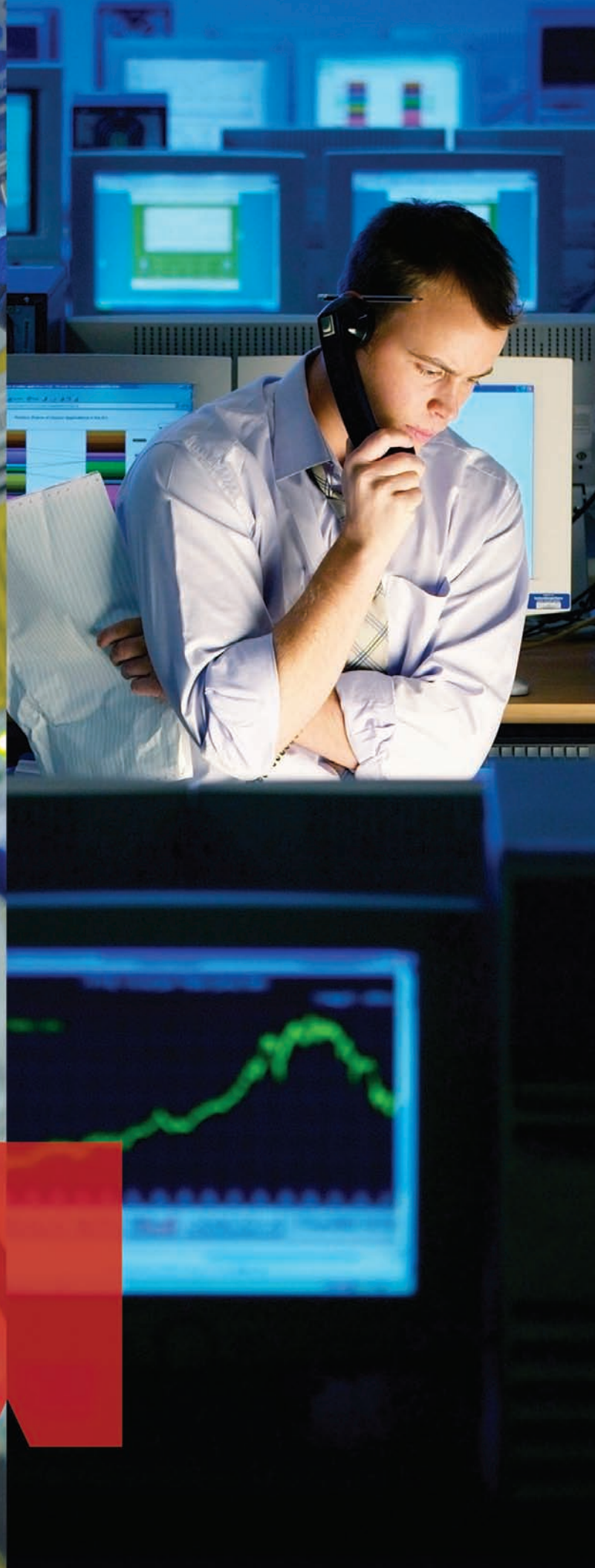




The Security Division of EMC

White paper

Creación de una Función de Operaciones de Seguridad Eficaz



El conocimiento de los problemas de seguridad resulta fundamental para lograr una política eficaz.

Cuando pensamos en un Centro de Operaciones de Seguridad (SOC), generalmente imaginamos una sala grande repleta de personas sentadas en filas perfectas, con su atención dividida entre sus monitores de escritorio y una gran pantalla ubicada en el frente, similar a la imagen que tenemos del Centro Espacial de Houston durante el lanzamiento de un transbordador espacial. Es cierto que existen lugares así. Sin embargo, en muchas organizaciones la realidad es bastante diferente. A pesar de que prácticamente todas las empresas cuentan con una función de operaciones de seguridad, esta se puede desarrollar de varias maneras. En algunos casos, es un

grupo diseñado formalmente con personal e instalaciones exclusivas. En otros casos, las operaciones de seguridad simplemente consisten en un conjunto de personas que cuentan con varias responsabilidades y enfrentan los problemas de seguridad a medida que se van originando.

