Amenazas Invisibles:

Cómo usar la IA para adelantarse a los ciberataques

La aceleración tecnológica ha impulsado un crecimiento exponencial en la cantidad de datos generados, almacenados y utilizados, lo que ha ampliado considerablemente la superficie de ataque ante las ciberamenazas. En este escenario, la inteligencia artificial (IA) ha emergido como una herramienta revolucionaria para la ciberseguridad, brindando la capacidad de anticipar amenazas y optimizar las defensas. Sin embargo, esta misma tecnología, que ofrece grandes ventajas en la protección de datos, también ha sido aprovechada por los ciberdelincuentes.

Los actores maliciosos ahora emplean IA para crear ataques cada vez más sofisticados y difíciles de detectar, como el phishing avanzado y la explotación en tiempo real de vulnerabilidades, diseñados específicamente para el blanco objetivo. De este modo, la IA se convierte en un arma de doble filo, transformando tanto la defensa como el ataque en un campo de juego más dinámico y complejo.

En 2023, las violaciones de datos alcanzaron un costo promedio de **4.88 millones de dólares**.

Fuente: Cost of a Data Breach Report 2023, IBM

GBM CYBERSECURITY CENTER | IBM | GBM

Los riesgos se intensifican con el crecimiento de agentes de IA maliciosos, capaces de automatizar y amplificar ciberataques a gran escala. Incluso, el National Cyber Security Centre advierte sobre la proliferación de IA en la sombra, es decir, sistemas no autorizados o mal gestionados que incrementan los riesgos. Sin duda, esto subraya la necesidad urgente de implementar estrategias avanzadas para proteger los activos más críticos.
El impacto de las filtraciones de datos es aún más crítico en entornos híbridos y multicloud, donde la dispersión de datos incrementa la vulnerabilidad. Según estudios recientes, el 40% de las filtraciones afecta datos almacenados en diversas plataformas, y las nubes públicas representan el mayor costo promedio por violación, con 5.17 millones de dólares por incidente.

Sin duda, la IA se convierte en un aliado indispensable para gestionar este nivel de complejidad, permitiendo identificar y proteger datos críticos, rastreando vulnerabilidades en tiempo real.

En este eBook, exploraremos la manera de proteger los datos y sistemas de su organización a través del uso de la IA. Desde anticipar amenazas hasta gestionar accesos críticos, esta guía ofrece un enfoque que transforma la forma en que las empresas enfrentan los desafíos de ciberseguridad.

¿Cómo proteger a tu empresa con IA?

En un entorno donde las amenazas evolucionan rápidamente y los datos se dispersan en múltiples entornos, es crucial replantear la estrategia de ciberseguridad:

Anticipación:

IA como herramienta para detectar riesgos futuros

En un entorno donde las amenazas avanzan a la par de la tecnología, la clave no es solo reaccionar, sino adelantarse. Las organizaciones deben adoptar un enfoque preventivo que combine análisis en tiempo real, aprendizaje automático y estrategias basadas en inteligencia artificial.

Esta capacidad de anticipación permite detectar patrones anómalos antes de que se conviertan en riesgos, cerrar brechas de seguridad críticas y priorizar recursos en los puntos más vulnerables.

La pregunta ya no es si se enfrentarán ataques cibernéticos, sino qué tan preparadas están las empresas para mitigarlos antes de que generen un impacto significativo. El futuro de la ciberseguridad radica en transformar datos en decisiones y amenazas en oportunidades para fortalecer su postura de seguridad.

GBM CYBERSECURITY CENTER | IBM | GBM

Tipos de amenazas emergentes ***impulsadas por IA***

Ataques automatizados

Bots que exploran redes en busca de configuraciones débiles y las explotan en segundos.

Phishing dirigido

Correos electrónicos personalizados generados por IA que imitan a la perfección el tono y el estilo de comunicación empresarial.

Riesgos Criptográficos Avanzados

La capacidad de romper algoritmos de cifrado más rápido mediante tecnologías como la computación cuántica.

