IBM QRadar Advisor with Watson

Automatice su Centro de Operaciones de Seguridad (SOC) con Inteligencia Artificial (IA)

Puntos destacados

- Iniciar una Nueva Asociación entre los Analistas y la Tecnología
- Automatizar el Análisis de Incidentes y Obligar a Multiplicar los Esfuerzos de su Equipo
- Llevar a Cabo investigaciones Consistentes y Detalladas
- Hacer Escalamientos de Incidentes más Rápidos y Decisivos
- Disminuir el Tiempo de Permanencia

Visite nuestro sitio web

Hable con un especialista

Desafíos del SOC Hoy en Día

Ya sea que tenga un equipo de seguridad para dos o cien, sus objetivos consisten en garantizar que su negocio prospere. Y eso implica proteger sistemas esenciales, y datos, que detectan y responden a las amenazas, y estar un paso adelante del delito cibernético. Sin embargo, hay una serie de desafíos en el SOC hoy en día que podrían mermar sus facultades para cumplir sus objetivos.

Amenazas que no son solucionadas

Se pasa por alto mucha información simplemente porque sus analistas podrían no saber cómo está conectada la información. Es difícil descubrir insights sobre los cuales se pueda actuar, y sus analistas podrían, de esta manera, decidir trabajar únicamente con casos en los que se sientan seguros, lo que podría llevar a la pérdida de algunas investigaciones y podría poner en riesgo su organización.

Sobrecarga de Insights

El gran volumen, variedad y velocidad de los insights que se analizan hace difícil priorizar su trabajo y obtener una causa raíz. Eso es real en compañías de todos los tamaños, no solo en grandes empresas. Ningún analista sabe dónde empezar a unir el contexto local que los ayuda rápidamente y con efectividad a identificar el problema de inmediato. Ellos están abrumados por el trabajo repetitivo, y la mayoría de los analistas con experiencia se sienten cansados, lo que genera una crisis en los procesos definidos y una gran probabilidad de que un indicador de compromiso (IoC) importante se pierda.

El 93 por ciento[1] de las organizaciones no logra armar una escala de prioridades de las amenazas relevantes. Casi un cuarto[2] de ellas siente que tuvo suerte de haber escapado sin ningún impacto empresarial por no haber investigado estas alertas.

El Tiempo de Permanencia Está Empeorando

Una de las métricas más populares que usan los profesionales de seguridad para medir el éxito de protección y defensa de sus datos es el tiempo de permanencia; principalmente, el MTTD (Tiempo medio de detección) y el MTTR (Tiempo medio de respuesta). El tiempo de permanencia mide la duración en la que un actor malintencionado logra acceso sin ser detectado a una red hasta que se lo elimina por completo.

A pesar de tener más soluciones y datos que nunca, el promedio del tiempo de permanencia varía en cualquier lado entre 50 y 200 días. ¿Por qué es tan importante? Según el Ponemon Institute, las empresas que identifican una infracción en menos de 100 días ahorran más de 1 millón de dólares en comparación con aquellos que demoran más de 100 días. De la misma manera, las empresas que contienen una violación de seguridad en menos de 30 días ahorran más de 1 millón de dólares en comparación con aquellas que llevan más de 30 días para resolver el problema.[3]

La falta de consistencia, de investigaciones de alta calidad y de una gran cantidad de contexto lleva a una crisis en los procesos existentes y una gran probabilidad de perder insights importantes, lo que pone en peligro a su organización.

Falta de Talento para la Seguridad Cibernética y Fatiga Laboral

Como la mayoría de los analistas, su equipo probablemente trabaja en exceso, sin satisfacción y abrumado, y no es culpa de este. Es humanamente imposible estar al día con el escenario de amenazas que crece continuamente, en especial, si se tiene en cuenta lo ocupado que puede estar un equipo durante las tareas de operaciones de seguridad del día a día en su SOC.