Cuando se da ese tipo de situación, la comprensión de todas las actividades y todos los roles dentro de una función de operaciones de seguridad constituye el primer paso para lograr que dichas operaciones sean más eficaces, lo que le permitirá aprovechar la experiencia de la fuerza de trabajo y las inversiones en tecnología relacionadas, y obtener así las mayores ventajas.

Operaciones de Seguridad Definidas: “¿Qué hace exactamente?”

“Operaciones de seguridad” es un término que ha surgido en los últimos años para describir una serie de actividades cuyo objetivo consiste en proteger los activos de información de una organización. En el pasado, las tareas de seguridad se dividían entre el personal de seguridad, los administradores de red y los equipos de operaciones del servidor de manera ad hoc. Existe una tendencia cada vez mayor a reunir estas responsabilidades dentro de las operaciones de seguridad.

Actividades Diarias

Cuente o no con un centro de operaciones de seguridad (SOC, *Security Operations Center*) formal, es muy probable que los miembros del personal realicen ciertas tareas de rutina de algún modo. Estas actividades diarias están diseñadas para mantener los sistemas de seguridad a un nivel de funcionamiento óptimo a fin de que los procesos de negocios estén protegidos contra ataques y abusos, y aún poder funcionar de manera transparente y sin interrupciones.

La administración de vulnerabilidades mantiene alejados a hackers (y auditores).

La identificación de sistemas sin parches, contraseñas vulnerables y configuraciones erróneas desempeña dos funciones: ayudarlo a mejorar la seguridad y el cumplimiento de normas. Brinda una imagen precisa de las vulnerabilidades de seguridad, de modo que, por ejemplo, puede incentivar al personal de operaciones de servidor para que corrija los sistemas. Además, puede estar un paso adelante de los hackers, quienes probablemente deseen explotar esas vulnerabilidades, y los auditores, ante quienes será responsable de proteger la infraestructura en función de las normas establecidas.

La administración de dispositivos de seguridad aumenta la precisión de la detección de amenazas.

El mantenimiento de políticas de firewall actualizadas y la adaptación de reglas para sistemas de detección de intrusiones (IDS, *Intrusion Detection System*) y administración de eventos e información de seguridad (SIEM, *Security Information and Event Management*) le permiten ajustar continuamente la precisión de las alertas. Cuando la tecnología que implementó funciona de manera eficaz, el tráfico de red puede fluir donde sea necesario, el software se puede ejecutar sin interrupciones y no se desperdicia el tiempo del personal en la investigación de falsos positivos.

El monitoreo proporciona una advertencia temprana cuando se produce algún problema.

La exploración del entorno de seguridad en busca de indicios de problemas constituye una tarea continua. Esta incluye la verificación del funcionamiento adecuado de los sistemas de seguridad, la comprobación de varios canales de comunicación para alertas automáticas que pueden requerir seguimiento y la exploración de otros indicadores, como aumento inexplicable del tráfico de red, lo que puede indicar el inicio de un ataque.

La investigación de amenazas indica qué buscar y cómo responden los demás.

Existen muchos recursos disponibles para ayudarlo a realizar el seguimiento de vulnerabilidades detectadas recientemente, cómo se explotan y qué correcciones se desarrollaron como respuesta. Estos recursos incluyen asesoría sobre seguridad para proveedores, paneles de anuncios, listas de correo y organizaciones, como el Equipo Comercial de Respuesta Ante Emergencias Informáticas (CERT®, *Computer Emergency Response Team*), SANS Internet Storm Center y Alertas de Seguridad Cibernéticas del Departamento de Seguridad de la Nación. La información que proporcionan puede ayudarlo