Para las empresas, esto representa un desafío crítico: adaptarse a estas amenazas con estrategias predictivas capaces de identificar señales sutiles, reforzar configuraciones y cerrar brechas antes de que sean explotadas. Ignorar estas medidas puede resultar en afectaciones económicas significativas. Además, las brechas de seguridad dañan la reputación organizacional, afectando la confianza de los clientes y socios, lo que a menudo resulta en pérdidas de oportunidades comerciales.

Prevención inteligente:

Más allá de la respuesta reactiva

En un entorno donde las amenazas evolucionan constantemente, confiar en soluciones reactivas deja brechas críticas. Según el Cost of a Data Breach Report 2023 de IBM, el 35 % de las filtraciones estuvieron relacionadas con datos ocultos, lo que demuestra que la proliferación de datos está dificultando realizar el rastreo y la protección.

La prevención inteligente basada en inteligencia artificial se diferencia por su capacidad para analizar grandes volúmenes de datos que tiene una organización en tiempo real, identificar patrones anómalos y anticipar riesgos antes de que se materialicen.

A través del aprendizaje automático, la IA no solo detecta vulnerabilidades conocidas, sino que también predice amenazas emergentes adaptándose a nuevas tácticas de ataque. La cifra de organizaciones que usan inteligencia artificial automatizada de forma limitada también creció del 33% al 36%, según el Cost of a Data Breach Report 2023 de IBM. Por otro lado, automatiza las respuestas, corrige configuraciones inseguras y prioriza los riesgos según su nivel de criticidad, reduciendo significativamente la ventana de oportunidad para los atacantes.

GBM CYBERSECURITY CENTER | IBM | GBM

¿Cómo funciona la prevención inteligente?

1. ***Evaluación continua:*** La IA analiza configuraciones, accesos y comportamientos en tiempo real para identificar posibles riesgos.

2. ***Asignación de prioridades:*** Cada vulnerabilidad se clasifica según su nivel de criticidad, asegurando que los recursos se enfoquen en los riesgos más relevantes.

3. ***Automatización de respuestas:*** Cuando se detecta una anomalía, se toman medidas inmediatas, como bloquear accesos o aplicar parches.

La implementación de este enfoque de prevención inteligente es posible con herramientas avanzadas diseñadas para ofrecer una gestión integral de riesgos:

1

Descubrimiento y clasificación automatizada de datos

Identifican y catalogan datos sensibles en entornos locales y en la nube, proporcionando una visión integral de los activos de información.

2

Monitoreo continuo de actividades

Supervisan en tiempo real el acceso y uso de datos, detectando comportamientos anómalos que puedan indicar amenazas internas o externas.

3

Análisis avanzado de amenazas

Utilizan inteligencia artificial para analizar patrones de acceso y detectar actividades sospechosas, permitiendo una respuesta rápida y efectiva.

4

Automatización de la conformidad

Facilitan el cumplimiento de normativas mediante flujos de trabajo automatizados y generación de informes, reduciendo la carga operativa y asegurando la adherencia a regulaciones.

5

Protección de modelos de IA

Aseguran los modelos de inteligencia artificial, monitoreando su uso y detectando vulnerabilidades específicas de estos entornos.

Este enfoque proactivo no solo reduce el tiempo de exposición a amenazas, además:

- Protege la reputación empresarial.
- Mitiga costos asociados a filtraciones de datos y garantiza la continuidad del negocio.
- Evita impactos financieros.
- Evita interrupciones operativas al anticipar y neutralizar riesgos antes de que afecten sistemas críticos.

Descubrimiento de patrones inusuales:

Detectando lo que no es evidente

La identificación de patrones inusuales, mediante algoritmos que analizan el comportamiento esperado de usuarios, sistemas y aplicaciones, es clave para proteger el negocio. Detectar actividades anómalas de forma temprana permite evitar accesos no autorizados, prevenir pérdidas de datos sensibles y minimizar interrupciones operativas. Para las organizaciones, esto se traduce en mayor estabilidad, cumplimiento normativo y una reducción significativa de los riesgos financieros y reputacionales.

