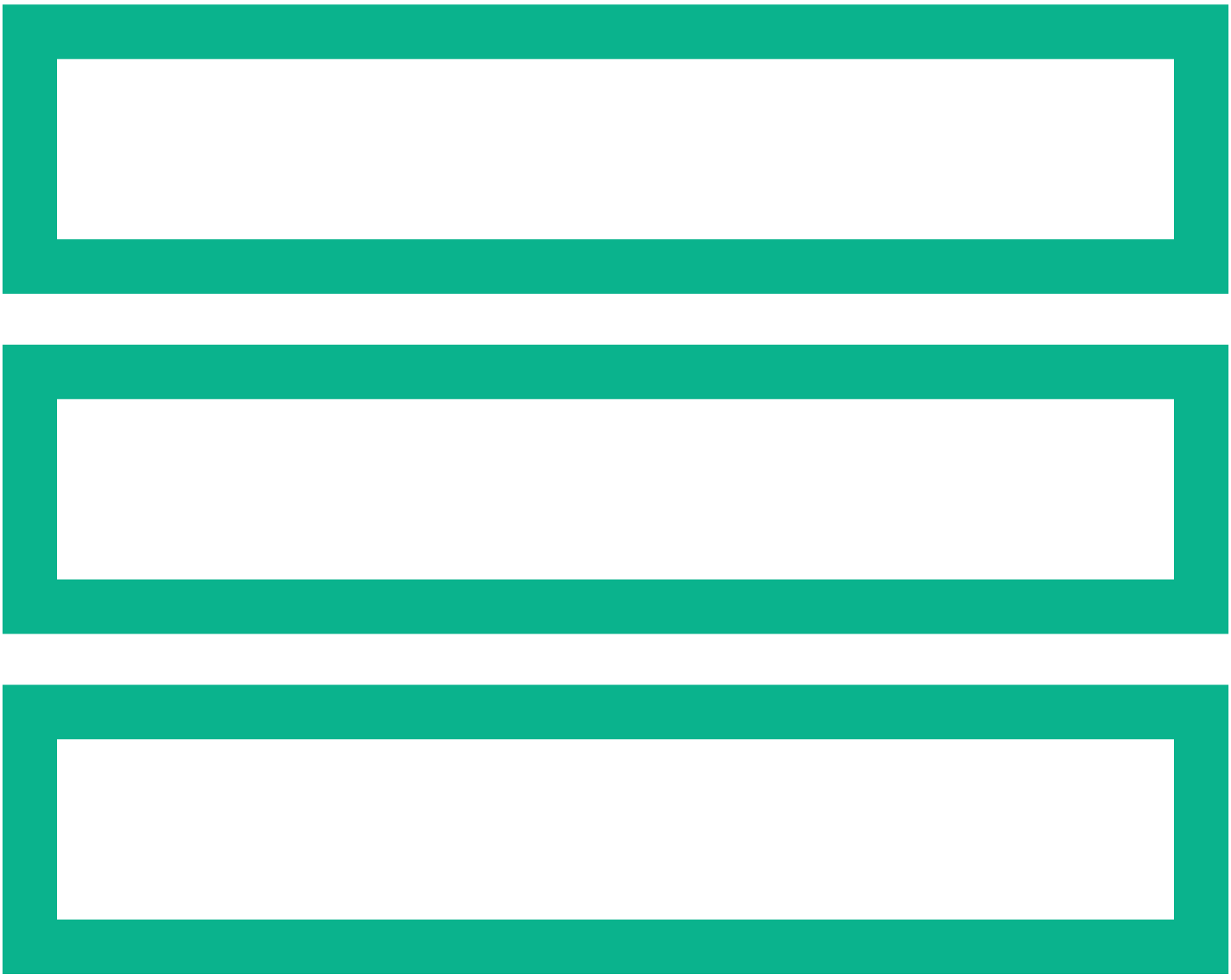
Hewlett Packard Enterprise

Estado de operaciones de seguridad

Informe de 2017 sobre las capacidades y la madurez de las organizaciones de defensa cibernética



Índice

Me complace compartir nuestras conclusiones en este cuarto informe anual sobre el estado de las operaciones de seguridad. Habiendo presenciado cómo crecieron y maduraron las organizaciones de defensa cibernética en los últimos 20 años, puedo decir que estos son tiempos interesantes. Nunca ha habido una mayor conexión entre las iniciativas de seguridad y las metas de negocios. La velocidad a la que las nuevas organizaciones adoptan las innovaciones como la nube, la IoT y las grandes plataformas de datos compite sin tregua con el avance de los atacantes. La sofisticación, la agilidad y la magnitud de los ataques convirtieron a la velocidad en algo imperativo para el éxito de cualquier centro de operaciones de seguridad y ha dado lugar a un enfoque renovado de la automatización, la detección en tiempo real y la respuesta a escala.

Junto con este enfoque, continuamos viendo una lucha para encontrar y mantener los recursos especializados necesarios para ejecutar las operaciones de seguridad. Para aliviar esta carga se han utilizado la automatización y la subcontratación con distintos grados de éxito, como se puede ver en el informe. A lo largo de nuestras evaluaciones, realizadas en los 6 continentes, hemos visto diversas personas de SOC, procesos y configuraciones de tecnología. Nuestros datos nos ofrecen una visión más eficaz de las configuraciones, además de reflexiones sobre las oportunidades y limitaciones de la automatización y la subcontratación.

En este año también se ha experimentado un fuerte descenso en la madurez de las organizaciones que han optado por quedarse fuera del monitoreo en tiempo real en favor de las tecnologías de búsqueda post-evento. Si bien esta es una tendencia preocupante, las organizaciones que han adoptado capacidades de «hunt team» (equipo de búsqueda) como un complemento de sus actuales programas de monitoreo en tiempo real han tenido éxito en la detección rápida de problemas de configuración, infecciones de malware detectadas anteriormente e identificación de ataque SWIFT. Esta información ayudará a la industria a comprender realmente qué funciona y qué no, con análisis de datos de seguridad y capacidades de búsqueda.

Mientras esperamos el próximo año, vemos que habrá grandes retos: una mayor adopción del nuevo estilo de TI, que se adhiere a la nueva normativa como GDPR, un aumento de los ataques motivados políticamente y mucho más. Reafirmo la creencia de que la mejor defensa de las organizaciones será mantenerse firmes con sus bases de operaciones de seguridad. ***Concéntrese en las personas****. Las personas van a impulsar el proceso y este garantizará el uso más eficaz de las tecnologías. Destáquese en los aspectos básicos y mejore las capacidades de análisis para descubrir ataques avanzados con mayor visibilidad en toda la organización, proporcionando la confianza para que su empresa innove de manera segura.*

Matthew Shriner
Vicepresidente de Servicios profesionales, HPE Security

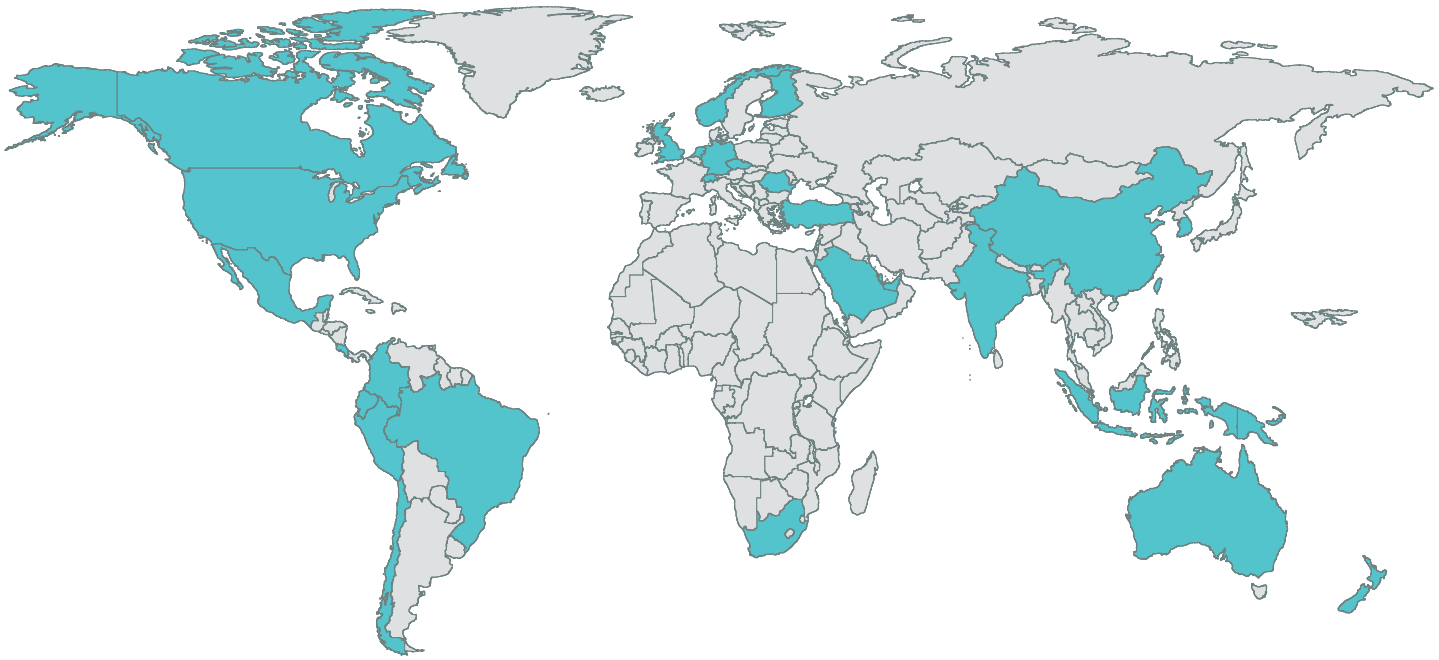
Resumen ejecutivo

Diversas organizaciones de todo el mundo están invirtiendo fuertemente en capacidades de defensa cibernética para proteger sus activos más importantes. Ya sea proteger la marca, el capital intelectual y la información de los clientes o proporcionar controles para la infraestructura crítica, los medios de detección y respuesta a incidentes para proteger los intereses de la organización tienen elementos comunes: las personas, los procesos y la tecnología.

La madurez de estos elementos varía enormemente entre organizaciones e industrias. En este cuarto informe anual sobre el estado de las operaciones de seguridad, Hewlett Packard Enterprise proporciona actualizaciones de las capacidades actuales y emergentes, mejores prácticas y niveles de rendimiento de las operaciones de seguridad extraídos de evaluaciones realizadas en todo el mundo.

Con más de una década de experiencia en el suministro de la tecnología y los servicios de seguridad informáticos que se encuentran en el núcleo de los programas de defensa cibernética y SOC empresariales más avanzados del mundo, HPE ha trabajado con más equipos de defensa cibernética líderes a nivel mundial que cualquier otra organización y está singularmente calificado para publicar el presente informe.