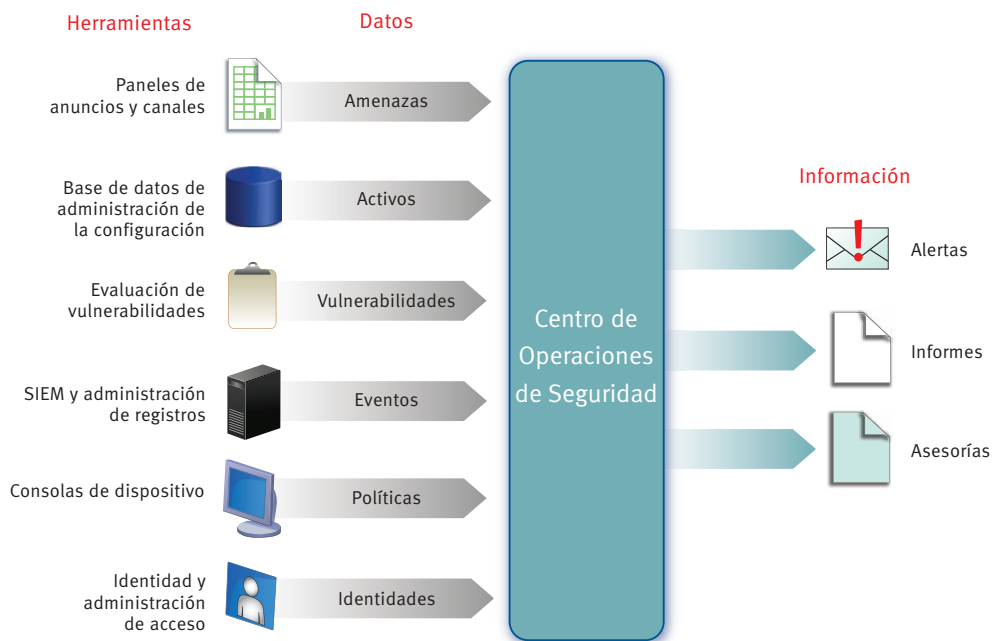


Figura 1.
Una Instantánea de las Operaciones de Seguridad

Al utilizar una amplia variedad de herramientas y recursos de información, la función de Operaciones de Seguridad monitorea continuamente el entorno de seguridad de una organización, responde a amenazas inmediatas y vulnerabilidades a mayor plazo, y proporciona pautas y consejos sobre asuntos de seguridad a unidades de negocio y administración senior.

a reconocer rápidamente un ataque y tomar las medidas necesarias para reducir el riesgo. A más largo plazo, puede ayudarlo a dar prioridad a las inversiones de seguridad para proteger mejor el entorno.

Administración de Problemas e Incidentes

Más allá de las operaciones diarias, se llevan a cabo un conjunto de tareas en respuesta a los incidentes de seguridad. En las organizaciones más pequeñas, estos eventos solo ocurren periódicamente; en las organizaciones más grandes, es probable que ocurran con mayor frecuencia y requieran la atención del personal dedicado a operaciones de seguridad.

La respuesta rápida ante incidentes reduce el impacto en los ataques.

El SOC dirige la respuesta a ataques y vulnerabilidades de alto riesgo, toma medidas inmediatas para mitigar el impacto de un ataque en desarrollo y proporciona pautas a administradores de red y operadores de sistemas sobre medidas adicionales que detienen o rectifican una amenaza.

La evaluación de problemas y la administración de incidentes lo ayudarán a asegurarse de que está utilizando el tiempo de manera conveniente.

La mayoría de los equipos de operaciones de seguridad tienen más trabajo del que pueden administrar. El establecimiento de un proceso de evaluación de problemas permite que el

personal evalúe incidentes y problemas rápidamente, y dé prioridad a quienes representan el mayor riesgo para el negocio. A su vez, puede asignar recursos experimentados a los problemas más urgentes e importantes. Además, los procedimientos bien definidos de escalamiento y flujo de trabajo ayudan a garantizar que los incidentes de alto riesgo se resuelvan con la mayor rapidez posible.

