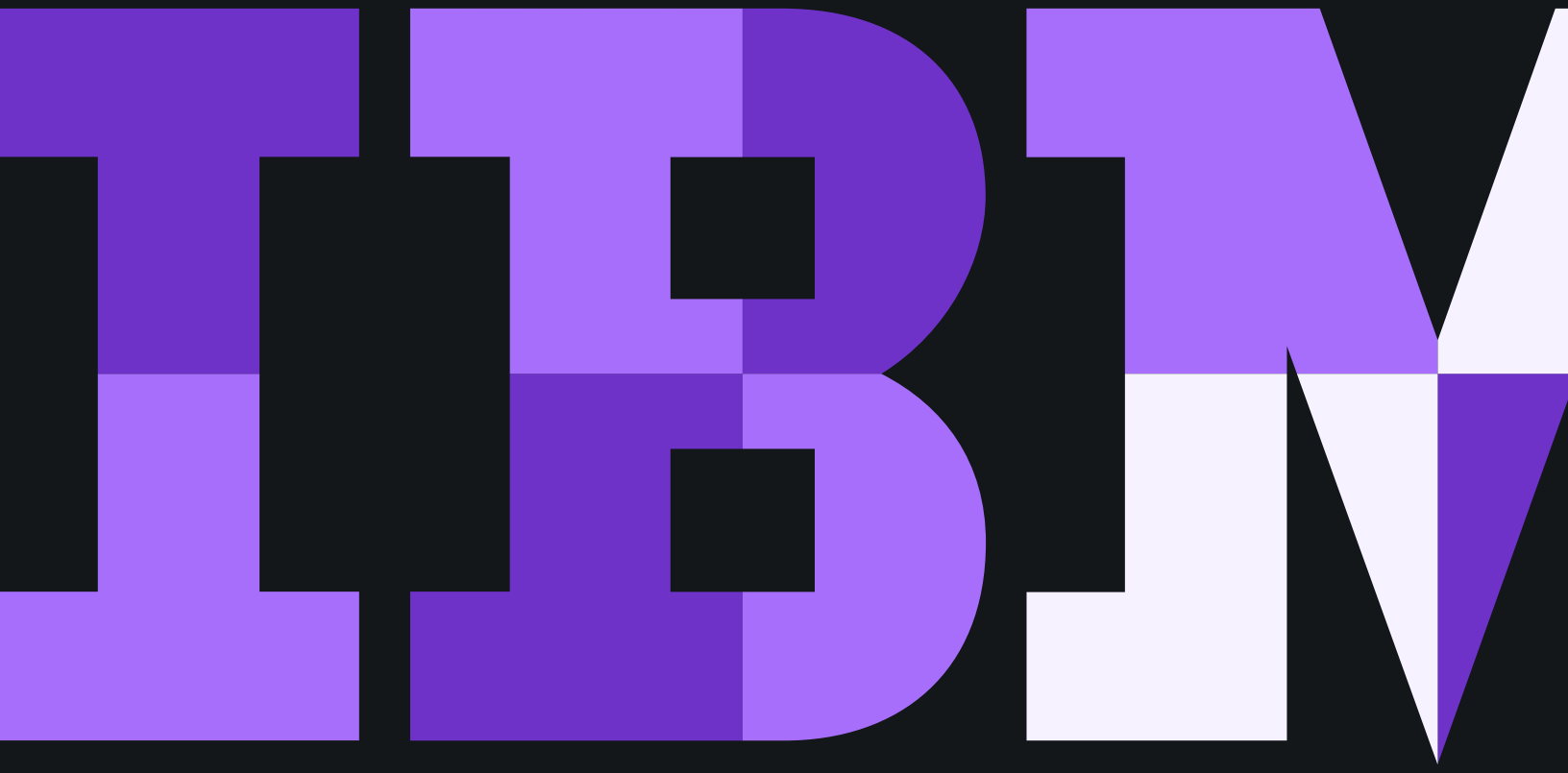
IBM **Security**

Enero de 2020

Impulse la protección

Aceleración del desempeño de la gestión de amenazas



IBM

Contenido

¿Su entorno de seguridad está construido para ganar?