Desde 2008, HPE Security Intelligence and Operations Consulting (SIOC) ha evaluado la capacidad y madurez de 137 SOC discretos a través de 183 evaluaciones en profundidad. Las evaluaciones de madurez incluyen organizaciones de los sectores público y privado, empresas de todos los sectores verticales de la industria y proveedores de servicios de seguridad gestionada. Geográficamente, estas evaluaciones incluyen SOC localizadas en 31 países de los seis continentes en 9 regiones. Este es el mayor conjunto de datos disponible para sacar conclusiones sobre el estado de la defensa cibernética y operaciones de seguridad empresarial en todo el mundo.



En los últimos cinco años, Hewlett Packard Enterprise ha encontrado que el 26,61 % de las organizaciones de defensa cibernética que fueron evaluadas no ha podido lograr un modelo de madurez de operaciones de seguridad (SOMM) de nivel 1, una reducción del 1 % con respecto al año pasado y una disminución por segundo año consecutivo. Estas organizaciones operan de manera ad hoc con procesos de indocumentados y lagunas importantes en la gestión de riesgos y seguridad.

Sin embargo, tras las evaluaciones realizadas este año, hemos encontrado que durante los últimos 5 años el 18 % de las organizaciones evaluadas cumplen con los objetivos del negocio y están trabajando hacia o han alcanzado los niveles de madurez recomendados, es decir un 3 % más que los resultados del año anterior y un 5 % de mejora en 2 años.

Las evaluaciones han mostrado algunas tendencias interesantes:

- La coherencia de la misión, la tecnología, la gerencia y el personal tiene un fuerte efecto sobre la madurez de las organizaciones de defensa cibernética. Los equipos con baja rotación, sólida alineación con el negocio y que siguen los planes multianuales tienden a tener mayores capacidades, así como también madurez general.
- Las organizaciones continúan probando diversos modelos para crear operaciones del tamaño adecuado, que incluyen la asociación con proveedores de servicios o la subcontratación para funciones o roles específicos (como vigilancia de nivel 1). Esto proporciona resultados dispares y a menudo el resolver un reto crea otros nuevos.
- Se están adoptando rápidamente equipos de búsqueda que realicen análisis de registros históricos (en contraposición al análisis en tiempo real). HPE descubrió que se emplea una gran cantidad de tiempo y esfuerzo en higiene de datos, contextualización y preparación antes de que estos equipos de búsqueda puedan distinguir las verdaderas amenazas de una infinidad de sistemas mal configurados y deficiencias de procesos en la gestión de los recursos de TI.
- El aumento de los niveles de flujo de trabajo y la automatización de procesos permite a las organizaciones mejorar la coherencia, el ancho de banda y la velocidad de las operaciones. Muchas organizaciones están invirtiendo en investigación de los incidentes de seguridad y herramientas de gestión. La implementación deliberada y diligente de estas capacidades, así como también la gestión adecuada, han arrojado resultados positivos.

La distribución desigual de los resultados de madurez en las diferentes industrias puede relacionarse directamente con la experiencia del impacto financiero negativo frente a ataques malintencionados. Las organizaciones que han experimentado una pérdida financiera directa debido a ataques maliciosos son más eficaces al realizar una maduración inmediata a un nivel superior.**Este grupo de empresas sigue creciendo considerablemente en número.**

Resumen de resultados

Disminuyó la madurez con los programas de solo búsqueda
La proliferación de programas de búsqueda de amenazas es una tendencia constante para las organizaciones de operaciones de seguridad en 2016.

La adopción generalizada de las implementaciones de lago de datos (data lake) utilizando software de código abierto y hardware básico ha proporcionado las soluciones de retención y recuperación de datos necesarios para apoyar las operaciones de búsqueda. Las organizaciones han competido para implementar herramientas de análisis de seguridad con el fin de aprovechar estos almacenes de datos, esperando que emerja de ellos información útil. Si bien a menudo estas herramientas descubren varios patrones e indicadores interesantes, a veces estas carecen de contexto significativo y requieren una investigación más amplia. En los programas de búsqueda actuales, la mayoría de las investigaciones apuntan a revelar problemas en la recopilación de datos o aplicaciones y sistemas mal configurados.

hpe.com/software/huntingtoday

En algunos casos, las organizaciones han llegado a optar por la búsqueda abierta como el único medio para la detección y respuesta y han eliminado los esfuerzos de monitoreo en tiempo real basados en SIEM. Muchas de estas organizaciones se vieron frustradas debido operaciones de seguridad que eran difíciles para el personal y no producían el valor esperado y, por lo tanto, decidieron probar algo nuevo. ¿El resultado? Más de lo mismo. Búsquedas que devuelven datos de aplicaciones y sistemas mal configurados, pero no mucho en términos de resultados útiles acerca de las amenazas a la organización. La madurez de estas organizaciones en realidad retrocedió y los riesgos aumentaron, mientras que la respuesta a amenazas poco conocidas se ralentizó y disminuyó la consistencia. En la mayoría de los casos se perdió el contexto operacional de la solución anterior en la transición a un nuevo enfoque.

Si bien la mayoría de las organizaciones que se encuentran en la fase de adopción temprana de esta área emergente de las operaciones de seguridad están experimentando resultados dispares, hay algunas que han incorporado correctamente la capacidad de búsqueda de amenazas a sus programas de seguridad en formas complementarias a las actuales operaciones en tiempo real. HPE está trabajando con organizaciones que han aprovechado las metodologías maduras que llevaron el éxito a sus programas del centro de operaciones de seguridad (SOC) y expandió estas lecciones aprendidas a la búsqueda de amenazas.

Desarrollo de centros de fusión

El desarrollo de centros de fusión de seguridad (centros de intercambio de información interna) es una tendencia emergente para muchas organizaciones de operaciones de seguridad de grandes empresas y del sector público en 2016.

El desafío común descrito por estas organizaciones es la incapacidad para ver la imagen completa del riesgo y la seguridad de sus actuales entornos de SOC repartidos en varias regiones y líneas de negocio. Simplemente hay tantas aplicaciones, datos, sistemas y usuarios dentro de grupos funcionales que las organizaciones tienen problemas al consolidar la información necesaria para tomar decisiones de riesgo eficaces. Las grandes organizaciones han intentado manejar este desafío empleando más personas o más soluciones de tecnología.

Sin embargo, la mayoría de las organizaciones terminan o bien implementando herramientas que requieren apoyo y generan más volumen, o terminan sin el conocimiento humano para apoyar el entorno. En muchas de estas organizaciones en silos surgen operaciones de seguridad que representan las unidades de negocios, una empresa, un departamento u otras divisiones lógicas dentro de la organización, cada una con diferentes grados de madurez mientras y que proporciona visibilidad de una porción del negocio, pero no de la organización principal en su totalidad.

Las organizaciones que mejor han superado estos desafíos han adoptado un modelo de organización que designa o crea un SOC como centro de fusión de toda la organización. Estos centros de fusión ofrecen gobernanza de procesos, intercambio de información y conocimientos sobre seguridad que permiten a cada suscriptor del SOC colaborar mejor o replegarse y convertirse en clientes funcionales de uno de los SOC que esté en una etapa más madura de servicio. Las grandes empresas que utilizan este enfoque suelen observar un beneficio global de las economías de escala y una mejor coordinación de un conjunto reducido de procesos comunes, el uso de soluciones de tecnología comunes y la utilización de métricas comunes desde un centro de fusión.

Prestación de indicadores empresariales eficaces

Los centros de operaciones de seguridad continúan su lucha por el desarrollo de métricas que comuniquen una efectiva contribución empresarial.

La mayoría de los centros de operaciones de seguridad desarrollan paquetes de métricas que informan atributos tecnológicos como sistema de salud, nivel de políticas y desempeño funcional. ¿Cómo demuestran estos indicadores una reducción del riesgo, un incremento de la seguridad o la satisfacción de los objetivos de cumplimiento? Los parámetros enumerados son fundamentales para los responsables de la gestión de la tecnología, pero aportan poco valor a las partes interesadas que buscan lograr un resultado de negocios.

Los principales SOC van más allá de informar los datos de rendimiento funcional básicos e implementar programas de métricas centrados en la medición de las actividades operacionales vinculadas directamente a las prioridades de la empresa y comunicadas en términos de negocios. Estas métricas comunican la seguridad a un menor costo total directo, indirecto y de oportunidad a lo largo del tiempo. Las actividades diarias como ajuste de directivas, optimización del rendimiento, personalización contextual y automatización de respuesta se informan junto con sus repercusiones inmediatas y de tendencias para la organización.

Intentos de transferir el riesgo con servicios gestionados

Sin una gestión adecuada de los proveedores de servicios, las organizaciones que buscan transferir el riesgo migrando a un modelo de servicio gestionado experimentan una disminución en la eficacia de las operaciones de seguridad a lo largo del tiempo.

A través de la externalización, las organizaciones pueden recibir una reducción del costo y un aumento inmediato en la madurez de los procesos operativos y tecnológicos, especialmente en los casos en que esta capacidad no existe todavía. Sin embargo, al entregar por completo la solución a un proveedor que no conoce las operaciones diarias y el cambio dentro de la organización, se produce una erosión progresiva en el valor de negocio de las soluciones de seguridad subcontratadas que da lugar a lagunas al gestionar el riesgo, la seguridad y los objetivos de cumplimiento.

Después de un período prolongado de subcontratación, las organizaciones suelen terminar con sus soluciones de seguridad gestionadas más de acuerdo con los contratos de nivel de servicio convenidos que con un contexto organizacional útil. Los prestadores asumen la responsabilidad diaria de aplicar de manera proactiva las políticas actualizadas del proveedor, actualizar el firmware, realizar un seguimiento del tiempo de actividad y la disponibilidad e informar las métricas de rendimiento de la tecnología, sin embargo, estas actividades no producen un aumento de los niveles de madurez sin las interacciones recurrentes de los clientes y las revisiones frecuentes necesarias para mantener el valor de la solución.

Además, la subcontratación de la gestión de la solución a un proveedor a menudo se considera erróneamente como equivalente a transferir el riesgo de los negocios al prestador de servicios. Este no es el caso. Los prestadores de servicios se aseguran de que las organizaciones individuales sigan siendo responsables de gestionar su propio riesgo empresarial global mediante la definición de servicios con parámetros estrictos y asumiendo una responsabilidad limitada basada en el alcance del servicio. Las organizaciones que necesitan aumentar la capacidad de seguridad pero no pueden añadir personal deben considerar la posibilidad de adoptar una estrategia de solución de personal u operacional híbrida para las operaciones de seguridad.

Aumento de la capacidad a través de soluciones híbridas

Las organizaciones que emplean un enfoque híbrido para soluciones de servicios gestionados tienen más probabilidades de mantener y mejorar la madurez a lo largo del tiempo.

