NÚMERO 79 | JUNIO 2023

NTT DATA
Trusted Global Innovator

Radar

El magazine de ciberseguridad

¿TENDREMOS IAG (INTELIGENCIA ARTIFICIAL GENERAL) PARA FINALES DE 2023?

El desarrollador Sigi Chen, citando fuentes anónimas, tuiteaba hace unas semanas "*Me dijeron que GPT-5 está programado para completar el entrenamiento este diciembre y que OpenAI espera que alcance la IAG*".

¿Pero, que es exactamente la IAG?

IAG o Inteligencia Artificial General es cuando una IA aprende y comprende tareas o conceptos comúnmente realizados por humanos. A diferencia de la IA especializada o estrecha, que se centra en tareas específicas y está diseñada para un propósito particular, la IAG puede adaptarse y enfrentarse a problemas nuevos y desconocidos, mostrando un nivel de autonomía y flexibilidad cognitiva similar al de los humanos. A diferencia de la inteligencia artificial, que se basa en conjuntos de datos en constante expansión para realizar tareas más complejas, la IAG exhibirá los mismos atributos que los que se relacionan directamente con el cerebro humano, se describe como un tipo de IA que permite comprender, aprender y realizar tareas intelectuales de forma muy parecida al cerebro humano. **En otras palabras, IAG, es la capacidad de la IA de aprender del mismo modo que los humanos.**

La IA se refiere a una máquina que puede copiar las capacidades cognitivas humanas, como la resolución de problemas y el aprendizaje. Pero un humano tiene que programar primero la máquina para que pueda aprender de patrones pasados para crear nueva información o resolver un problema. Mientras que la IA está preprogramada para llevar a cabo una tarea que un humano puede realizar, pero de forma más eficiente, la IAG espera que la máquina sea tan inteligente como un humano. Hasta la fecha, la IAG es un objetivo en la investigación de inteligencia artificial, pero aún no se ha logrado.

Como todas las tecnologías, la IAG tiene su lado bueno (aumentar la productividad al acelerar los procesos habilitados por la IA y liberar a los humanos del trabajo repetitivo, impulsar la economía global o ayudar a conseguir nuevos descubrimientos científicos) y su lado digamos "imprevisto o menos bueno" (propagación de bots de apariencia humana extremadamente convincentes en plataformas de redes sociales, concentración de esta tecnología en pocas manos, desplazamiento laboral, uso indebido).

Precisamente para evitar estos últimos efectos no deseados, se debe trabajar más en conseguir que estos sistemas sean más precisos, seguros, interpretables y transparentes, para ello se debería trabajar con los legisladores y promover el desarrollo de sistemas sólidos de gobierno de IA, estos deberían incluir como mínimo: autoridades reguladoras nuevas y capaces dedicadas a la IA, así como supervisión y seguimiento de sistemas de IA de alta capacidad y grandes volúmenes de capacidad computacional, en este sentido ya tenemos algunas iniciativas como la **Ley de Inteligencia Artificial (AI Act),** que es un reglamento propuesto el 21 de abril de 2021 por la Comisión Europea cuyo objetivo es introducir un marco normativo y jurídico común para la inteligencia artificial, pero está claro que hay que seguir trabajando en esta línea.

Si finalmente ChapGPT 5 conseguirá la IAG o no, es algo que está por ver, y al igual que pasa con otros temas de tecnología de última generación como la supremacía cuántica (el momento en el que un procesador cuántico sea capaz de realizar una determinada tarea que no pueda ser ejecutada por ningún ordenador clásico en una cantidad de tiempo razonable), hay opiniones de todo tipo, de los que piensan que ya se ha obtenido (en concreto por científicos chinos) a los que, mucho más escépticos, piensan que nunca se conseguirá, lo cierto es que hay muchas personas y esfuerzo detrás de todos estos temas y al menos respecto a la IAG, puede que salgamos de dudas a finales de este mismo año ChapGPT-5 mediante….!!! y esperemos que para entonces se haya cubierto el puesto que publicaba hace días OPEN AI que buscaba un "**ingeniero para un interruptor de muerte**" (o de apagado) que debería estar pendiente de desconectar los servidores en caso de catástrofe….

María Ángeles Gutierrez

Manager de Ciberseguridad en NTT DATA Europe & Latam

© 2023 NTT DATA. Todos los derechos reservados. Prohibido su uso, copia, reproducción, divulgación, distribución, difusión o modificación, total o parcial, con fines comerciales sin autorización de su titular.