En una carrera de autos, se trabaja mucho para ganar antes de que el evento comience. Los equipos de carrera buscan el mejor motor, los mejores neumáticos y toda la inteligencia que puedan obtener que les dé una ventaja en la pista. Los equipos de seguridad operan casi de la misma manera. Reúnen los mejores productos, personas y prácticas para garantizar un manejo del rendimiento de máximo nivel cuando comience la carrera por detener amenazas.

Entonces, la pregunta es, ¿qué impulsa su rendimiento de seguridad? Es posible que haya creado su propio motor de seguridad de docenas de diferentes piezas, ¿pero están ajustadas e integradas para desempeñarse a una capacidad y una eficiencia óptimas? ¿Puede ver las métricas y las condiciones de rendimiento desde un solo panel para solucionar problemas de manera eficaz, aislar problemas y responder a emergencias en tiempo real? ¿Su equipo de boxes está preparado para el ransomware o para la siguiente gran amenaza? Si no está en la pista para lidiar con las amenazas con confianza en cada vuelta, incluso sus mejores esfuerzos de seguridad podrían estancarse.

Los entornos SOC complejos de la actualidad presentan docenas de herramientas diferentes.[1] ¿Qué impulsa su éxito de seguridad?

En 2019, aún le toma 206 días a los equipos de seguridad encontrar sus amenazas más avanzadas — y otros 73 días eliminar esas amenazas de la red[2]

Elimine los puntos ciegos con una visión de 360° de la seguridad

Cada auto tiene un punto ciego, un área donde la visibilidad queda comprometida. Las soluciones de seguridad tienen puntos ciegos también. Quizás su punto ciego evita que vea amenazas difíciles de hallar o detectar problemas de cumplimiento más adelante. Donde sea que existan, los puntos ciegos ponen en riesgo la capacidad de su equipo de seguridad para identificar, protegerse y responder ante amenazas de manera oportuna.

Si desea obtener una visibilidad de 360 grados de su seguridad, necesita la telemetría correcta; es decir, un panel único en el que se recopile y reporte información sobre la seguridad. La mayoría de los equipos de seguridad enfrentan la fragmentación de información. Es posible que tengan una herramienta que informe sobre los ataques a las redes, otra que escanee el cumplimiento y una tercera que detecte las escalaciones de privilegio de acceso. Y por lo tanto, en lugar de una visión simple y holística de los datos de seguridad, los equipos de seguridad dedicaban mucho tiempo y esfuerzos a intentar unir los pedazos de la gran imagen de un mosaico de diferentes monitores y piezas móviles.

IBM Security Threat Management les da a los equipos de seguridad la visibilidad que necesitan para tener éxito. Al unificar los datos de seguridad, los equipos de seguridad pueden desplazarse con confianza; identificando no solo los datos en riesgo, sino las vulnerabilidades entre las redes, o miles de puntos finales y entre las nubes. El enfoque unificado de IBM Security ayuda a los equipos de seguridad a detectar actividades sospechosas y anomalías que a menudo se pierden en el “ruido” de las operaciones de seguridad diarias. IBM Security también proporciona los equipos de seguridad de inteligencia para amenazas que se necesitan para fortalecer su postura de seguridad y evitar riesgos.

Protéjase con las AAA: Automatización, AI (Inteligencia Artificial) y Aplicaciones

La gestión de amenazas, como una carreras de autos, combina la inteligencia humana con la maquinaria. **Los análisis de seguridad y los cazadores de amenazas son los conductores, que corren contra reloj y evitan el peligro utilizando inteligencia artificial y aprendizaje automático para acelerar sus esfuerzos con tareas y respuestas de seguridad automatizadas.** Con las soluciones de IBM Security Threat Management, se puede beneficiar con la gente capacitada que aporta mucha experiencia, y la tecnología avanzada que automatiza las tareas adecuadas para acelerar su respuesta a las amenazas urgentes.