La investigación forense revela el origen subyacente de los incidentes de seguridad.

Con las herramientas y la información adecuadas, los analistas de seguridad pueden estudiar las circunstancias relacionadas con un ataque o violación de seguridad, y seguir el rastro de la evidencia hasta el origen. A su vez, el personal de SOC puede ofrecer protección contra eventos repetidos y la organización puede tomar medidas contra las partes conocidas (por ejemplo, empleados, asociados de negocios o contratistas) que estén involucradas.

Guía y Asesoría Estratégica

Durante la realización de sus tareas, Operaciones de Seguridad recopila datos valiosos sobre el entorno de TI y la manera en la que la organización se encarga de la seguridad. La conversión de esos datos operacionales en una asesoría de negocios efectiva también constituye una tarea esencial.

Figura 2.
¿Quién es Quién en el SOC?

Hasta en una función de operaciones de seguridad relativamente pequeña, los roles, las responsabilidades y la estructura de reporting suelen asemejarse a algún tipo de variación de este modelo. Las áreas sombreadas representan la superposición de funciones.

	Tareas estratégicas	Respuesta ante incidentes	Tareas diarias
CSO	Asesoría estratégica		
	Recopilación de métricas		
Administrador de seguridad		Recopilación de métricas	Recopilación de métricas
		Supervisión de RI	
Experto en seguridad		Evaluación de problemas	Investigación de amenazas
		Investigación	
Analista de seguridad			Investigación
			Monitoreo y alertas
			Administración de configuración de dispositivos
			Administración de vulnerabilidades

La asesoría estratégica sobre seguridad soporta el crecimiento y la innovación del negocio.

Con una visión amplia y altamente detallada del entorno de seguridad, las Operaciones de Seguridad se encuentran en una posición excelente para asesorar al negocio sobre cómo la seguridad puede soportar iniciativas estratégicas, entre ellas, adquisiciones y fusiones, redes de asociados de negocios y desarrollo de nuevas líneas de negocio.

Las métricas de las operaciones de seguridad reflejan las áreas que requieren mejoras.

Los datos operacionales recopilados a partir de logs de eventos e informes de incidentes manifiestan las diferencias entre las expectativas de cómo debe funcionar el SOC y la realidad diaria que debe enfrentar el personal. El análisis de datos operacionales permite indicar las áreas que requieren mejoras con respecto al personal, la capacitación, los procesos, las políticas o la tecnología.

Por ejemplo, una falla constante en el parche de vulnerabilidades puede indicar una necesidad de capacitación integral o mayor comunicación orientada al personal encargado de las

operaciones del servidor. La disminución extendida del ritmo de la red causada por ataques externos podría manifestar la necesidad de un monitoreo más exhaustivo de las amenazas o un proceso de escalamiento imprescindible. En estos y otros casos, una vez que se toman medidas correctivas, los datos de tendencias también se pueden medir si estas acciones tienen el efecto deseado.

Las asesorías específicas de la organización crean conciencia e impulsan el cambio.

Una responsabilidad clave del equipo del SOC consiste en convertir los propios incidentes de seguridad de la organización, además de la información sobre amenazas generada por CERT, SANS y otras fuentes confiables, en recomendaciones útiles que sean específicas para la organización. Cuando se realizan de manera consistente y oportuna, estas recomendaciones pueden mejorar continuamente el panorama general de seguridad. Por ejemplo, las asesorías pueden proporcionar pautas a arquitectos empresariales y otras personas sobre los tipos de controles que se deben implementar para proteger el negocio.

Además, las asesorías con un mayor nivel de estrategia por naturaleza pueden crear conciencia ejecutiva sobre los problemas de seguridad, y ejercer influencia sobre las personas encargadas de tomar las decisiones a fin de incrementar la atención y la inversión en cuestiones de seguridad.

Funciones y Responsabilidades: ¿Quién es Quién en las Operaciones de Seguridad?