Su organización no está sola cuando se trata de fatiga laboral en el área de seguridad cibernética. Según ESG Research, el 51 por ciento de las organizaciones afirman haber tenido una "carencia problemática" de las habilidades en la seguridad cibernética en 2018. Esto se elevó hasta el 45 por ciento en 2017.[vi] La fatiga laboral en el área de seguridad cibernética es una realidad, y de acuerdo con ESG, el 38 por ciento de los profesionales en seguridad cibernética ya dicen que la carencia de habilidades en seguridad cibernética ha generado un índice alto de desgaste laboral y agotamiento del personal. Esta situación solo prevé que empeore como la montaña de datos que continúa creciendo mientras la brecha de habilidades se sigue extendiendo con 1,8 millones de trabajos en seguridad que se espera que queden vacantes para 2022.[5]

Por lo general, los analistas de primera línea o nivel 1 son nuevos en la industria y en la fuerza laboral. Realmente les lleva tiempo desarrollar las destrezas, la confianza y la madurez en las habilidades de investigación.

Rápida Adopción de más Soluciones Específicas

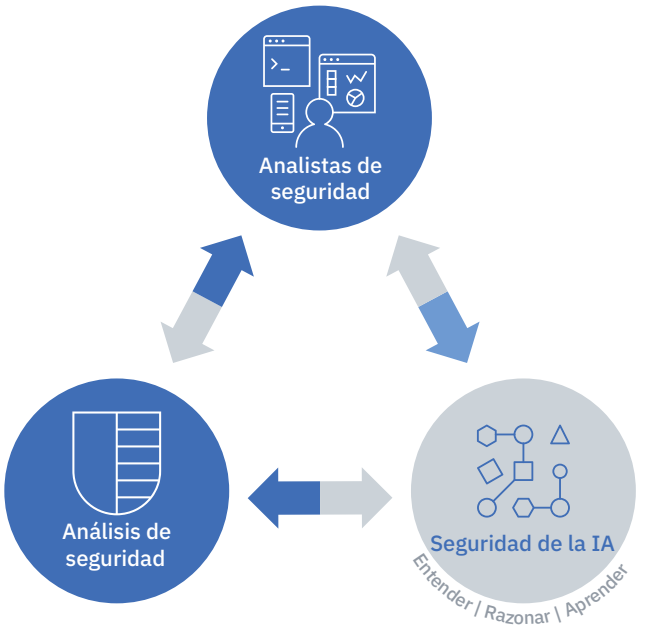
Los CISO están adoptando más soluciones específicas para detener las amenazas nuevas y evolucionadas. Independientemente de su caso de uso (protección de datos importantes, amenazas internas, gestión de identidad y acceso, abuso de credencial u otra cosa), es inevitable que cuente con una solución para eso. Por lo tanto, la integración entre la falta grave de escala y la dificultad de uso se están tornando un grave problema para las organizaciones.

Lo que Está en Juego todo el Tiempo

Con las excusas no se pagan las cuentas, ni ayudan a la hora de ganar nuevamente la confianza de un cliente insatisfecho. Según el Ponemon Institute, el costo total promedio de una violación de datos se eleva entre 3,62 y 3,86 millones de dólares, un incremento del 6,4 por ciento desde 2017.[6] Los líderes en seguridad también están enfrentando el incremento de análisis de una variedad de fuentes, incluidos el liderazgo ejecutivo, los clientes, los empleados, los inversores, los reguladores, las empresas de seguro y los grupos de vigilancia. Con lo que está en juego todo el tiempo, ¿su organización se puede permitir no estar lista?

Iniciar una Nueva Asociación entre los Analistas y la Tecnología

La inteligencia artificial une esta brecha e inicia una nueva asociación entre los analistas de seguridad y sus tecnologías. Cada uno cuenta con sus fortalezas como el sentido común con humanos y la eliminación de intereses y los análisis de compensación con la IA. Pero juntos, como equipo, pueden detener mejor las amenazas y disminuir el tiempo de permanencia.



Beneficios de la IA en el SOC

Automatizar el Análisis de Incidentes y Obligar a Multiplicar los Esfuerzos de su Equipo

No pierda capital humano en los análisis de rutina. Al contrario, deje que la IA haga de manera automatizada las tareas repetitivas de SOC, enfoque mejor a sus analistas en los elementos más importantes de la investigación, aumente la eficiencia de los analistas.

Llevar a Cabo Investigaciones Consistentes y Detalladas

¿Usted sabía que los analistas únicamente pueden estar al día con un ocho por ciento de la información necesaria para realizar sus trabajos? Para actualizar su SOC, permita de manera automática que la IA encuentre puntos en común entre los incidentes mediante el razonamiento cognitivo y brinde comentarios accionables con contexto. Considere a la IA como su consejero personal. La IA debería salir afuera y recolectar inteligencia de amenazas externas para ayudarlo a agregar más contexto a sus análisis, y debería encadenar los diferentes incidentes posibles que están relacionados entre sí con el objetivo de ahorrar tiempo.