Las soluciones híbridas combinan la capacidad operativa de un proveedor de servicios con una capacidad de operaciones de seguridad interna centrada en generar valor a partir de los controles de seguridad total implementados para proteger el negocio. Esto puede incluir gestión de la tecnología, monitoreo de ojos en la pantalla, intercambio de operaciones autoaprovisionadas y otros varios modelos que hacen que las organizaciones y los prestadores de servicios colaboren estrechamente.

El éxito de la subcontratación requiere que las organizaciones mantengan algunas capacidades operativas autoaprovisionadas para asegurarse algunas cosas. En primer lugar, la capacidad operativa interna es capaz de realizar la diligencia que se necesita para gestionar adecuadamente los riesgos En segundo lugar, las organizaciones mantienen un actor interno que saca el máximo provecho de lo que el proveedor tiene para ofrecer, y que es capaz de coordinar rápidamente las actividades relacionadas con la respuesta ante incidentes basándose en su familiaridad con el entorno. Por último, y quizás la más importante de todas, las organizaciones mantienen un funcionamiento interno en el que recae el éxito de la organización y desarrolla una canalización del talento en la que la organización puede confiar para los años venideros.

Las relaciones de servicio exitosas van más allá de la gestión de proveedores para los acuerdos de nivel de servicio estándares de la industria. Exigen transparencia de servicio e interacciones que permiten que los líderes de seguridad puedan evaluar el rendimiento del servicio rápidamente a través de los principales indicadores de rendimiento establecidos, los que garantizan que las consideraciones financieras y de riesgo que llevaron a la subcontratación en un principio se sigan cumpliendo. Los proveedores de servicios pueden ser integrales para el éxito de una organización cuando existe una base sólida de procesos que garantiza que los principales atributos de la organización estén constantemente integrados en el servicio gestionado y sean medidos y optimizados para cumplir con los objetivos de esta. Todos estos factores, trabajando en conjunto, dan como resultado operaciones híbridas eficaces cuya madurez se puede medir a lo largo del tiempo.

Public Sector SOC StrugglesLuchas de los SOC del sector público

Las organizaciones de los SOC del sector público luchan mucho para crecer más allá de su nivel de madurez gestionado.

Estar en una etapa de madurez gestionada en sí misma no es algo malo. Generalmente significa que los SOC del sector público han planeado y ejecutado la aplicación de un SOC en conformidad con una política, decreto, ley o estatuto basándose en la misión de la organización matriz; estos SOC emplean a personas calificadas con recursos suficientes para producir resultados predecibles. Hay un alto grado de repetibilidad y los actores pertinentes están involucrados en las operaciones. Todos estos son atributos positivos.

Sin embargo, desafíos aumentan rápidamente debido a las deficiencias en estas tres áreas: expectativas no alineadas, falta de continuidad del personal y roles y responsabilidades organizacionales rígidos. De manera similar a muchas organizaciones que utilizan servicios gestionados, los líderes del sector público dependen en gran medida de proveedores externos y suponen erróneamente que el empleo de un proveedor es equivalente a transferir el riesgo. La mayoría de las veces este no es el caso. Los líderes del sector público siguen siendo responsables de garantizar que la seguridad de las operaciones desplegadas cumpla con el objetivo global de la organización. El proveedor puede ser un asesor de confianza, pero un sólido programa de métricas debe demostrar con éxito operaciones de seguridad y no simplemente una plantilla de personal básica y repetibilidad.

Nivel de Somm	Calificación	Descripción
Nivel 0	Incompleto	No existen elementos operacionales
Nivel 1	Inicial	Ad-hoc
Nivel 2	Gestionado	Repetible
Nivel 3	**Definido**	**evaluado subjetivamente***
Nivel 4	**Medido**	**evaluado cuantitativa-mente****
Nivel 5	Optimización	Rígido, redundante

Consulte el Apéndice para obtener una descripción completa de cada nivel

* Objetivo para el sector comercial y público

** Objetivo para los proveedores de servicio

Los SOC del sector público son muy explotados y por eso el personal del proveedor que se desempeña en roles clave tiende a sufrir un recambio constante. Las organizaciones invierten en actividades de formación y desarrollo, sin embargo, generalmente la movilidad ascendente de la carrera es limitada para los miembros del equipo en base al alcance establecido por el contrato con el proveedor externo. Y sin la capacidad de ascender dentro de la organización, los profesionales de seguridad capaces que han sido contratados buscarán oportunidades de crecimiento e influencia por fuera de ella. Los que quedan generalmente sufren una deficiencia de cobertura operacional hasta que se soluciona la falta de personal, lo que causa que los SOC del sector público SOC sufran un estancamiento en la aparición de iniciativas y el aumento de su madurez.

HPE ha observado también un efecto adverso en los roles y responsabilidades organizativos rígidos dentro de los SOC del sector público. El reconocimiento del alcance de cada equipo, el rango de los individuos involucrados o los protocolos de comunicación para hacer las cosas influye significativamente en las interacciones y la prontitud de la respuesta a eventos que implican riesgos, seguridad y prioridades de cumplimiento. Esto se traduce en una menor madurez y menor valor en soluciones de seguridad para la organización. Los líderes de estos SOC suelen ver a los procesos como una carga incómoda en lugar de ser un agente de cambio eficaz que permite a los profesionales de la seguridad proteger a la organización contra las amenazas emergentes.

Los SOC del sector público efectivos se benefician mucho con el liderazgo operacional aprovisionado internamente que proporciona supervisión y mide el éxito en términos de reducción del riesgo, mejora de la seguridad mejorada o cumplimiento satisfactorio. Estos interlocutores internos ayudan a los proveedores de servicios contratados a navegar estructuras organizativas complejas y permitir que el cambio se produzca de una manera oportuna, con la consiguiente optimización de las soluciones de seguridad que la organización ha implementado. La continuidad en el liderazgo puede superar algo de la rotación de personal esperable en una relación con un proveedor. HPE ha observado que cuando los líderes internos son eficaces para derribar muros, esto a menudo produce mayores tasas de retención del personal y la capacidad de concentrarse en los proyectos e iniciativas que hacen a la organización más madura con el tiempo.

Herramientas comerciales vs. código abierto en operaciones de seguridad

En 2016 algunos centros de operaciones de seguridad han aumentado su dependencia en las herramientas de código abierto. Esta estrategia puede añadir capacidad o reducir el gasto en licencias de software durante ese ciclo presupuestario, pero rara vez estas soluciones son implementadas con el nivel de apoyo, documentación y métricas que aseguran que el riesgo, la seguridad o los objetivos de cumplimiento de la organización sean sostenibles.

Muchas de las herramientas de código abierto y los recursos comunitarios disponibles para operaciones de seguridad requieren un grado de personalización y mantenimiento continuo que las organizaciones deben evaluar cuidadosamente. A través de nuestras evaluaciones durante los últimos ocho años HPE ha observado que el liderazgo de seguridad se recambia en promedio cada 18 meses, y algunos funcionarios lo hacen aún más rápidamente. Las transiciones del personal a esta velocidad pueden afectar negativamente la compatibilidad y la sostenibilidad de las soluciones patentadas y altamente personalizados y, en última instancia, la efectividad y madurez del SOC. HPE ha observado que esta migración al código abierto entorpece sistemáticamente a las organizaciones, donde la mayoría de los programas se deterioran y colapsan luego de la partida del personal que estaba íntimamente familiarizados con las soluciones personalizadas.

La mayoría de las organizaciones no descubre esta brecha hasta después de un evento adverso que le cuesta una cantidad considerable de recursos. Ciertamente hay lugar para herramientas personalizadas en SecOps, donde las aplicaciones comerciales se quedan cortas. Los líderes simplemente deben evaluar su estrategia de seguridad y determinar si el costo operacional de mantener estos sistemas produce un valor significativo y ventajas sobre el proveedor de soluciones compatibles.

Automatización y eliminación de analistas de nivel básico

Varias organizaciones están considerando la eliminación de la detección de primera línea y los analistas de respuesta y, en lugar de ello, optan por la automatización para abordar las nuevas amenazas para la organización. Dada la escasez de talentos en seguridad, este enfoque está en consonancia con una serie de líderes en seguridad. La realidad de cómo se desarrolla esto no es tan obvia o tan beneficiosa como suena.

Rara vez se concreta el nivel de automatización que la mayoría de las organizaciones prevé. La verdadera detección y respuesta automatizada, no solo aumentó la recopilación de datos, requiere un alto grado de fiabilidad y de precisión en la configuración de la gestión de los datos. Esto parece ser un área donde la mayoría de las organizaciones verdaderamente sufren en términos de madurez, con información acerca de las aplicaciones, usuarios, sistemas y datos que residen en distintos repositorios o no están disponibles en absoluto. La automatización puede ser posible en segmentos de una red pequeños, estáticos o altamente controlados, pero en la mayoría de las organizaciones el riesgo de romper algo que no está bien documentado y es muy importante para la organización es un elemento disuasorio suficiente para impedir que la automatización eficaz siquiera se implemente.

Desanimados debido a que su último objetivo de automatización no pudo realizarse, la mayoría de los líderes de seguridad se vuelcan hacia otra práctica de determinación de prioridades ineficaz: la generación de tickets automatizada. Este enfoque no siempre es malo. Cuando los indicadores de ataque son atómicas o computados, este nivel de automatización tiene sentido. Los resultados de estos indicadores son viables o no y aquellos que tienen un alto grado de fidelidad y son aplicables deben avanzar hacia el próximo paso en el proceso de respuesta a incidentes. Sin embargo, al tratar con el comportamiento de un actor de amenazas avanzado y campañas coordinadas que se extienden en el tiempo, este enfoque transforma al analista en un respondedor miope.