El componente más importante de un centro de operaciones de seguridad exitoso es un equipo que funciona correctamente. En las organizaciones más pequeñas, esto puede incluir solo una o dos personas que manejen todas las tareas del SOC con un enfoque que se limita estrictamente a las actividades más urgentes o críticas. Las empresas más grandes pueden contar con un amplio equipo de personal dedicado a operaciones de seguridad, cada uno con áreas de especialización específicas. La figura 2 muestra las tareas clave de cada función y su interrelación.

Analistas de Seguridad

Los analistas de seguridad están a la “vanguardia” de las operaciones de seguridad. Tienen la responsabilidad de garantizar que las herramientas de seguridad se implementen adecuadamente y se ejecuten de manera óptima. Monitorean constantemente el entorno en busca de problemas y, a menudo, constituyen el primer punto de contacto cuando se emite una alerta de alto riesgo o cuando un posible ataque comienza a afectar las operaciones del negocio. Generalmente, los analistas también llevan a cabo las etapas iniciales de una investigación forense.

Especialistas en Investigación

Detrás de los SOC más exitosos se encuentran uno o más expertos en seguridad cuyo título correcto puede ser Especialista en Investigación o Analista Senior. En general, estos individuos cuentan con vasto conocimiento técnico y amplia experiencia. La seguridad ocupa un lugar fundamental para ellos y se solicita su ayuda en caso de que se produzcan incidentes de seguridad especialmente complejos que generan mucha presión. Debido a su conocimiento en materia de tecnología y desafíos de seguridad, también pueden actuar como consultores del Administrador de SOC y del Director de Seguridad de la Información (CISO, *Chief Information Security Officer*) para aconsejarlos sobre estrategias de seguridad.

Administrador del SOC

El Administrador del SOC supervisa las operaciones de seguridad diarias y pone en práctica personas, herramientas, procesos y métodos de medición necesarios para lograr los objetivos del SOC en cuanto al soporte del negocio. El Administrador del SOC funciona como interfaz entre el SOC y el CISO. En esta función, el Administrador convierte los requerimientos y objetivos del CISO en un conjunto de acciones para que ejecute el equipo del SOC y concientiza al CISO sobre los problemas que requieren inversión y atención ejecutiva.

CISO

Como la principal interfaz entre la organización de seguridad y el negocio, el CISO tiene la responsabilidad de garantizar que los recursos del SOC y las actividades se alineen para soportar la estrategia general del negocio y ayudar a crear valor al negocio. El SOC convierte los requerimientos del negocio en objetivos de operaciones de seguridad, prioriza dónde se gasta el presupuesto y, a menudo, funciona como instructor e informa a los ejecutivos del negocio el modo en que la seguridad puede garantizar la innovación del negocio y se puede utilizar para administrar los riesgos de la información.

Cada vez son más los centros de operaciones de seguridad que implementan herramientas como SIEM y administración de logs, para automatizar la recopilación de información, alertas y reporting.

Los equipos del SOC más avanzados enriquecen aún más los conocimientos sobre el entorno de seguridad con información contextual proporcionada por otras herramientas y fuentes de información.

Herramientas del SOC: Nivel Inicial a Avanzado

La tecnología es un elemento clave de las operaciones de seguridad y proporciona los medios necesarios para centralizar procesos, automatizar tareas repetitivas y, en general, incrementar la productividad de las personas. La mayoría de los equipos de operaciones de seguridad utilizan las siguientes herramientas básicas:

- Software y dispositivos de seguridad perimetrales (por ejemplo, firewall, productos antivirus e IDS) que cuentan con sus propios mecanismos de reporting y alertas, además de consolas, para realizar cambios de políticas. En los SOC's rudimentarios, estas herramientas constituyen a menudo el primer punto de entrada para que los analistas investiguen o solucionen un problema de seguridad.
- Las herramientas de evaluación de vulnerabilidad son productos comerciales o herramientas de código abierto, como Nessus. Ambos proporcionan información valiosa sobre los sistemas que están corregidos y configurados correctamente, y sobre los sistemas que representan un riesgo para la seguridad del entorno.
- Las herramientas de diagnóstico freeware se pueden descargar fácilmente y son muy útiles, incluso para el analista de operaciones de seguridad más experimentado. Las herramientas de exploración de red, como nmap, las herramientas de exploración inalámbrica (Kismet) o las herramientas de prueba de penetración, como Metasploit, pueden ser muy valiosas para probar y diagnosticar los problemas de seguridad.