Factores que determinan patrones anómalos

Frecuencia	*Ubicación*	*Flujo de datos*
Accesos más frecuentes de lo habitual a ciertos sistemas.	Intentos de inicio de sesión desde ubicaciones inesperadas o no autorizadas.	Transferencias de datos inusualmente grandes o en horarios inusuales.

La inteligencia artificial no solo detecta amenazas ocultas, sino que transforma la forma en que las organizaciones gestionan su seguridad. Al analizar datos en tiempo real, la IA permite identificar patrones anómalos y actuar de inmediato para mitigar riesgos antes de que afecten las operaciones.

¿Cómo su organización puede implementarla de manera efectiva?

1. Evaluar el estado actual de su seguridad

Antes de adoptar la IA, es esencial comprender su panorama actual:

- Identifique puntos vulnerables en sus sistemas y procesos.
- Realice auditorías de accesos, datos sensibles y cumplimiento normativo.

2. Automatizar la detección de amenazas

La IA puede detectar patrones anómalos y amenazas ocultas con mayor rapidez y precisión.

- Configure monitoreo continuo en sus redes, aplicaciones y datos. Implemente algoritmos de aprendizaje automático para identificar actividades inusuales.

3. Priorizar riesgos según su impacto

No todas las amenazas tienen el mismo nivel de criticidad. Use la IA para:

- Clasificar vulnerabilidades y asignarles niveles de riesgo.
- Enfocar recursos en mitigar las amenazas más críticas.

4. Responder de manera automatizada y efectiva

Una de las mayores fortalezas de la IA es su capacidad para actuar en tiempo real.

- Programe respuestas automáticas, como el bloqueo de cuentas sospechosas.
- Genere reportes detallados que faciliten la toma de decisiones.

5. Implementar un modelo de aprendizaje continuo

La IA mejora con el tiempo, pero necesita retroalimentación constante:

- Analice los resultados de las respuestas automatizadas.
- Ajuste los modelos para adaptarse a nuevas amenazas.

6. Asegurar una integración sin fricciones

El éxito radica en la colaboración:

- Trabaje con equipos de TI, seguridad y cumplimiento para implementar estas herramientas.
- Asegúrese de que los usuarios finales entiendan su rol en la nueva estrategia de seguridad.

Soluciones como **IBM Guardium e IBM Guardium AI Security** juegan un papel esencial en este proceso, ofreciendo análisis avanzado, monitoreo continuo y capacidades de respuesta automatizada que se adaptan a los entornos tecnológicos más complejos. Integrarlas como parte de su estrategia no solo fortalece la resiliencia, sino que también asegura que su organización esté preparada para un panorama de riesgos en constante cambio.

Seguridad de datos críticos:

Protección desde la raíz

Las organizaciones deben gestionar la seguridad de los datos en todo su ciclo de vida, desde su creación y almacenamiento, hasta el acceso y la eliminación, asegurando una protección integral que abarque múltiples plataformas.

Según el Cost of a Data Breach Report 2023 de IBM, el costo promedio de una filtración de datos es de 5.27 millones de dólares. Teniendo esto en cuenta, este enfoque es crucial para evitar filtraciones en puntos vulnerables, garantizar la confidencialidad y mantener la integridad de los datos críticos, independientemente de dónde se encuentren.

Aspectos esenciales en la seguridad de datos

1) Identificación: Clasificación de datos según su nivel de sensibilidad.

- **Datos confidenciales:** Información altamente sensible como datos personales, financieros, médicos o propiedad intelectual.
- **Datos restringidos:** Información interna cuya exposición podría causar impacto moderado en la organización.
- **Datos públicos:** Información no confidencial que puede ser compartida sin riesgo.