HPE ha evaluado sistemáticamente las organizaciones donde el marco de tiempo correlativo que resultó en un ticket automático no fue lo suficientemente largo como para capturar la verdadera intención y las acciones del actor de la amenaza. La creación de un ticket influye en la mentalidad analítica del analista que responde y su comportamiento se altera para buscar la conclusión más rápida. Este nivel de automatización produce dos resultados adversos observados en la mayoría de las organizaciones que los emplean: mayores costos de determinación de prioridades y respuesta basados en la interrupción del proceso analítico. Se les recomienda a las organizaciones que están considerando la eliminación de los analistas de primera línea debido a una incapacidad de atraer o retener talentos que revisen las publicación **Cultivo de un analista de seguridad** y la subsiguiente **Operaciones de seguridad inteligente: Una guía sobre el personal.**

Conclusiones adicionales

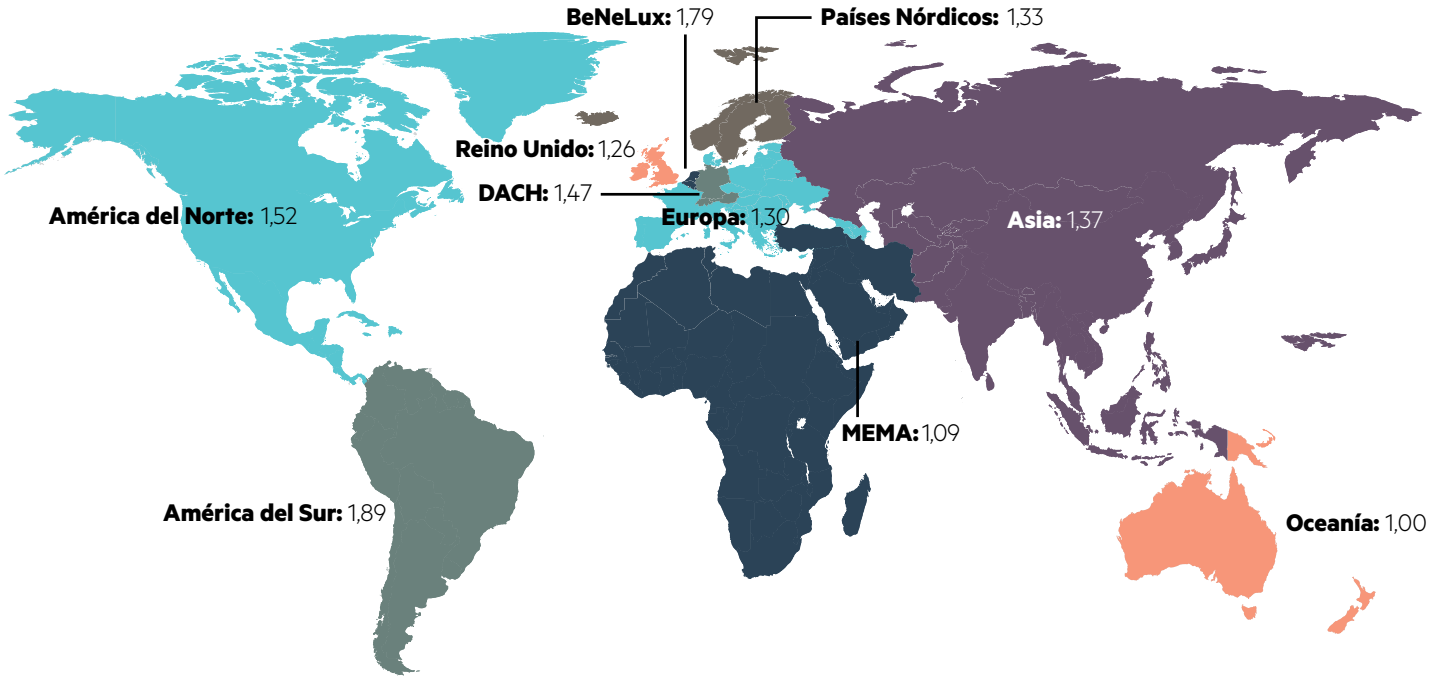
Las evaluaciones de Hewlett Packard Enterprise a organizaciones de todo el mundo continúan mostrando que el nivel de madurez promedio de los equipos de defensa cibernética sigue muy por debajo de los niveles óptimos. Muchas de las conclusiones y observaciones del anterior informe Estado de las operaciones de seguridad (**ssl.www8.hp.com/us/en/ssl/leadgen/secure_document.html?objid=4AA6-3593ENW&siebelid=560013401**) son todavía válidas. Además, se obtuvieron las siguientes observaciones y conclusiones a lo largo de este último año de evaluación:

- Los SOC están gastando una gran parte de su tiempo en identificar problemas de configuración. Idealmente, estos problemas podrían ser gestionadas por un equipo de TI liberando la organización de operaciones de seguridad para que se centre en identificar e investigar los ataques.
- La mayoría de los SOC son heterogéneos, admiten múltiples tecnologías del proveedor y la proliferación de la automatización y las herramientas. La visibilidad y amplitud de estos SOC es una ventaja porque pueden reunir las mejores características de cada solución de tecnología implementada aunque también puede ser engorroso cuando estos deben realizar el trabajo de integración por sí mismos.

- La Regulación de protección de datos de la Unión Europea (GDPR) está en el radar de las organizaciones con una fecha límite de cumplimiento que es mayo 2018, sin embargo, las organizaciones aún no han implementado los cambios necesarios. Además de otros requisitos, la obligación de detectar e informar a los ciudadanos de la UE acerca de los datos personales compromisos dentro de las 72 horas impulsará la detección de nuevos SOC y casos de uso de respuesta e investigación de cumplimiento en todo el mundo.
- Los malware y ransomware destructivos han exigido unos vínculos más estrechos entre el SOC y la recuperación de desastres y los equipos de continuidad de los negocios.
- El recambio y los problemas de personal siguen azotando a la industria. A través de las entrevistas realizadas durante nuestras evaluaciones de madurez encontramos que el problema número uno frente a las organizaciones de operaciones de seguridad sigue siendo la identificación y retención de los recursos humanos necesarios para el funcionamiento de la empresa. A menudo, la dotación de personal óptima no es alcanzable y no se pueden alcanzar los perfiles de habilidades requeridos.
- Los esfuerzos para converger y optimizar las funciones, herramientas y recursos entre operaciones de seguridad y operaciones de TI continúan. Las mejores prácticas todavía prescriben grupos funcionales separados, sin embargo, es posible e incluso necesario trabajar en estrecha colaboración y con un nivel de convergencia.

Tendencias regionales

Sólo hay pequeñas diferencias en madurez y capacidades regionales en todo el mundo. Mientras que los SOC de América del Norte en general han experimentado puntuaciones de SOMM ligeramente mayores, el acceso de los SIOC de HPE a nuevas organizaciones de proveedores de servicio en América del Sur ha producido una maduración en esa región en el año pasado. Esto se debe a un aumento en la inversión en las áreas de monitoreo de seguridad, operaciones, servicios gestionados y automatización. La región MEMA (Oriente Medio, Mediterráneo y África) registró un incremento significativo en las puntuaciones SOMM en comparación con el año pasado con inversiones de diferentes organizaciones de los sectores comercial y público en las personas y los procesos de sus programas de seguridad. Asia y DACH registraron un ligero descenso con la entrada de nuevos participantes en el espacio en 2016. El resto de Europa (BeNeLux, los países nórdicos y Reino Unido) se mantuvo estable en 2016, con pocos ingresantes en el espacio.



Tamaño de la empresa vs. madurez

HPE no observa una relación directa entre el tamaño de la organización y la madurez operativa en las organizaciones comerciales y del sector público. Si bien hay grandes organizaciones en o cerca de la cima, una investigación de las organizaciones de menor rendimiento muestra a algunas de las grandes multinacionales que simplemente no han priorizado las operaciones de seguridad. La asignación del presupuesto de TI y de seguridad para proteger los ingresos presupuestarios, la privacidad, la infraestructura crítica, la cuota de mercado, la seguridad y el capital intelectual es importante cuando hay mucho que perder. A pesar de tener acceso a importantes recursos, esas organizaciones no son más maduras. La seguridad como un factor diferenciador de la competencia, su liderazgo en el mercado y la alineación con el sector son mejores predictores de madurez según nuestros datos.

Promedios de la industria

Mirando las puntuaciones promedio en la vertical de la industria, vemos que las organizaciones de servicios han tenido los más altos puntuaciones de SOMM durante los últimos cinco años. Este es un cambio con respecto a los 2 años anteriores en los cuales los SOC en la vertical de tecnología lideraban todas las organizaciones. Como industria, las organizaciones de servicios demuestran una fuerte inversión en la alineación con el negocio y las dimensiones de las personas del SOMM durante los últimos 5 años, lo que produjo su surgimiento por sobre otras verticales que todavía están centradas principalmente en sus implementaciones de tecnología. Durante los últimos cinco años, Hewlett Packard Enterprise (en ese momento HP) ha continuado viendo el bajo rendimiento de las organizaciones de la industria de telecomunicaciones. Mientras el equipo investigaba la tendencia multianual en telecomunicaciones, señaló que las nuevas organizaciones de telecomunicaciones que ingresaban en el mercado de defensa cibernética en las economías en desarrollo a través de una nueva oferta de servicios gestionados deberían mejorar a medida que formalizaran la inversión en estos programas.

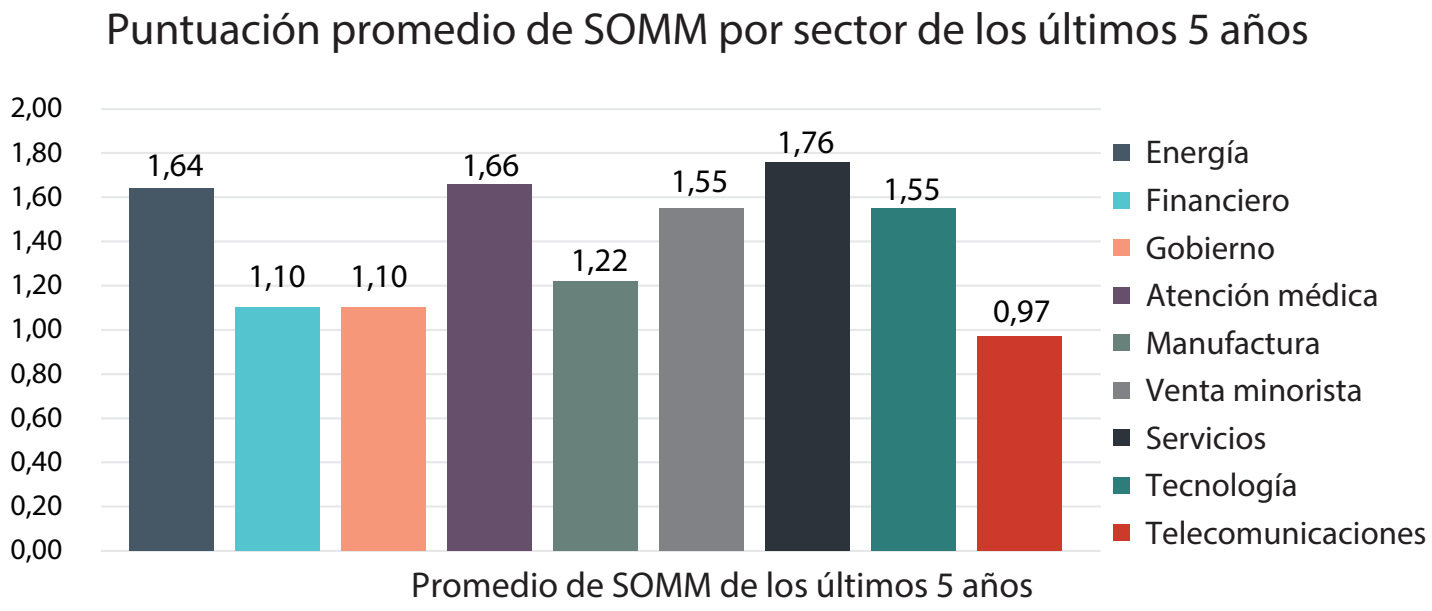


Figura 1. Puntuación promedio de SOMM por industria, últimos cinco años

- Las compañías de **asistencia médica** se han convertido en un objetivo preferido del ransomware debido a los datos sensibles al tiempo que dirigen su actividad. Es imprescindible una estrecha colaboración con los equipos de recuperación de desastres y copia de seguridad para reducir la ventana de aprovechamiento de estos ataques.
- Las organizaciones de **gobierno** luchan con la madurez a largo plazo. Los contratos de longitud fija para la unidad de recursos externalizados utilizan métricas basadas en la dotación de personal en lugar de la madurez y eficacia.
- Las instituciones **financieras** han sufrido grandes ataques a través de Society for Worldwide Interbank Financial Telecommunication (SWIFT). Las organizaciones que monitorean los indicadores específicos de compromiso (IoCs) para estos tipos de ataques han sido más eficaces al reducir el riesgo.
- Las empresas de **energía** han incrementado la vigilancia de sistemas de control físico, SCADA e industrial para combatir la creciente amenaza de ataques a la infraestructura. La supervisión en tiempo real ha demostrado ser más eficaz en la identificación de estos ataques para una rápida corrección.
- Las compañías de **telecomunicaciones** generalmente se preocupan por la disponibilidad del servicio. Las organizaciones que se han expandido a servicios administrados y seguridad como un diferenciador competitivo han demostrado mayor madurez.