Más Allá de los Conceptos Básicos

Cada vez son más los centros de operaciones de seguridad que implementan herramientas como administración de eventos e información de seguridad (SIEM) y herramientas de administración de logs, para automatizar la recopilación de información, alertas y capacidades de reporting. Por ejemplo, la solución SIEM de RSA, la plataforma RSA enVision®, simplifica las operaciones de seguridad ya que:

- **Proporciona información de seguridad útil y en tiempo real.** Las alertas en tiempo real señalan los problemas de alto riesgo y permiten que los profesionales de seguridad prioricen sus actividades. Las capacidades de correlación escalable mejoran la productividad de los analistas al reducir los falsos positivos.
- **Permite realizar investigaciones forenses.** La plataforma RSA enVision soporta trabajos de investigación sobre los incidentes de seguridad pasados al brindar la habilidad de buscar eventos de varias maneras, por ejemplo, por período de tiempo, ID de usuario, número de puerto y servidor de host, para lograr obtener rápidamente el origen del incidente. El flujo de trabajo acelera el ciclo de vida de resolución de problemas desde la investigación inicial, el direccionamiento a los miembros del equipo adecuado del escalamiento automático de alta prioridad o los incidentes difíciles de resolver, hasta la resolución, el cierre y el archiving.
- **Aumenta la visibilidad de la eficacia de las medidas de seguridad.** La tecnología RSA enVision ayuda a las organizaciones a evaluar la eficacia del programa de seguridad al brindar información acerca de la efectividad de los controles de acceso que se están ejecutando, además de los servicios de red y las aplicaciones no autorizadas.

El Contexto es Clave

Los equipos de operaciones de seguridad más avanzados enriquecen aún más los conocimientos sobre el entorno de seguridad con información contextual proporcionada por otras herramientas y fuentes de información. Por ejemplo, la base de datos de administración de configuración, la cual captura los datos de configuración para una amplia gama de activos, facilita la evaluación de los requerimientos para implementar cambios de seguridad en toda la empresa, así como también el impacto en el negocio y el potencial impacto operacional de dichos cambios. Los sistemas de administración de acceso e identidad (IAM, *Identity and Access Management*) proporcionan visibilidad del comportamiento del usuario para incidentes de seguridad específicos y para detectar tendencias de IAM más amplias. Esto ayuda a aumentar la

responsabilidad del usuario y, al mismo tiempo, permite que el personal del SOC detecte más fácilmente el uso indebido de privilegios por parte de miembros de la empresa.

Introducción: ¿Cómo Poner en Funcionamiento las Operaciones de Seguridad?

Una vez que haya identificado las funciones y los roles de las operaciones de seguridad actuales dentro de la organización, deseará identificar las brechas e ineficacias, y comenzar a solucionarlas. A continuación, se resumen algunas de las mejores prácticas clave utilizadas por las organizaciones líderes de TI.

Comencemos por simplificar la vida del analista

La función del analista de seguridad puede resultar frustrante. A menudo, es una función reactiva y, si no existe una estructura definida implementada para priorizar y escalar problemas, puede convertirse fácilmente en un trabajo de extinción de incendios en los que el personal elimina constantemente los indicios más evidentes de amenazas contra la seguridad sin resolver los problemas subyacentes. Además, si los analistas de seguridad no pueden acceder de manera oportuna a la información precisa de lo que está sucediendo en el entorno, es imposible que sepan si se están implementando los controles adecuados.