2) Cifrado: Uso de tecnologías robustas para proteger información en tránsito y en reposo como:

- **Protocolos de cifrado avanzado:** Es una técnica para proteger los datos mediante algoritmos de cifrado.
- **Gestión de claves cifrado:** Es el proceso de generación, intercambio, almacenamiento y gestión de claves criptográficas para garantizar la seguridad de los datos cifrados.
- **Cifrado homomórfico:** Una tecnología emergente que permite realizar cálculos en datos cifrados sin necesidad de descifrarlos, ideal para entornos donde se requiere proteger datos sensibles durante procesos analíticos.
- **Cifrado basado en atributos (ABE):** Una técnica de cifrado avanzada que asocia permisos a los datos cifrados, permitiendo acceso según atributos específicos del usuario, como roles o ubicación.

3) Supervisión continua: Monitoreo de accesos y modificaciones para detectar posibles vulnerabilidades como:

Accesos no autorizados:

- **Credenciales comprometidas:** Usuarios malintencionados o atacantes externos que obtienen acceso a través de credenciales robadas.
- **Accesos desde ubicaciones inusuales:** Intentos de inicio de sesión desde geografías inesperadas o dispositivos desconocidos.

Modificaciones no autorizadas:

- **Alteración de datos críticos:** Cambios inesperados en bases de datos sensibles que podrían indicar sabotaje o fuga de información.
- **Cambios en permisos de acceso:** Ajustes no aprobados que otorgan privilegios innecesarios a ciertos usuarios o sistemas.

Anomalías en patrones de uso:

- **Volúmenes inusuales de transferencia de datos:** Grandes exportaciones de información que podrían ser señales de robo de datos.
- **Frecuencia de acceso elevada:** Repetidos intentos de acceso a datos sensibles en un periodo corto de tiempo.

Datos ocultos:

- **Almacenamiento no controlado:** Identificación de datos sensibles en ubicaciones no supervisadas o en dispositivos no autorizados.
- **Sistemas en la sombra:** Aplicaciones o servidores no documentados que acceden a datos críticos sin control.

Actividad de malware o agentes maliciosos:

- **Comportamientos automatizados sospechosos:** Bots o scripts que acceden o modifican datos a través de procesos no legítimos.
- **Intentos de escalación de privilegios:** Ataques para obtener mayores niveles de acceso al sistema.

Adoptar un enfoque integral en la gestión de datos asegura no solo su confidencialidad, sino también su integridad y disponibilidad frente a posibles incidentes.

Identidad y acceso:

Control sobre lo esencial

Garantizar que solo las personas adecuadas accedan a sistemas críticos es clave en ciberseguridad. Algunos errores suelen ser el punto de partida para ataques mayores, por ello, monitorear y controlar el comportamiento de los usuarios es esencial:

1

Gestión de contraseñas

Supervisar: Uso de contraseñas seguras y actualizaciones periódicas.

¿Cómo hacerlo?

1)Implementar gestores de contraseñas y políticas de longitud mínima y caracteres especiales.
2)Usar autenticación multifactorial (MFA) como refuerzo.

2

Monitoreo de accesos

Supervisar: Intentos de acceso desde ubicaciones inusuales o dispositivos no autorizados.

¿Cómo hacerlo?

1)Configurar alertas automáticas para actividades sospechosas.
2) Utilizar herramientas de inteligencia artificial para analizar patrones de acceso.

3

Control de permisos

Supervisar: Usuarios con permisos excesivos o desactualizados.

¿Cómo hacerlo?

1)Auditar permisos periódicamente y ajustar según el principio de privilegio mínimo.
2) Implementar soluciones de control de acceso basadas en roles (RBAC).

4

Actividad inusual de los usuarios

Supervisar: Analizar patrones de uso para detectar accesos sospechosos.

¿Cómo hacerlo?

1)Monitorear actividades en tiempo real con herramientas de detección de anomalías.
2)Generar informes automáticos de actividades críticas.

5

Gestión de cuentas inactivas

Supervisar: Cuentas de usuarios que no se han utilizado durante largos periodos.

¿Cómo hacerlo?

1)Configurar políticas de desactivación automática para cuentas inactivas.
2)Revisar accesos regularmente como parte de auditorías de seguridad.