Incluso con el aumento de la normativa para las industrias del sector financiero y minorista, la puntuación promedio está por debajo del nivel "administrado" (2) y muy por debajo del nivel recomendado de "Definido" (3)*. Analizando más profundamente, la mayoría de las verticales de la industria son ahora más fuertes en la categoría negocios. Este es un cambio con respecto a años anteriores en los que las organizaciones generalmente tenían un exceso de inversión en tecnología. La mayoría de las industrias son más débiles cuando se trata de la categoría de proceso. Es en los procesos donde la mayoría de los SOC deberían esforzarse por desempeñarse mejor ya que aquellas organizaciones que lo hacen obtienen más valor de sus soluciones de personas y tecnología.

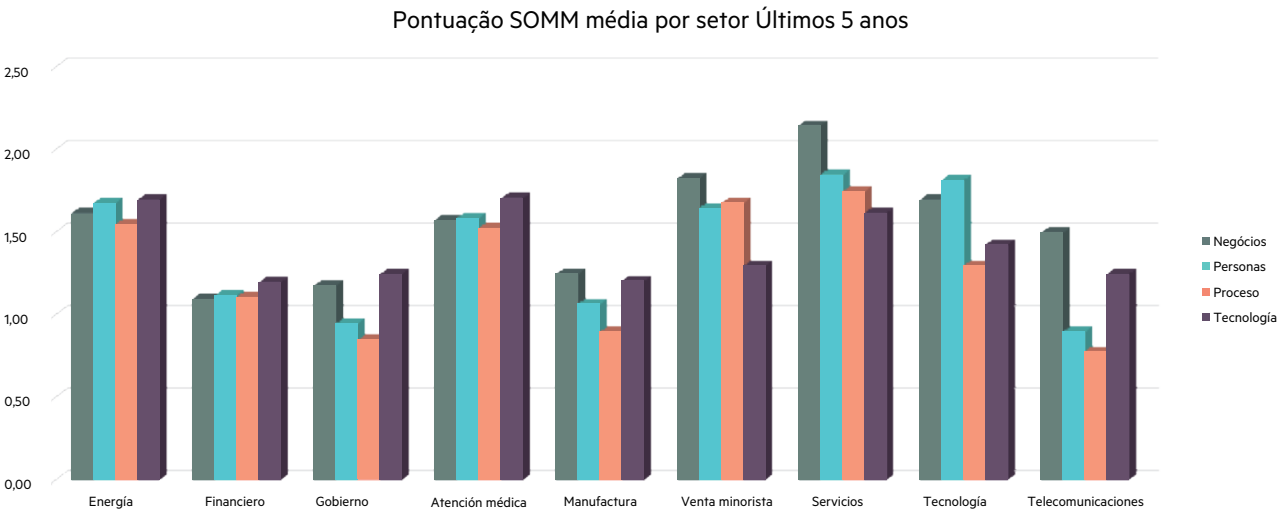


Figura 2: Puntuación promedio de SOMM por industria de los últimos 5 años

* Consulte el Apéndice para obtener una descripción completa de cada nivel

Resultados de categorías

Los cuatro elementos de la capacidad de operaciones de seguridad se pueden subdividir en categorías de evaluación que se utilizan en las evaluaciones de madurez de HPE.

Promedios de categorías

En el transcurso de ocho años, Hewlett Packard Enterprise ha realizado evaluaciones de madurez en 183 SOC alrededor del mundo. Este conjunto de datos le permite a Hewlett Packard Enterprise sacar conclusiones acerca de la madurez global de los programas de defensa cibernética instalados en las empresas más grandes del mundo.

En cada una de las áreas medidas, la puntuación promedio de la industria sigue estando entre 1 y 2. Por segundo año consecutivo, el área del SOMM empresarial produjo la mayor puntuación media de 1,52. Esto es coherente con el rápido crecimiento de la seguridad dentro de las organizaciones que hemos visto en los últimos años y refleja el impacto que esto tiene en todo el negocio, no solo en una organización de TI.

La tecnología permanece fuerte con la segunda puntuación de SOMM, con una promedio de 1,40. La tecnología tradicionalmente ha obtenido las puntuaciones más altas porque las tareas de implementación de ingeniería y tecnología son generalmente el foco en la mayoría de las organizaciones de seguridad empresarial. La madurez empresarial ha aumentado significativamente en los últimos tres años debido a la mayor concientización sobre las amenazas de violaciones de alto perfil.

Las puntuaciones de las personas y los procesos permanecen bajas, cerca de 1,3 y 1,2 respectivamente. Esto refuerza lo que vemos al trabajar con empresas que tienen un SOC, así como aquellos que todavía no han incorporado esta capacidad. La mayoría de las organizaciones se centran en gran medida en soluciones de tecnología y herramientas sin que ese esfuerzo coincida con las cuestiones de personas y procesos de un programa de defensa cibernética.

Puntuación general promedio de SOMM por dimensión de los últimos 5 años

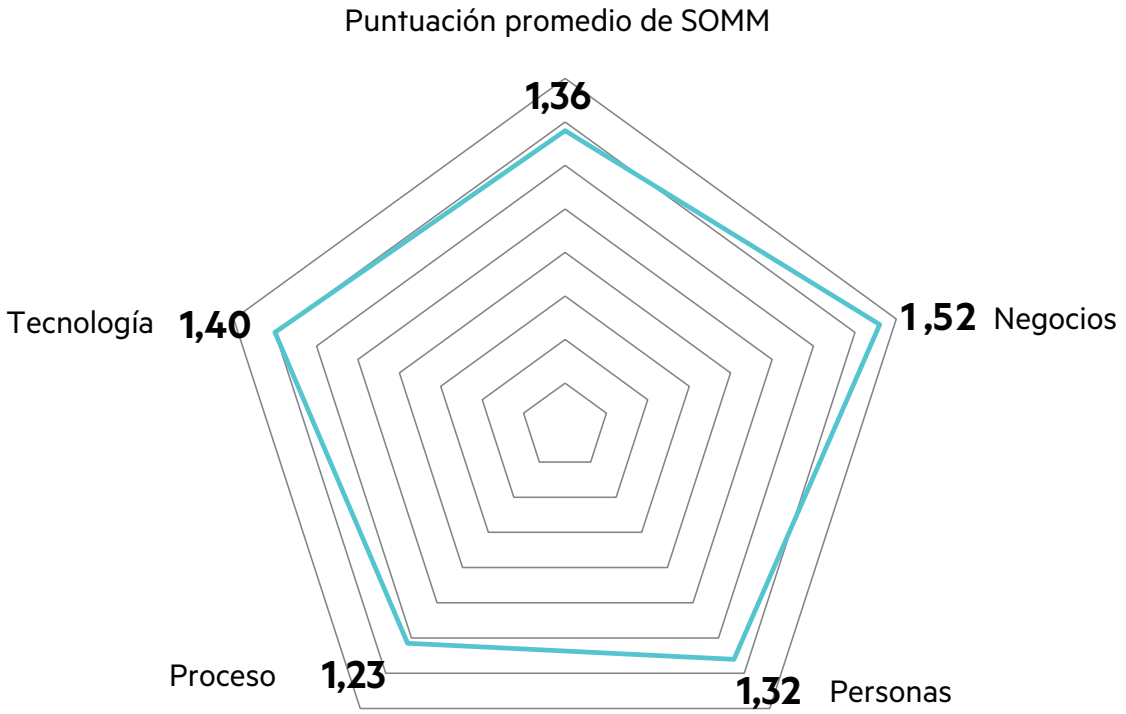


Figura 3: Puntuación promedio de SOMM por industria, últimos cinco años

Puntuación de SOMM para personas

Promedio: 1,56; promedio de 5 años: 1,32

Mín.:0,1

Máx.:3,8

Obtenga más información sobre cómo dotar de personal a su SOC: **hpe.com/software/StaffingSOC**

A continuación se presentan los resultados y las lecciones aprendidas de cada uno de los elementos: personas, procesos, tecnología y negocios.