La mayoría de las organizaciones están plagadas de datos de seguridad de diferentes aplicaciones. Es posible que tengan una herramienta de gestión de eventos e incidentes de seguridad (SIEM) de un proveedor, una solución de análisis de conducta del usuario (UBA) de otro, detección de malware de un tercero, y así sucesivamente. En caso de no filtrarse todos estos datos de seguridad, será más difícil encontrar amenazas reales, desde ransomware anidada en su red hasta credenciales en peligro que guardan las claves de datos valiosos. IBM Security Threat Management puede filtrar este ruido en forma automática, y exponer las amenazas reales en tiempo real.

Arme el equipo correcto y empodérelo

Un equipo de seguridad es como un equipo de boxes en momentos de crisis. No querrá darles un sistema complejo de herramientas de seguridad, pantallas, tableros y bases de datos, que puedan poner en peligro su agilidad y conocimiento. Deberá empoderarlos con las herramientas y la tecnología adecuadas para investigar de manera rápida y profunda indicadores de riesgo (IoC, por sus siglas en inglés), ataques de múltiples cadenas y otras señales de amenazas.

IBM Security Threat Management le brinda las herramientas que usted necesita para investigar las amenazas de manera inteligente, desde SOAR (organización de la seguridad, automatización y respuesta) hasta SIEM, el análisis avanzado y la inteligencia artificial, y las conecta con las aplicaciones de seguridad y las operaciones de TI de terceros bajo un simple tablero. El resultado es un entorno de seguridad integrado y organizado que mejora drásticamente los tiempos de respuesta, detecta las amenazas ocultas y convierte a los analistas de seguridad en cazadores maestros. Además de eso, respaldamos a su equipo con nuestro equipo: los expertos en seguridad de nivel mundial de IBM X-Force; para proporcionar inteligencia contra amenazas de manera oportuna y capacitación del mundo real que le ofrece una ventaja interna contra las amenazas cibernéticas.

65 %

de las organizaciones dicen que el volumen y la gravedad de los ataques está aumentando[3]

77 %

de las organizaciones tiene dificultades para contratar y retener profesionales de seguridad de TI[3]

Acelere su respuesta a las amenazas

Las herramientas de seguridad de múltiples proveedores no son la única fuente de fragmentación. Muchos equipos de seguridad están distribuidos en diferentes geografías, lo que dificulta la respuesta a las amenazas de manera consistente y eficaz. A medida que las amenazas se mueven por su escenario de seguridad, ¿usted presenta un frente unificado o cada analista de seguridad actúa por su cuenta? **Si no implementó un plan estratégico que incluya la respuesta automatizada a incidentes, una visión única de los datos de seguridad y las comunicaciones en tiempo real durante la resolución, su mayor amenaza podría ser tener sus propias defensas divididas.**

IBM Security Threat Management le ayuda a responder a amenazas de manera constante y rápida en toda su organización. Mediante el uso de manuales dinámicos y herramientas de seguridad automatizadas, IBM Security Threat Management ofrece una respuesta organizada a las amenazas en tiempo real que vincula a las personas con los procesos sin inconvenientes para lograr una seguridad verdaderamente unificada. Una visión holística de los datos de seguridad y de las tareas de gestión de amenazas garantiza que sus analistas de seguridad puedan coordinar su respuesta en un solo equipo, incluso si están implementados en diferentes campos de acción.