Ya sean las 16h30min de un viernes o las 10h de un lunes, sus analistas deberían estar enfocados en realizar investigaciones consistentes y detalladas todas las veces.

Disminuir el Tiempo de Permanencia

Disminuya el MTTD y el MTTR con un proceso de escalamiento más rápido y decisivo. Para determinar el análisis de la causa raíz establezca los próximos pasos con seguridad, delinee el ataque en su libro de tácticas dinámicas, como el modelo MITRE ATT&CK.

IBM QRadar Advisor with Watson: con IA para los analistas de seguridad de primera línea

IBM® QRadar® Advisor potencia a los analistas de seguridad a llevar a cabo investigaciones consistentes y hacer escalamientos de incidentes más rápidos y decisivos, lo que genera un tiempo de permanencia reducido y un incremento de la eficiencia del analista.

Obligar a Multiplicar los Esfuerzos de su Equipo

- Dar prioridad a una lista de investigaciones con el mayor riesgo.
- Filtrar y ordenar datos más rápido según la criticidad.
- Tomar alguna acción frente a un comentario mejorado de IBM Watson® con información de inteligencia de amenazas internas y externas.

Llevar a Cabo Investigaciones Consistentes y Detalladas

- Vincular automáticamente investigaciones mediante elementos observables conectados con análisis entre investigaciones y extenderlos más allá del posible incidente actual.
- Evitar el doble esfuerzo.
- Determinar si necesita un ajuste adicional en el caso de investigaciones duplicadas generadas por los mismos eventos.

Disminuir el Tiempo de Permanencia

- Visualizar cómo ocurrió y se desarrolló el ataque, un nivel de confianza para cada progreso, qué tácticas hubo, y qué tácticas todavía podría haber con el modelo MITRE's ATT&CK.
- Sacar provecho del Scoring de incidente fácil para que sus analistas tengan un proceso de escalamiento más rápido y decisivo.
- Incrementar la eficiencia del analista y disminuir el MTTD y el MTTR.

No se quede con nuestra palabra; vea los beneficios que nuestros clientes están teniendo con la IA. Los analistas en Sogeti Luxembourg lograron disminuir el tiempo de investigación de dos a tres horas a dos a tres minutos. Ese es el tiempo valioso en el que los analistas pueden emplear mejor el tiempo en investigar en profundidad las amenazas reales y agregar más contexto a sus investigaciones.

Muchos otros clientes están usando la IA para obligar a multiplicar los esfuerzos de su equipo. Y con la IA, pueden usar trabajadores menos habilidosos para ocupar los puestos de analista del nivel 1, lo que incentiva a los analistas actuales del nivel 1 a enfocarse en las responsabilidades del nivel 2 y obligar a multiplicar los esfuerzos de sus equipos.

Para saber más de historias exitosas y obtener más información sobre cómo asociarse con la IA, visite ibm.biz/learnAI

Para obtener más información

Para obtener más información acerca de QRadar Advisor with Watson, comuníquese con su representante de ventas de IBM o visite:

ibm.com/us-en/marketplace/cognitive-security-analytics

Visite nuestro sitio web

Hable con un especialista

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Producido en los Estados Unidos de América en noviembre de 2018

1 McAfee Labs Threat Report. McAfee. 2016. (https://www.mcafee.com/ content/dam/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2016.pdf)

2 McAfee Labs Threat Report. McAfee. 2016. (https://www.mcafee.com/ content/dam/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2016.pdf)

3 Cost of a Data Breach. Ponemon, 2018. (https://www.ibm.com/security/ data-breach)

4 Cybersecurity Realities and Priorities for 2018 and Beyond. Enterprise Strategy Group. 2018. (https://www.thehaguesecuritydelta.com/media/ com_hsd/report/213/document/ESG-Research-Insights-Paper-Spirent-2018.pdf)

5 Cybersecurity Realities and Priorities for 2018 and Beyond. Enterprise Strategy Group. 2018. (https://www.thehaguesecuritydelta.com/media/ com_hsd/report/213/document/ESG-Research-Insights-Paper-Spirent-2018.pdf)

6 Cost of a Data Breach. Ponemon, 2018. (https://www.ibm.com/security/ data-breach)

Por favor recicle

24021824-COES-00