Personas

Contar con la gente adecuada a menudo puede tener profundas repercusiones en la capacidad general de un SOC. La capacidad y madurez de las personas se obtienen por la evaluación de los siguientes elementos fundamentas de las personas que trabajan en, alrededor y liderando el SOC:

Categoría de evaluación y elementos	Conclusiones
General – Definición de roles – Estructura organizativa – Niveles de dotación de personal – Retención del personal	El principal problema que enfrentan las organizaciones de operaciones de seguridad es encontrar los recursos necesarios para el funcionamiento de la empresa. A menudo, la dotación de personal óptima no es alcanzable. Contratar las personas adecuadas es posiblemente el elemento más crítico. La contratación de analistas experimentados en el mercado presenta una serie de desafíos, especialmente para una organización nueva que no ha establecido todavía una masa crítica de cultura positiva y procesos establecidos. Otro problema común es la deserción. Donde existen requisitos de supervisión de seguridad durante todo el día, la programación 24x7 sigue representando un reto para la mayoría de las organizaciones.
Capacitación – Financiación – Relevancia – Eficacia	Existe una alta demanda de recursos de seguridad calificados y encontrar las habilidades adecuadas puede ser una tarea desalentadora. La mayoría de los SOC luchan para encontrar y retener a personas calificadas. Contratar recursos con la debida competencia puede tomar meses y, a menudo, es simplemente imposible, por lo que muchas organizaciones han recurrido a programas de desarrollo para formar y cultivar sus analistas.
Certificaciones – Financiación – Relevancia – Eficacia	La capacitación en aula y las certificaciones no son un sustituto de la experiencia de dominios múltiples cuando se trata de contratar personal para los roles de defensa cibernética. Son necesarios programas de capacitación específica para el entorno y específica del proveedor para refinar las habilidades específicas requeridas por los encargados de la defensa cibernética.
Experiencia – Industria – Organizativo – Entorno – Rol	Algunas organizaciones están favoreciendo los equipos de 8x5 en lugar de las operaciones 24x7 (con personal subcontratado o interno). En estos modelos, las reglas de correlación de alta fidelidad y la automatización se aprovechan para condiciones fuera de horas, mientras que las actividades de análisis y respuesta se centran durante el horario laboral. Esto reduce significativamente la complejidad y los desafíos de las operaciones 24x7 mientras que sigue respaldando los requisitos de respuesta para muchas organizaciones.
Evaluaciones de habilidades – Frecuencia – Relevancia	Los equipos que cuentan con habilidades y especialidades diversas (arquitectura de red, administrador de bases de datos, soporte, automatización, etc.) son generalmente más efectivos. La evaluación de habilidades debe realizarse anualmente en toda la organización y cualquier laguna que se identifique debe llenarse con capacitación o nuevos miembros en el equipo.
Trayectoria profesional – Grupos de candidatos – Planificación de la sucesión – Oportunidad	Existe una amplia disparidad en la calidad de los SOC existentes en el mercado. Si bien los analistas procedentes de otros SOC llegan con experiencias valiosas, también vienen con su equipaje. Si construye un equipo completo con estos individuos, el resultado es, a menudo, conflictos e incoherencia. Aunque ser un analista de operaciones de seguridad puede ser un rol emocionante y flexible, se necesitan coherencia y previsibilidad operativas, de lo contrario, puede causar estragos en el desempeño de la SOC. Además, los analistas experimentados en el mercado están buscando un ascenso profesional y no están interesados en otro papel de analista de nivel 1. Como sabemos que las organizaciones están trabajando muy duro para mantener a sus analistas con mejor rendimiento, existe la posibilidad de que aquellos con experiencia en SOC que están buscando funciones de analista de seguridad de nivel 1 no son los mejores en su equipo. Los analistas a menudo surgen de personas que muestran pasión y aptitud para la seguridad y proceden de la administración de TI, soporte de sistemas y funciones externas como el orden público. Las organizaciones con estos programas de desarrollo también se benefician al asegurarse de que los conocimientos que se imparten son exactamente las habilidades necesarias para sus operaciones.

Puntuación de SOMM para los procesos

Promedio: 1,35; promedio de 5 años: 1,23%

Mín.:0,12

Máx.:3,81

Categoría de evaluación y elementos	Conclusiones
Liderazgo – Visión – Alineación de la organización – Soporte de RH – Estilo y comentarios – Experiencia – Alcance del control	La gestión y liderazgo de equipo tienen un enorme impacto sobre el conjunto de la capacidad y la eficacia de un equipo de defensa cibernética. Los líderes deben poder cultivar y mantener una cultura donde los individuos crean en la labor que están realizando y se sientan apoyados por el liderazgo en sus actividades diarias, así como en su desarrollo profesional. Los líderes deben poder superar eficazmente las barreras organizacionales para llevar a cabo tareas complejas. Deben equilibrar también el conocimiento sobre la materia con la toma de conciencia de cuando es necesaria la asistencia externa. La estructura organizacional influye significativamente en la capacidad y la madurez de un SOC. La mayoría de las operaciones maduras reportan en forma ascendente a través de una organización orientada a la seguridad, el riesgo o las leyes, a menudo a un director de seguridad informática (CISO), quien informa al Director General o a un director de riesgo o cumplimiento. Los SOC que están organizados dentro de una organización de operaciones de TI pueden tener una alta madurez de los procesos, pero normalmente tienen dificultades con la capacidad efectiva. Esto se debe a un conflicto de prioridades, ya que se enfocan sobre la disponibilidad y el rendimiento, en lugar de centrarse en la integridad y la confidencialidad en los niveles superiores de la organización.

Proceso

Para que un SOC alcance altos niveles de madurez global debe existir una base sólida, actual y relevante en los procesos y procedimientos que guían la ejecución coherente de las tareas críticas y definen las expectativas y los resultados. Un buen conjunto de procesos y procedimientos permiten que el SOC pueda operar en forma sostenible y medible y hacen posible que este respalde fácilmente los esfuerzos de cumplimiento cuando sea necesario.

Sin procesos y procedimientos sólidos, los SOC pasan a depender del "conocimiento tribal" de los individuos. Las ausencias y la rotación de estos individuos puede inutilizar la capacidad del SOC. A la hora de evaluar la dimensión de los procesos del SOC, Hewlett Packard Enterprise evalúa los siguientes elementos:

Categoría de evaluación	Conclusiones
General – Herramientas de gestión del conocimiento – Control de documentos – Vigencia de la documentación	Los SOC más exitosos están utilizando un proceso adaptable, portátil y operacionalmente integrado y un sistema de gestión de conocimiento del procedimiento. Se utilizan herramientas comercialmente disponibles y de código abierto, como una wiki, para mantener la documentación organizacional y que siga siendo relevante y actual. La portabilidad y la facilidad de mantenimiento son fundamentales en los sistemas que permiten publicar y compartir imágenes, capturas de video, secuencias de comandos y otros materiales operacionales con todo el equipo. Los gerentes siguen y miden las contribuciones a la documentación como uno de los KPI del SOC.
Procesos operativos – Roles y responsabilidades – Gestión de incidencias – Programación – Rotación de turnos – Gestión de casos – Respuesta ante la crisis – Problema y cambio – Incorporación de empleados – Capacitación – Evaluación de habilidades – Gestión de estado operativo	Los entornos híbridos requieren madurez avanzada en sus procesos para ser eficaces y para evitar el mal manejo de incidentes. La utilización de modelos híbridos de personal, tales como subcontratar el análisis de primera línea, no sólo puede reducir el efecto negativo de la deserción o la adquisición de habilidades, sino que también hace el coste total de recuperación más caro. Las organizaciones híbridas deben prestar especial atención a los procesos de escalamiento y recambio entre las funciones autoaprovisionadas y las contratadas externamente. Los procesos definidos y seguidos estrictamente garantizan que toda la información relevante se transmita entre los grupos y facilita las mejores capacidades para identificar y aislar brechas.

Categoría de evaluación	Conclusiones
Procesos analíticos – Inteligencia de amenazas – Investigaciones – Exploración de datos – Seguimiento específico – Análisis forense – Contenido avanzado – Fusión de información	Los equipos de defensa cibernética exitosos utilizan de amenazas y construyen los procesos en torno a su uso. El consumo de esta inteligencia, por herramientas y personas, debe definirse de modo que se pueda actuar rápidamente cuando sea necesario. Los SOC más capaces y maduros están llevando las responsabilidades del manejo de incidentes más a la vanguardia de los equipos de operaciones. Algunas organizaciones están ejecutando actividades de respuesta o de contención a nivel del analista y responden eficazmente a las amenazas de forma más rápida y eficiente; están reduciendo el costo de respuesta a incidentes y aumentando el ROI del SOC al mantener la carga de trabajo fuera de las organizaciones CERT.
Procesos técnicos – Arquitectura de la solución y del sistema – Flujo y calidad de los datos – Incorporación de datos – Aprovisionamiento de usuarios – Controles de acceso – Gestión de la configuración – Ciclo de vida del caso de uso – Mantenimiento – Salud y disponibilidad – Copia de seguridad y restauración	Los SOC que utilizan equipos de caza están obteniendo el valor cuando integran los hallazgos a sus procesos. En la práctica, la actividad de «búsqueda» tiene tanto que ver con la comprensión de la actividad normal que mejora otras medidas detectivescas como directamente con la detección de actividad maliciosa. Una búsqueda comienza con alguna forma de inteligencia de amenazas cibernéticas o concientización interna como base para la formación de una hipótesis. Esta hipótesis es una suposición sobre la base de los conocimientos previos y la observación que la búsqueda prueba o valida al recopilar y analizar los datos necesarios. Cuando se detectan patrones o ataques, debe haber un proceso que defina cómo se usa dicha información y cómo actuar en consecuencia. Además, los resultados deben retroalimentarse en las operaciones en tiempo real, de modo que puedan manipularse mediante procesos de SOC regulares en el futuro.
Procesos del negocio – Misión – Patrocinio – Compromiso de servicio – Métricas e indicadores clave de rendimiento (KPI) – Cumplimiento – Gestión de proyectos – Mejora continua – Gestión del Conocimiento – Continuidad de los negocios (BC)/ Recuperación ante desastres (DR)	La orquestación de los deberes antes, durante y después de una violación puede reducir el costo que tiene esta para la organización. La automatización e integración del cumplimiento, el análisis, la auditoría y las herramientas de respuesta ante incidentes deben aplicarse antes de que ocurra el incidente para que sean eficaces. La rotación de funciones es fundamental en el SOC. Las organizaciones que esperan que los analistas de nivel 1 realicen una supervisión constante durante largos períodos de tiempo experimentan los niveles más bajos de capacidad y los más altos de deserción. Los SOC más exitosos rotarán los analistas en períodos de turnos de monitoreo que se alternan con otras tareas basadas en proyectos tales como comunicaciones, investigación, proyectos especiales, y análisis no estructurados. Sin embargo, no se les debe asignar a los analistas tareas de administración que no están alineadas con la misión del SOC, ya que esto va en detrimento de su eficacia.

