IA impulsada por la ciberseguridad

Descripción: La tecnología está creciendo rápidamente y el mundo está siendo moldeado por nuevas tendencias y oportunidades. Se están produciendo desarrollos interesantes en todo el espectro de tecnologías como la inteligencia artificial (IA), el Internet de las cosas (IOT), la computación en la nube, la realidad aumentada, etc. Estas tecnologías emergentes tienen sus propios beneficios y desafíos. Veamos cómo la IA está impulsada por la ciberseguridad.

Ciberseguridad (CS)

La ciberseguridad es un proceso para proteger, prevenir y detectar ataques no deseados o accesos no autorizados. La ciberseguridad es una combinación de personas, políticas, procesos y tecnologías utilizadas por las organizaciones para salvaguardar sus activos cibernéticos. La ciberseguridad se optimiza a niveles definidos por el negocio, equilibrando los requisitos de recursos con la facilidad de uso/gestión y el grado de compensación de riesgos (Glosario de Gartner). A medida que aumenta la dependencia y el uso de la tecnología, también lo hace el impacto de las amenazas y los ataques cibernéticos. Las prácticas de ciberseguridad protegen contra amenazas como el phishing, la denegación de servicio (DOS), los ataques de malware, et.al. que se originan interna o externamente en cualquier espacio empresarial o incluso personal.

Además, según el informe de la revista digital Atos (2023), existen varias categorías de amenazas cibernéticas, por ejemplo:

Amenazas de ransomware: Es un tipo de software malicioso diseñado para cifrar los archivos de la víctima y exigir el pago de la clave de descifrado.

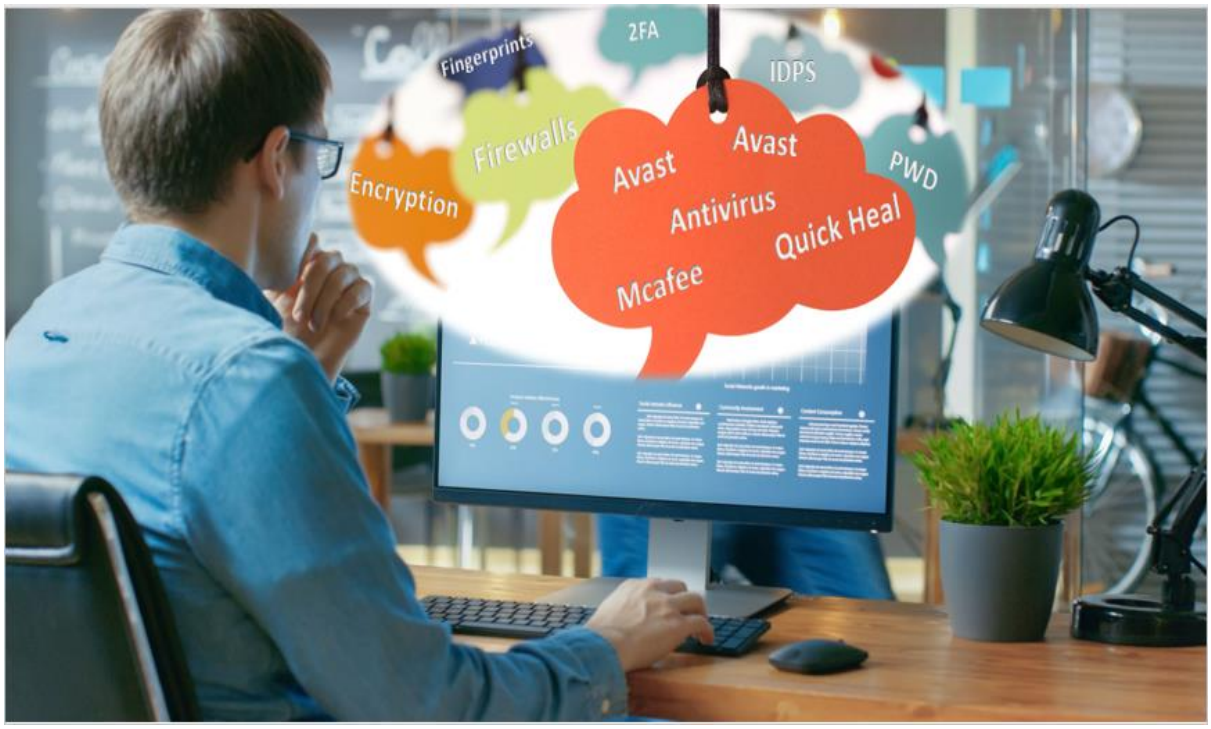
Amenazas a la cadena de suministro: Se dirige a las redes y sistemas de proveedores y vendedores que tienen acceso a los sistemas informáticos y datos de una organización. Estas amenazas pueden provocar la pérdida de datos, pérdidas monetarias y daños a la reputación.

Amenazas en la nube: Se dirige a entornos de computación en la nube, que consisten en almacenar, procesar, acceder a datos y aplicaciones en servidores de terceros con acceso a Internet.

Amenazas móviles: Se dirige a dispositivos móviles que almacenan datos confidenciales y se utilizan tanto para fines personales como profesionales.