Durante un mes, evalúe las actividades en las que los analistas emplean su tiempo y priorice los puntos en los que cree que el personal adicional o la tecnología podrían tener el mayor impacto en la mejora de la eficacia.

Brinde la información correcta a las personas para que desempeñen sus tareas

En todas las áreas del SOC, la realización eficaz del trabajo depende de contar con la información correcta en el momento oportuno. Considere el uso inteligente de tecnología para poner esa información al alcance de las personas.

- **Analistas:** alertas oportunas, con prioridad basada en la urgencia. Datos de activos y logs para proporcionar información contextual acerca de incidentes de seguridad.
- **Especialistas en investigación:** información detallada sobre incidentes de seguridad en el momento en el que ocurren para acelerar la resolución. Datos sobre amenazas emergentes para recomendar medidas de protección.
- **Administradores de seguridad:** estado actualizado sobre los problemas de seguridad pendientes. Datos sobre cómo se están utilizando los recursos de personal.

- **CISOs:** información resumida sobre los incidentes y problemas de seguridad más urgentes. El riesgo y el panorama de seguridad general del negocio.

Enfoque sobre la mejora de procesos en lugar de la automatización del SOC

No es probable que la tecnología alguna vez reemplace al personal de operaciones de seguridad, pero las herramientas como la administración de logs y SIEM, pueden simplificar algunos de los procesos más tediosos y repetitivos, y aumentar así la productividad.

Un ejemplo sería tomar las alertas de IDS, compararlas con una lista de equipos vulnerables al ataque particular que se ha detectado y reiniciar los servicios en los dispositivos afectados. Cuando los dispositivos pertenecen a otro grupo, es posible que deba negociar el permiso para automatizar la medida correctiva en esos dispositivos.

Logre que la tecnología sea útil para las personas y no al contrario

Una función exitosa de las operaciones de seguridad depende principalmente de contar con un equipo integrado de personas con el soporte de procesos bien definidos e información oportuna que permita tomar decisiones acertadas. La tecnología es útil porque logra que las personas sean más eficaces, por lo tanto, utilice soluciones como SIEM de manera coherente para optimizar los procesos y brindar la información de manera que se pueda procesar fácilmente.

Cuando deba decidir acerca de la tecnología de SIEM adecuada para la función de operaciones de seguridad, busque lo siguiente:

- Una solución fácil de implementar que acelere y simplifique los procesos.
- Una solución en la que estén disponibles inmediatamente todos los datos que las personas necesitan para realizar sus tareas.
- Una solución que le brinde las herramientas necesarias para convertir los datos operacionales en información útil que mejore el panorama de seguridad y soporte las iniciativas estratégicas del negocio.

Acerca de RSA

RSA, la División de Seguridad de EMC, es el principal proveedor de soluciones de seguridad para aceleración del negocio y ayuda a las más importantes organizaciones del mundo a alcanzar el éxito resolviendo los más complejos y delicados desafíos de seguridad. El enfoque hacia la seguridad centrado en la información que ofrece RSA protege la integridad y la confidencialidad de la información durante todo su ciclo de vida, sin importar dónde se la mueva, quién acceda a ella o cómo se la use.

RSA ofrece soluciones líderes en verificación de la identidad y control de acceso, prevención de pérdida de datos, encriptación y administración de claves, administración de información de seguridad y cumplimiento de normas, y protección contra fraudes. Estas soluciones brindan confianza a millones de identidades de usuarios, las transacciones que realizan y los datos que se generan. Para obtener más información, visite argentina.rsa.com y argentina.emc.com.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

RSA, enVision y RSA Security son marcas registradas o marcas comerciales de RSA Security Inc. en los Estados Unidos y en otros países. EMC es una marca registrada de EMC Corporation. CERT es marca registrada de Carnegie Mellon University. Todos los otros productos o servicios mencionados son marcas comerciales de sus respectivos dueños. ©2008 RSA Security Inc. Todos los derechos reservados.

SOC WP 0808

White Paper de RSA