Puntuación SOMM para tecnología

Promedio: 1,54; promedio de 5 años: 1,40

Mín.: 0,13

Máx.:4,06

Tecnología

La tecnología del SOC debe apoyar, reforzar y medir los procesos que se están ejecutando. La tecnología no proporciona valor independiente de las personas y los procesos, y cualquier implementación de tecnología en un SOC necesita tener el ecosistema necesario para producir ROI. Los elementos de tecnología que se evalúan en este informe son los siguientes:

Categoría de evaluación	Conclusiones
Arquitectura – Proceso arquitectónico – Documentación – Cobertura de la tecnología – Alineación con los requisitos empresariales	Los SOC recientemente formados darán un nivel de visibilidad de la infraestructura que las organizaciones no podían reconocer previamente, a menudo poniendo de manifiesto configuraciones erróneas, desviaciones de arquitecturas de referencia y procesos de negocios desconocidos. Los SOC más exitosos actúan como un multiplicador de fuerzas para las inversiones en tecnología de seguridad en toda la organización mediante la optimización de configuraciones y la integración de tecnologías a través de actividades de análisis y respuesta.
Recopilación de datos – Cobertura – Calidad de los datos – Consolidación – La propiedad de los datos – Acceso a los datos	Las organizaciones están maximizando las inversiones tecnológicas mediante la aplicación de una metodología de casos de uso para determinar qué fuentes de eventos monitorear activamente. Los recursos técnicos son finitos, por lo tanto cada fuente de evento monitoreada por el SOC debería tener un determinado caso de uso asociado. Se pueden ejecutar proyectos ULM en paralelo a la los proyectos creados del SOC, pero los eventos que se supervisarán activamente necesitan ser definidos cuidadosamente como casos de uso antes presentarlos para su análisis. Las operaciones que ponen como prerrequisito para el desarrollo del SOC una amplia recopilación de registro exitosa sufren demoras y reelaboración innecesarias.
Seguimiento y análisis – Gestión del flujo de trabajo y medición – Investigación – Herramientas de visualización de datos – Cobertura – Salud y disponibilidad	Las organizaciones que implementan herramientas que empujen la identificación y corrección de incidentes más cerca a los analistas de primera línea ahorrarán dinero. Un ejemplo es la integración del clic en el botón derecho con un firewall de una consola de SIEM que permite que un analista bloquee temporalmente una IP sospechosa o maliciosa. Esto permite recursos menos costosos para remediar incidentes y además los soluciona más rápido de lo que sería posible con un camino de escalamiento. Las organizaciones bien integradas implementan casos de uso de monitoreo de la seguridad de las aplicaciones en sus centros de defensa cibernética. Esto les permite identificar problemas con las aplicaciones que se ejecutan en producción, lo que puede indicar posibles violaciones graves.
Correlación – Agregación – Normalización – Tecnología cruzada – Correlación pertinente a activos – Correlación de reglas del negocio – Detección de eventos sutiles – Alertas automáticas – Correlación de etapas múltiples – Detección de patrones – Paneles e informes;	Con frecuencia, las empresas adquieren soluciones de tecnología puntuales, pero no logran reunir los datos para una corrección de riesgos y detección de amenazas eficaz. Las organizaciones que alcanzan el nivel más alto de capacidad están utilizando casos de uso avanzado para monitorear la seguridad y el análisis aprovechando la tecnología de SIEM. A menudo esto incluye personalizar una SIEM con el contexto empresarial, los detalles de los activos, la información de identidad y correlación inteligente que evalúa los datos para operaciones y el análisis a corto y largo plazo. Sin embargo, aún hay entidades que dependen de los perfiles de detección predeterminados del proveedor que sólo aborda un conjunto básico de casos de uso para la organización.
General – Gestión y administración de la infraestructura y los terminales – Importancia de los datos recopilados – Vigencia	Los SOC exitosos evalúan todos los aspectos de sus operaciones (personas, procesos, tecnología y negocios) antes de realizar cambios drásticos. Algunas organizaciones culpan a la tecnología por el fracaso en el ROI o la mitigación de amenazas, lo que conduce a una eliminación y reemplazo de sistemas. Estos grandes proyectos conducen a una reducción de la madurez de las operaciones, al tiempo que las nuevas soluciones se aceleran y a menudo no resuelven los problemas originales.

Puntuación de SOMM para negocios

Promedio: 1,52; promedio de 5 años: 1,52

Mín.: 0,59

Máx.:3,46

Negocios

La medición de las funciones empresariales y la capacidad ha aumentado constantemente en los últimos años. Las tendencias básicas, las conclusiones generales y las áreas de evaluación son las siguientes:

Categoría de evaluación	Conclusiones
Misión – Alineación con los objetivos del negocio – Comprensión coherente entre los negocios – Alineación de la capacidad operacional con la misión	Los SOC más capaces y maduros definen una misión, conservan el patrocinio ejecutivo y comunican clara y frecuentemente la misión en toda la organización. Definir de objetivos de nivel de servicio para el negocio, así como mediciones eficaces a nivel empresarial de efectividad y eficiencia garantizan un soporte y un foco empresarial sostenible. El patrocinio ejecutivo y la comunicación son fundamentales para crear una capacidad sostenible. Aquellas organizaciones que no logran obtener un patrocinio ejecutivo adecuado se encuentran trabajando con presupuestos cada vez más ajustados. Con la excepción de los proveedores de servicios gestionados, los SOC son un centro de costes. Cuando los presupuestos se ajustan, se les pedirá a los SOC que no cuentan con un fuerte patrocinio ejecutivo que hagan más con menos. Es importante que el SOC comunique sus éxitos con frecuencia al resto de la organización, incluidos los equipos que no pertenecen a la TI.
Rendición de cuentas – Compromisos operativos y de nivel de servicio – Mediciones y KPI – RoI en el cumplimiento de normativas	Los SOC maduros desarrollan e informan métricas operativas y KPI para demostrar el valor de las inversiones en seguridad. Las métricas de seguridad deben medir la eficiencia y eficacia de las operaciones de seguridad. Además, los SOC con fuerte apoyo a la inversión de la empresa son vistos como contribuyentes claves para la disminución de costos y las iniciativas de reducción de riesgos dentro de la organización. El criterio o medición de éxito más importante es la detección precisa de los ataques en curso.
Patrocinio – Apoyo ejecutivo de los SOC – Niveles de interés – Alineación de la organización	Los SOC más capaces y maduros definen una misión, conservan el patrocinio ejecutivo y comunican clara y frecuentemente la misión en toda la organización. Definir de objetivos de nivel de servicio para el negocio, así como mediciones eficaces a nivel empresarial de efectividad y eficiencia garantizan un soporte y un foco empresarial sostenible.
Relación – Relaciones con el cliente – Alineación con los grupos de pares	Los SOC eficaces a menudo están alineados con el GRC o las organizaciones legales. Esta alineación puede dar más autoridad a la organización de seguridad para actuar durante los incidentes. También puede hacer posible un presupuesto más estable que no esté siendo redireccionado constantemente para la TI. Independientemente del lugar donde se asiente el SOC dentro de la organización, las organizaciones de seguridad deben reconocer y abordar los objetivos del negocio constantemente.
Entregables – Inteligencia de amenazas – Notificaciones de incidentes – Informes y artefactos – Informes operativos	La visibilidad a nivel directivo y de nivel-C de las amenazas de seguridad ha llevado a un aumento de la necesidad de comunicación a nivel empresarial sobre el estado de la defensa cibernética y los proyectos asociados de la organización. Las organizaciones con operaciones de seguridad maduras deben poder proporcionar explicaciones sobre las amenazas y los incidentes y sus repercusiones sobre los sectores específicos de la empresa. Los informes ejecutivos deben tener un alto grado de automatización para el cálculo de los datos y deben proporcionarse con una cadencia regular. El SOC necesita ser visto como un facilitador empresarial.
Compromiso de proveedores – Niveles de soporte – Recursos dedicados – Entendimiento empresarial – Escalamientos	Un SOC puede crearse con funcionamiento solo en horario comercial (8x5), con funcionamiento en horario extendido (12x5, 18x7, 24x7), o como un híbrido autoaprovisionado y con contratación externa. El ROI percibido para dichas soluciones híbridas puede variar ampliamente en función de una variedad de factores, pero la percepción de que la seguridad puede ser subcontratada completamente a un tercero claramente ha disminuido en favor de soluciones híbridas. Las organizaciones que utilizan este modelo saben que el nivel de capacidad variará entre los equipos internos y los subcontratados, y han tomado una decisión basada en el riesgo de que el costo de utilizar su propia gente no se compensa con tener una capacidad más profunda. Un proveedor de MSS nunca sabrá tanto acerca de una organización como un equipo interno, pero aún tiene valor poder aprovechar un MSS en ciertas situaciones. Muchas empresas todavía están construyendo y operando una disponibilidad 24x7 interna. Otras están adoptando el punto de vista de que un equipo cualificado interno centrado en el horario comercial y con herramientas eficaces puede, independientemente o con el aumento de un servicio gestionado, cumplir sus objetivos.

Conclusión

La capacidad de detección y respuesta de las organizaciones continúa cambiando y evolucionando. Las herramientas de colaboración, intercambio y código abierto de la industria ahora proporcionan un punto de entrada para las organizaciones que luchan con presupuestos de seguridad mínimos para implementar las operaciones de seguridad. Algunas regiones del mundo están experimentando un auge y cambio hacia la subcontratación a través de servicios de seguridad gestionados para superar la escasez de profesionales de la seguridad cibernética que afecta a las organizaciones. En algunas regiones y sectores hay un cambio gradual hacia la contratación interna a través de un modelo híbrido de personal de seguridad, que les permiten a las organizaciones recuperar la estrategia global de seguridad y gestionar una relación con el proveedor donde estos realizan lo que mejor saben hacer. Para otros, las violaciones o un evento adverso dentro de su industria aceleran los plazos y las partes interesadas buscan una solución de seguridad.

Sin importar en qué etapa se encuentran las organizaciones, debería ser evidente que no hay un producto o servicio de solución rápida que pueda brindar la protección y la conciencia operativa que una organización necesita. Los programas de operaciones de seguridad exitosos requieren una evaluación de la gestión de riesgos, la seguridad y el cumplimiento de los objetivos de la organización y la optimización constante de las personas, los procesos y la tecnología de los componentes de las soluciones implementadas. Para alcanzar y mantener la madurez son necesarias inversiones dirigidas en todas las facetas del programa de operaciones de seguridad.

HPE Security Intelligence and Operations Consulting ha trabajado con algunos de los centros de operaciones de seguridad más avanzados del mundo. Durante los últimos cuatro años, a través del informe del Estado de las operaciones de seguridad, hemos compartido los hallazgos de 183 evaluaciones en 137 organizaciones de SOC discretas en 31 países. Al compartir perspectivas sobre lo que hace que algunos de los más avanzados centros de defensa cibernética del mundo sean exitosos, confiamos en que usted también pueda aprovechar los beneficios de los análisis avanzados, la inteligencia de amenazas y los procesos repetibles implementados dentro de su organización.

Acerca de los productos de seguridad HPE

Hewlett Packard Enterprise es un proveedor líder de soluciones de seguridad y cumplimiento para la empresa moderna que busca mitigar el riesgo en entornos híbridos y defender contra las amenazas avanzadas. Sobre la base de investigaciones y productos líderes en el mercado de HPE Security ArcSight, HPE Security Fortify, HPE Data Security (Voltage/Atalla) y HPE Security Research, HPE Security Intelligence Platform ofrece en exclusiva correlación avanzada, orquestación de respuesta a incidentes, protección de aplicaciones y defensas de la información para proteger la infraestructura de TI híbrida actual de las amenazas cibernéticas sofisticadas.

Obtenga más información en
hpe.com/software/SIOC

La puntuación de madurez totalideal es nivel 3: "definido".

Apéndice

La **HPE methodology** para las evaluaciones se basa en el Modelo de madurez de capacidades para la integración del Instituto de ingeniería de software Carnegie Mellon (CMMI-sei) y se actualiza a intervalos regulares para seguir siendo pertinente con las actuales tendencias en seguridad y las capacidades de amenaza. El foco de las evaluaciones incluye los aspectos de la alineación con el negocio, las personas, los procesos y la tecnología de las operaciones de seguridad del sujeto. La detección fiable de actividad maliciosa y las amenazas a la organización y un enfoque sistemático para gestionar estas amenazas son los criterios más importantes de éxito para una capacidad de defensa cibernética madura.