A medida que la tecnología evoluciona y se vuelve más omnipresente en nuestra vida diaria, también aumenta la probabilidad de ataques cibernéticos. Luego, los especialistas en

tecnología idearon formas de defenderse contra los ataques cibernéticos. Estas soluciones de ciberseguridad se pueden clasificar según su funcionalidad, como la seguridad de la red, la seguridad de los datos, la seguridad de las aplicaciones, la seguridad en la nube, la gestión de accesos, etc. Estas soluciones protegen la información confidencial y, al mismo tiempo, preservan la confidencialidad de los datos.



Inteligencia artificial (IA)

La inteligencia artificial es una palabra de moda que crea mucho ruido, ya sea en los negocios, la investigación o la educación. Según la definición del NIST, la IA es una rama de la informática que se centra en la creación de sistemas de procesamiento de datos que pueden participar en actividades como el razonamiento, el aprendizaje y la superación personal que suelen asociarse a la inteligencia humana. Se puede resumir como un sistema que realiza tareas como la toma de decisiones basada en la percepción y el procesamiento del lenguaje natural que normalmente necesitarían el intelecto humano. Déjame darte un ejemplo, cuando subes imágenes a Facebook, puedes observar que el sistema detecta rostros y etiqueta automáticamente a las personas en la imagen. El sistema escanea los datos disponibles utilizando algoritmos de aprendizaje automático para reconocer rostros y detectar patrones que le permiten hacer coincidir con precisión los rostros con las personas. Facebook utiliza tecnología de reconocimiento facial impulsada por IA que funciona con algoritmos de aprendizaje profundo para poder reconocer los patrones faciales de las personas.

Cómo contribuye la inteligencia artificial al campo de la ciberseguridad?

En resumen, podemos decir que la IA es un habilitador de la ciberseguridad. La IA tiene el potencial de detectar, prevenir y responder a los ciberataques, mejorando la eficacia de las soluciones de ciberseguridad. Por ejemplo:

- Los algoritmos de IA ayudan a analizar conjuntos de datos y encontrar tendencias que apuntan a posibles ciberataques;

- También analiza los patrones de comportamiento de un virus de software malicioso y evalúa los riesgos;

- La IA tiene el potencial de mejorar los procedimientos de autenticación;

- La IA puede automatizar las respuestas a posibles ataques y reducir el tiempo de respuesta y el daño, al tiempo que predice futuros ataques.

Por otro lado, los hackers o ciberdelincuentes también utilizan la IA para aumentar el impacto de sus ataques. Los ciberdelincuentes utilizan métodos impulsados por IA para crear técnicas complejas para evadir la detección e infiltrarse en los sistemas y redes informáticas.

Mientras tanto, la ciberdelincuencia aumenta continuamente a medida que utilizamos más y más tecnología. Los analistas de operaciones de seguridad (SOA) se están centrando en la IA para detectar posibles ataques. Además, se están esforzando por personalizar para incorporar características únicas que minimicen significativamente el tiempo de respuesta a

este tipo de ataques. A partir de ahora, entendemos que la IA está apoyando las soluciones de ciberseguridad. Echemos luz sobre si la ciberseguridad es mejor que la IA.

Sin embargo, por un lado, la ciberseguridad proporciona soluciones o estrategias para proteger los sistemas, y la IA crea patrones inteligentes para aplicar esas soluciones de manera efectiva para un mejor resultado. El CSET (Centro de Seguridad y Tecnología Emergente) está trabajando en un proyecto llamado CibernéticaIA. El objetivo del proyecto es automatizar las operaciones cibernéticas y la prevención mediante el uso de la IA. El objetivo del proyecto es automatizar las operaciones cibernéticas y la prevención mediante el uso de la IA.

Según una publicación de Deloitte Insights (Tech Trends, 2022), las organizaciones pueden responder más rápido de lo que un atacante puede moverse mediante el uso de CibernéticaIA. También puede ayudarles a predecir el próximo movimiento de un atacante y preparar una respuesta inmediata. Las herramientas y la tecnología de CibernéticaIA aún se encuentran en las primeras fases de adopción. Además, la publicación también afirma que la IA puede actuar como un multiplicador de fuerza, ayudando a los profesionales de la tecnología a automatizar tareas que requieren mucho tiempo y acelerando la contención y la respuesta.

El objetivo principal de la ciberseguridad es salvaguardar los sistemas, las redes, los datos, etc., y la IA puede emplearse para reforzar las defensas de ciberseguridad. Por lo tanto, tanto la ciberseguridad como la IA son importantes para gestionar las ciberamenazas en evolución.

Referencias

CNBC Negocios. (13 de septiembre de 2022). La inteligencia artificial está desempeñando un papel más importante en la ciberseguridad, pero los malos pueden ser los que más se beneficien. AI has bigger role in cybersecurity, but hackers may benefit the most (cnbc.com)

Deloitte Insights. (2022). CibernéticaIA : Defensa Real. The future of cybersecurity and AI | Deloitte Insights

Glosario de Gartner, Definition of Cybersecurity - Gartner Information Technology Glossary

Glosario de definiciones del NIST, Laboratorio de Tecnología de la Información, Centro de Recursos de Seguridad Informática. CSRC Topics - artificial intelligence | CSRC (nist.gov)

Publicación de PWC. (2021). Equilibrio entre el poder y la protección: la IA en la ciberseguridad y la ciberseguridad en la IA. pwc-balancing-power-protection-ai-cybersecurity.pdf

Threats Predictions for -2023. (2023). The top 10 cybersecurity threats for 2023 - Atos