

IBM lanza tecnología abierta para acelerar la respuesta a amenazas cibernéticas en nube

- La primera capacidad de la industria para detectar las amenazas que se encuentran en varias herramientas de seguridad y nubes, sin mover los datos



ARMONK, NY. Noviembre 20, 2019. - IBM anunció hoy Cloud Pak for Security, presentando innovaciones que son primicia en la industria para conectarse con cualquier herramienta de seguridad, nube o sistema instalado localmente (on-premise), sin mover los datos de su fuente original. La nueva plataforma incluye tecnología abierta para detectar amenazas, capacidades de automatización para ayudar a acelerar la respuesta a ataques de ciberseguridad y la habilidad para ejecutarse en cualquier entorno.

Cloud Pak for Security es la primera plataforma de la industria basada en tecnologías abiertas que puede buscar y traducir datos de seguridad de una variedad de fuentes, al reunir información crítica de todo el entorno de múltiples nubes de TI de la empresa. La plataforma es extensible, de modo que se pueden agregar herramientas y aplicaciones adicionales con el tiempo.

A medida que las empresas avanzan en la adopción de nube, las aplicaciones y los datos se extienden a través de múltiples nubes públicas y privadas, así como recursos on-premise. Los intentos de proteger este entorno de TI fragmentado requieren que los equipos de seguridad realicen integraciones complejas y cambien continuamente entre diferentes pantallas y productos puntuales. Más de la mitad de los equipos de seguridad dicen que tienen dificultad para integrar datos con herramientas analíticas y de seguridad dispares y combinar esos datos en sus entornos de nube para detectar amenazas avanzadas.[1]

Tres capacidades iniciales incluyen:

- **Obtener información de seguridad sin mover datos** Transferir datos para analizarlos genera complejidad adicional. IBM Cloud Pak for Security puede conectar todas las fuentes de datos para descubrir amenazas ocultas y tomar mejores decisiones basadas en riesgo, dejando los datos donde residen. A través de la aplicación Cloud Pak for Security's Data Explorer, los analistas de seguridad pueden agilizar su búsqueda de amenazas a través de cualquier herramienta de seguridad o nube. Sin esta capacidad, los equipos de seguridad se ven obligados a buscar manualmente los mismos indicadores de amenaza (como una firma de malware o una dirección IP maliciosa) dentro de cada entorno individual. Cloud Pak for Security es la primera herramienta que permite este tipo de búsqueda sin necesidad de mover esos datos a la plataforma para su análisis.

- **Responder más rápido a los incidentes de seguridad con automatización** IBM Cloud Pak for Security conecta los flujos de trabajo de seguridad con una interfaz unificada y procedimientos de automatización para que los equipos puedan responder más rápido a los incidentes. La plataforma permite a las empresas organizar su respuesta a cientos de escenarios de seguridad comunes, guiando a los usuarios a través del proceso y brindando acceso rápido a los datos y herramientas de seguridad adecuados. La capacidad de Orquestación, Automatización y Respuesta de IBM Security se integra con procedimientos adicionales para Red Hat Ansible Automation. Al formalizar los procesos y actividades de seguridad en toda la compañía, las empresas pueden reaccionar de manera más rápida y eficiente, mientras se arman con la información necesaria para aumentar el escrutinio regulatorio.
- **Ejecutar en cualquier lugar. Conectar la seguridad de manera abierta** IBM Cloud Pak for Security se instala fácilmente en cualquier entorno: on-premise, nube privada o nube pública. Proporciona una interfaz unificada para simplificar las operaciones, compuesta por software en contenedores preintegrado con Red Hat OpenShift, la plataforma empresarial de Kubernetes más completa de la industria.

“Conforme las empresas trasladan cargas de trabajo de misión crítica a entornos híbridos multicloud, los datos de seguridad se distribuyen entre diferentes herramientas, nubes e infraestructura de TI. Esto genera brechas que dificultan la detección de amenazas, de modo que los equipos de seguridad deben recurrir a integraciones costosas y complejas o planes de respuesta manual,” señaló Mary O'Brien, Gerente General de IBM Security. “Con Cloud Pak for Security, estamos sentando las bases para un ecosistema de seguridad más conectado, diseñado para el mundo híbrido y multicloud.”

IBM colaboró con docenas de clientes y proveedores de servicios durante el proceso de diseño, desarrollando una solución para abordar los desafíos críticos de interoperabilidad que impregnan la industria de la seguridad. Cloud Pak for Security incluye conectores iniciales para integraciones preconstruidas con herramientas de seguridad populares de IBM, Carbon Black, Tenable, Elastic, BigFix, Splunk, así como proveedores de nube pública, incluidos IBM Cloud, Amazon Web Services[2] y Microsoft Azure. La solución se basa en estándares abiertos para que pueda conectar herramientas y datos de seguridad adicionales de toda la infraestructura de una empresa.

Para acelerar aún más la migración de la industria hacia la seguridad abierta, IBM también lidera proyectos de código abierto para hacer que las herramientas de seguridad trabajen juntas de forma nativa en todo el ecosistema de seguridad. Como miembro fundador de la [Open Cybersecurity Alliance](#), IBM y otras más de 20 organizaciones están trabajando juntas en estándares abiertos y tecnologías de código abierto que permiten la interoperabilidad de productos y reducen el bloqueo de proveedores en toda la comunidad de seguridad.

Diseñado para el mundo híbrido y multicloud

El 76% de las organizaciones informan que ya están usando entre dos y quince nubes híbridas, y el 98% pronostica que usarán múltiples nubes híbridas dentro de tres años.^[3] IBM Cloud Pak for Security se basa en tecnologías de código abierto que son fundamentales para el entorno de nube de las empresas, incluidos Red Hat OpenShift.

La creación de Cloud Pak for Security en estos bloques de construcción abiertos y flexibles permite una fácil implementación "en contenedores" en cualquier nube o en un entorno local. A medida que las empresas continúan agregando nuevas implementaciones y migraciones en la nube, Cloud Pak for Security se puede adaptar y escalar fácilmente a estos nuevos entornos, lo que permite a los clientes llevar incluso cargas de trabajo sensibles y de misión crítica a la nube, mientras mantienen la visibilidad y el control desde una plataforma de seguridad centralizada.

Cloud Pak for Security también proporciona un modelo para que los proveedores de servicios de seguridad administrados (MSSP) operen eficientemente a escala, conecten silos de seguridad y agilicen sus procesos de seguridad. Las organizaciones también pueden aprovechar una amplia gama de servicios de seguridad de IBM, como consultoría a pedido, desarrollo personalizado y respuesta a incidentes.

Sobre IBM Security

IBM Security ofrece uno de los portafolios más avanzados e integrados de productos y servicios de seguridad empresarial. Las soluciones, respaldadas por la investigación de renombre mundial de IBM X-Force®, permiten a las organizaciones gestionar eficazmente los riesgos y defenderse de las amenazas emergentes. IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más amplia del mundo, monitorea 70 mil millones de eventos de seguridad por día en más de 130 países y se le han otorgado más de 10,000 patentes de seguridad en todo el mundo. Para obtener más información, visite www.ibm.com/security, siga @IBMSecurity en Twitter o visite el blog de [IBM Security Intelligence](#).

[1] Encuesta de SANS Institute, [Effectively Addressing Advanced Threats](#), 2019.

[2] Disponible en el cuarto trimestre de 2019

[3] IBM Institute for Business Value, 2018