6

Respuesta a incidentes

Supervisar: Tiempo de reacción ante alertas de accesos indebidos o actividades sospechosas.

¿Cómo hacerlo?

1)Implementar sistemas de respuesta automática que bloqueen accesos en tiempo real.
2)Ajustar automáticamente permisos según el contexto, como el horario o la ubicación.

La gestión de accesos es mucho más que restringir entradas: es el primer frente de defensa contra amenazas cada vez más sofisticadas. La incorporación de inteligencia artificial transforma este proceso al permitir una supervisión constante y la detección de anomalías en tiempo real, fortaleciendo las barreras que protegen los sistemas críticos.

En un panorama donde los errores humanos siguen siendo el eslabón más débil, garantizar que solo los usuarios correctos accedan a los recursos correctos no es solo una necesidad, sino una estrategia clave para mantener la resiliencia operativa y prevenir riesgos mayores.

La ciberseguridad del futuro:

Cómo prepararse para el cambio constante

A medida que la tecnología avanza, también lo hacen las amenazas. La evolución de la ciberseguridad no es opcional: debe adaptarse para enfrentar desafíos que incluyen ataques más sofisticados, como los impulsados por la inteligencia artificial, y normativas globales que exigen mayor transparencia y gobernanza. Las empresas que no se anticipen corren el riesgo de exponerse a pérdidas financieras, reputacionales y operativas significativas.

Tendencias de la ciberseguridad en el futuro

Adopción de AIOps para gestionar la deuda técnica

Amenazas relacionadas con arquitecturas de AI agentic

Crecimiento de la nube privada para seguridad y soberanía

Reevaluación del ROI en ciberseguridad e IA

Enfrentar el futuro de la ciberseguridad requiere un enfoque flexible que combine análisis continuo, tecnologías modernas y una mentalidad proactiva. Las organizaciones que prioricen herramientas basadas en inteligencia artificial y estrategias alineadas con las regulaciones globales estarán mejor equipadas para convertir los desafíos en oportunidades, garantizando la continuidad y el crecimiento del negocio.

Hacia un esquema más sólido y proactivo

Las amenazas cibernéticas evolucionan constantemente, entendimos que garantizar la protección de datos y sistemas es fundamental para la continuidad y el crecimiento de las organizaciones. La inteligencia artificial ha transformado la ciberseguridad, permitiendo anticiparse a los riesgos, identificar vulnerabilidades y fortalecer los puntos críticos.

GBM CYBERSECURITY CENTER | IBM | GBM

Soluciones como **IBM Guardium** e **IBM Guardium AI Security** se destacan por su capacidad de gestionar la seguridad de gran manera, permitiendo:

Adaptabilidad a entornos complejos, arquitecturas más avanzadas, brindando protección integral a través de un enfoque unificado

Garantía en la seguridad de los datos, asegurando el cumplimiento de las normativas y estándares de seguridad más rigurosos.

Detección de vulnerabilidades y respuesta automática a configuraciones inseguras o accesos sospechosos a través de inteligencia artificial para identificar patrones inusuales.

Clasificación de niveles de criticidad a las amenazas detectadas, para que las empresas puedan concentrar recursos en los riesgos más importantes.

Bloqueo de accesos no autorizados, cuarentena de identificaciones sospechosas y emisión de alertas inmediatas para contención de riesgos.

Flujos de trabajo integrados y vista unificada para que los equipos de seguridad, TI y cumplimiento trabajen de forma coordinada en la protección de datos.

Automatización de reportes que aseguren el cumplimiento con normativas globales y reduzcan los costos y riesgos de auditorías.

Para maximizar el impacto de estas tecnologías, contar con el respaldo de expertos es esencial. **GBM** combina experiencia y conocimiento técnico para implementar estas soluciones de manera personalizada, asegurando que su empresa esté preparada no solo para los desafíos actuales, sino también para los que están por venir.

Conozca más ingresando aquí:

www.gbm.net/ibmsecurity

GBM CYBERSECURITY CENTER