La puntuación compuesta ideal de madurez para una capacidad de defensa cibernética empresarial es de nivel 3, cuya capacidad es "definida". Esto se logra con una mezcla complementaria de agilidad para ciertos procesos y gran madurez para otros. Hewlett Packard Enterprise ha observado que los niveles más altos de madurez son costosos de conseguir y que en la búsqueda de mayor madurez, las operaciones a menudo sufren estancamiento, rigidez y un bajo nivel de eficacia global.

Los equipos de defensa cibernética (o proveedores que ofrecen servicios de SOC gestionados) que aspiran a alcanzar los niveles de madurez "5" carecen de una comprensión o apreciación de la naturaleza de esas capacidades y las amenazas contra las que están defendiendo. Dada la agilizad y la capacidad de adaptación del actor de amenazas, la optimización el para la repetibilidad y la coherencia es solo marginalmente eficaz.

Los proveedores de servicios de seguridad gestionada (MSSP) deben apuntar a un nivel de madurez de entre 3 y 4 debido a la necesidad de consistencia en las operaciones y las posibles penas de compromisos de servicio no cumplidos, aun así existe un compromiso en agilidad, eficacia y amplitud que el MSSP y sus clientes aceptan con este nivel de madurez. Una vez que se alcanza el nivel de madurez ideal, un equipo de defensa cibernética debe centrarse en desarrollar capacidades continuamente para mantenerse a la par de la rápida evolución del panorama de amenazas.

Mientras la quinta generación (5G/SOC) de las operaciones de seguridad sigue evolucionando, están mejor equipados para reconocer el cambio en el panorama de amenazas y enfocan el desafío en forma holística. Están capacitando a los analistas en contra-inteligencia de seguridad, vigilancia, psicología criminal y pensamiento analítico para aumentar la inversión en tecnología. La mayoría de las organizaciones no han implementado 5G/SOC, pero aquellos que los tienen, parecen haberse beneficiado enormemente con las metodologías de inteligencia, intercambio de información y enfoque humano del adversario.

La industria sigue luchando con la medición del costo de las violaciones a la seguridad cibernética en las organizaciones comerciales. Se creía que, después de un evento adverso de seguridad las repercusiones podían medirse a través de la disminución de los precios de las acciones. Sin embargo, después de violaciones muy visibles en empresas de entretenimiento, servicios financieros, bancarios y de inversiones, así como en organizaciones de ventas, queda claro que más allá de la incertidumbre inmediata, los inversores y los consumidores no penalizan a las organizaciones.

Los datos del mercado muestran que la recuperación, en lo que respecta al precio de las acciones, toma un par de semanas. La interrupción del negocio y la pérdida de datos no representan los componentes de mayor costo en los eventos de seguridad significativos.[1] Hay un efecto a largo plazo en la rentabilidad ya que las organizaciones en recuperación enfrentan mayores costos provenientes de los nuevos programas de seguridad, los litigios y el recambio organizacional que se produce luego de una vulneración de la seguridad.

Este informe resume los datos recopilados durante las evaluaciones de madurez realizadas por Hewlett Packard Enterprise y comparte las tendencias de seguridad empresarial relacionadas con el estado actual de esta importante función de seguridad, incluyendo los errores comunes y lo que puede aprenderse de ellos. La finalidad del presente informe es exponer e impulsar la capacidad y la madurez de los equipos de defensa cibernética conforme las organizaciones avancen hacia los **centros de operaciones de seguridad de quinta generación**.

[1] Estudio sobre el costo de la delincuencia cibernética, Ponemon, octubre de 2015

Relevancia de nuestros datos: Calificación para presentar este informe
El portafolio HPE Enterprise Security Products incluye la suite de registro líder en el mercado HPE ArcSight SIEM además de servicios. Los productos de HPE ArcSight Enterprise Security Management (ESM) revolucionaron el mercado SIEM moderno.

SIEM a veces es considerado un "multiplicador de fuerza" para las tecnologías de seguridad y está en el centro de la defensa cibernética y los equipos de operaciones de seguridad modernos. Los SIEM realizan la centralización y correlación de tipos de datos discretos, habilitan la correlación inteligente de datos, integran el contexto de negocios y de activos, proporcionan una interfaz para la investigación y el flujo de trabajo operativo, así como también generan informes y métricas. El SIEM es el centro técnico neurálgico del programa de defensa cibernética y el SOC.

Hewlett Packard Enterprise (en ese momento HP) formó la práctica de SIOC en 2007, dedicada a definir las mejores prácticas de los SOC y construir SOC de clase empresarial. Este equipo combinó la experiencia adquirida al implementar SIEM dentro de los SOC desde 2001 con un grupo de expertos que han diseñado, construido y dirigido SOC para algunas de las organizaciones más importantes del mundo. Desde su creación, el equipo de SIOC ha madurado iterativamente una metodología para SOC que ha sido adoptada en decenas de organizaciones de todo el mundo.

Hewlett Packard Enterprise (en ese momento HP) creó el SOMM en 2008 para ayudar a los clientes a evaluar el estado actual de sus SOC con respecto a las mejores prácticas de la industria y los objetivos individuales. También creamos planes basados en la experiencia para cerrar la brecha de una manera eficaz y eficiente. El SOMM no es una autoevaluación que puede llevar a resultados engañosos, sino más bien una revisión objetiva de las capacidades de la organización dirigida por un experto en el tema. Los elementos de la evaluación dentro del SOMM se basan en la metodología HPE SIOC, derivada de más de una década de experiencia en decenas de entornos de SOC empresariales. Nuestros productos líderes en el sector, nuestras metodologías probadas y una década de experiencia con el conjunto de datos más grande de su tipo hacen que Hewlett Packard Enterprise esté calificada específicamente para elaborar este informe.

Metodología y modelo de madurez de las operaciones de seguridad
El CMMI es un enfoque de mejora de procesos que proporciona a las organizaciones los elementos esenciales de los procesos efectivos de seguridad informática. Puede utilizarse como guía para la mejora de procesos a en un proyecto, una división o una organización.

El CMMI ayuda a integrar las funciones organizativas tradicionalmente separadas, establecer prioridades y objetivos de mejora de procesos, proporcionar orientación para la mejora de la calidad y ofrece un punto de referencia para evaluar los procesos actuales. Hewlett Packard Enterprise ha modificado el enfoque de CMMI para medir de manera efectiva el grado de madurez de la capacidad de las operaciones de seguridad de una organización. El modelo de HPE, SOMM, se centra en varios aspectos de una exitosa y madura capacidad de vigilancia e inteligencia de seguridad, incluidas las personas, los procesos, la tecnología y las funciones de soporte de los negocios.

El SOMM utiliza una escala de cinco puntos similar al modelo CMMI. La puntuación de "0" corresponde a una completa falta de capacidad, mientras que "5" corresponde a una capacidad que es constante, repetible, documentada, medida, rastreada y continuamente mejorada. Las organizaciones que no tienen un equipo de monitoreo de amenazas formal suelen tener puntuaciones entre 0 y 1 porque incluso una organización sin un equivalente o equipo formal a tiempo completo (FTE) realiza algunas funciones de supervisión de manera ad hoc.

Los centros de operaciones de seguridad más avanzados del mundo suelen alcanzar una puntuación global entre nivel 3 y nivel 4. Hoy en día existen muy pocas de estas organizaciones. La mayoría de las organizaciones con un equipo centrado en la detección de amenazas tendrá una puntuación de entre 1 y 2.

Algunas áreas deben ser rígidas, repetibles y medidas mientras otros sectores deben ser flexibles, ágiles, adaptables y veloces.

Nivel de Somm	Calificación	Descripción
Nivel 0	Incompleto	No existen elementos operacionales
Nivel 1	Inicial	Se cumplen los requisitos mínimos para proporcionar supervisión de seguridad. Nada está documentado y acciones son ad hoc.
Nivel 2	Gestionado	Se cumplen los objetivos del negocio y las tareas operativas están documentadas, son repetibles y pueden ser realizadas por cualquier miembro del personal. Se cumplen los requisitos necesarios. Los procesos se definen o modifican reactivamente.
Nivel 3	Definido	Las operaciones están bien definidas, subjetivamente evaluadas y son flexibles. Los procesos se definen o modifican reactivamente. Los procesos se definen o modifican de forma proactiva.
Nivel 4	Medido	Las operaciones son evaluadas cuantitativamente, se examinan sistemáticamente y se realizan mejoras de manera proactiva utilizando métricas del negocio y de desempeño para impulsar estas mejoras. Este es el nivel de madurez ideal para la mayoría de los SOC del proveedor de servicios gestionados.
Nivel 5	Optimización	Se ha implementado un programa de mejora operativa para rastrear cualquier deficiencia y garantizar que todas las lecciones aprendidas impulsen mejoras continuas. Los procesos son rígidos y menos flexibles y es necesaria una sobrecarga considerable para administrar y mantener este nivel de madurez, lo que contrarresta los beneficios logrados.

Los SOC normalmente tienen una gran cantidad de procesos y procedimientos. El SOMM ofrece una gran arquitectura para ayudar a organizar, mantener y mejorar este cuerpo de trabajo. Para la mayoría de las organizaciones, una puntuación total agregada de SOMM de nivel 3 es un objetivo apropiado. Algunas áreas deben ser rígidas, repetibles y medidas mientras otros sectores deben ser flexibles, adaptables y ágiles.

La mezcla de procesos y procedimientos rígidos y flexibles permite que un SOC maduro asegure un monitoreo efectivo con una puntuación total de madurez de 3. Este nivel de madurez garantiza que los procesos críticos y los procedimientos están documentados. Están sujetos a una mejora demostrable y medida a través del tiempo, mientras que todavía permiten que surjan desviaciones y procesos ad-hoc para hacer frente a amenazas o situaciones específicas.

En términos prácticos, esto significa que cualquier analista de cualquier turno, en todas las regiones ejecutará un procedimiento determinado exactamente de la misma manera. Además, cuando un analista encuentra un error o es necesario un cambio en los procedimientos operativos, puede hacer una corrección en ese mismo instante y todos los analistas se beneficiarán inmediatamente con las mejoras.

La evaluación de SOMM de HPE se centra en cuatro categorías principales, cada una de las cuales tiene varias subcategorías. Se analizan factores de las personas, los procesos, la tecnología, así como también la alineación con el negocio, utilizando una combinación de técnicas de observación y entrevista. Se les pide a las organizaciones evaluadas que demuestren con pruebas documentadas los reclamos formulados durante las entrevistas con el fin de garantizar que las puntuaciones no sean infladas artificialmente.

Suscríbase para recibir actualizaciones

Hewlett Packard Enterprise

4AA6-9062SPL, marzo de 2017