Cuando las defensas de la gestión de amenazas se unen, el negocio se mueve más rápido

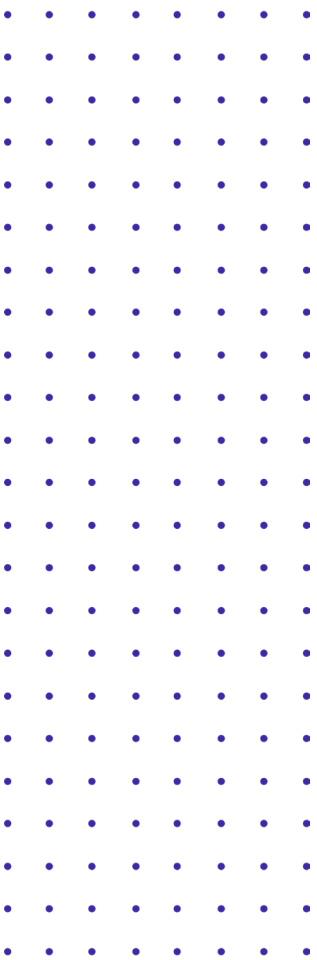
La gestión de amenazas unificada ayuda a los negocios a navegar por las amenazas de seguridad con velocidad y agilidad para poder seguir avanzando.

Vea el video

Mediante los manuales dinámicos y las herramientas de seguridad automatizadas, IBM Security Threat Management ofrece una respuesta a amenazas organizada y en tiempo real

Soluciones de IBM Security Threat Management: Construido para ganar

Puede crear su propia solución de gestión de amenazas, o puede elegir una solución diseñada con precisión por expertos. En IBM Security, nuestro registro de seguimiento habla por sí mismo, desde el reconocimiento de la industria hasta los clientes que representan a las empresas líderes del mundo. Nuestras soluciones de gestión de amenazas de seguridad presentan productos avanzados y personas excepcionales que trabajan juntas en perfecta alineación, incluyendo:



IBM Security QRadar: Una solución SIEM avanzada e inteligente que ayuda a los equipos de seguridad a visualizar, detectar y responder de manera automática a las amenazas, hasta 50 veces más rápido que la competencia.

IBM Security Resilient: Una solución SOAR líder en la industria que protege contra amenazas y acelera la respuesta a incidentes en toda la organización mediante manuales dinámicos y automatizados.

IBM Security i2: Una plataforma de inteligencia de amenazas que ayuda a los cazadores de amenazas a estar atentos y ser eficaces con una inteligencia optimizada por expertos del campo de seguridad y defensa nacional, orden público, equipos de fraudes a la industria y más.

Servicios de asesoramiento sobre inteligencia y operaciones de IBM Security: Profesionales de seguridad que evalúan, diseñan, crean y optimizan su entorno de seguridad para lograr un rendimiento superior.

IBM X-Force Red: Ofrece pruebas de penetración y programas de gestión de vulnerabilidad para ayudar a los líderes de seguridad a identificar y solucionar las fallas de seguridad que cubren todo su ecosistema digital y físico.

Servicios de gestión de amenazas de IBM X-Force: IBM X-Forces es su equipo de boxes personal para la gestión de amenazas, y le proporciona experiencia en seguridad cuando más la necesita, desde poner a prueba sus defensas de seguridad hasta luchar en la línea de batalla contra los ataques cibernéticos.

Servicios de inteligencia y respuesta ante incidentes (IRIS) de IBM X-Force: Un equipo élite de expertos de IBM X-Force que ofrece planes de respuesta ante incidentes probados e inteligencia de seguridad profunda que ayudan a su equipo de seguridad a reforzar sus defensas, combatir a los atacantes y recuperar el equilibrio luego de un ataque.

Fuentes

1. Estudio Ponemon: 53 Percent of IT Security Leaders Don’t Know If Cybersecurity Tools are Working Despite an Average of $18.4 Million Annual Spend” (Un 53 % de líderes de seguridad de TI no sabe si las herramientas de seguridad cibernética están funcionando a pesar de gastar $ 18,4 millones al año”, Business Wire (30 de julio de 2019).

2. Ponemon Institute, “2019 Cost of a Data Breach Study” (Estudio de costos de la violación de datos de 2019).

3. Ponemon Institute, “The Third Annual Study of the Cyber Resilient Organization” (El tercer estudio anual de la Organización de Resiliencia Cibernética).

IBM **Security**

IBM Global Services
Route 100
Somers, NY 10589
EE. UU.

Producido en Estados Unidos de América
Enero de 2020

PO7JWB3W