CIBERCRÓNICA

Comenzamos esta nueva edición del RADAR con el siguiente mensaje, la seguridad en línea sigue siendo una preocupación constante para las empresas y los usuarios de todo el mundo. Recientemente, el consultor de redes sociales y analista Matt Navarra informó en Twitter que los piratas informáticos habían ingresado en páginas verificadas de Facebook para publicar anuncios que distribuyen malware.

Uno de los sitios pirateados, Meta Ads, engañó a los usuarios para que descargaran una herramienta de administración 'más profesional y segura' debido a problemas de seguridad en el navegador. Sin embargo, en lugar de descargar una herramienta legítima, el enlace redirigió a los usuarios a una página web infectada con malware. La otra página pirateada pretendía ser Google AI y dirigía a los usuarios a enlaces falsos para acceder al chatbot de inteligencia artificial de Google. Ambas páginas podían comprar anuncios de Facebook y distribuir enlaces de descarga sospechosos.

> "Por lo tanto, es importante no fiarse nunca de los enlaces de supuestas webs oficiales que te envían por correo electrónico o SMS"

Afortunadamente, ambas páginas pirateadas fueron desactivadas, y Meta lanzó un programa de verificación llamado 'Meta Verified' para aumentar la seguridad de la plataforma. Sin embargo, los usuarios de Facebook e Instagram que deseen tener una protección proactiva de la cuenta deberán pagar un mínimo de doce euros al mes.

Este incidente destaca la importancia de la seguridad en línea y la necesidad de que las empresas implementen medidas de seguridad más sólidas para proteger a sus usuarios de los piratas informáticos. Sin embargo, no es solo la seguridad de las plataformas de redes sociales lo que debemos tener en cuenta.

Por otro lado, con la temporada de impuestos en marcha, los timadores también están aprovechando la oportunidad para engañar a las personas a través de correos y mensajes masivos con engaños en los que intentan que alguien pique en la trampa. Estos ataques, conocidos como phishing, consisten en enviar mensajes masivamente como si lanzaran cientos de miles de anzuelos, con la esperanza de que alguien pique en la trampa.

Los timadores utilizan tácticas engañosas, a menudo afirmando que Hacienda te va a devolver dinero. Además pueden incluir enlaces a páginas web fraudulentas que parecen oficiales, pero que están diseñadas para robar información personal, como números de tarjetas y códigos de seguridad. Estas páginas web son falsificaciones que utilizan logos y tipografías de Hacienda para parecer una web oficial. Es recomendable buscar la web de la Agencia Tributaria o donde queramos acceder, entrar en la página oficial y autenticarse desde ahí para buscar posibles notificaciones. En resumen, la seguridad en línea sigue siendo una preocupación constante. Con la temporada de impuestos en marcha, es importante tener precaución y estar atentos a los correos y mensajes que recibimos, ya que muchos de ellos pueden ser fraudulentos. Las empresas también deben implementar medidas de seguridad más sólidas para proteger a sus usuarios de los piratas informáticos.

© 2023 NTT DATA. Todos los derechos reservados. Prohibido su uso, copia, reproducción, divulgación, distribución, difusión o modificación, total o parcial, con fines comerciales sin autorización de su titular.

También cabe destacar la siguiente noticia. El Instituto Nacional de Ciberseguridad (INCIBE) está alertando sobre una nueva táctica fraudulenta en la que se suplanta la identidad de la Seguridad Social mediante el smishing.

El propósito de este engaño es obtener datos personales de las víctimas a través de un sitio web fraudulento que contiene un formulario. Los mensajes de texto indican que es necesario actualizar la tarjeta sanitaria utilizando el enlace adjunto en el cuerpo del mensaje. Si el usuario hace clic en la URL, será redirigido a un sitio web malicioso que solicita completar un formulario con la siguiente información: nombre, apellido, correo electrónico y fecha de nacimiento. Una vez que se ingresan estos datos, los ciberdelincuentes tendrán acceso a toda la información necesaria para llevar a cabo ataques cibernéticos y engañar a las víctimas.

Por otro lado, el INCIBE advierte que no se descarta la existencia de otras campañas similares a través de correos electrónicos solicitando la misma información. Además, los mensajes de texto reportados hasta ahora contienen errores ortográficos en su redacción, lo cual genera sospechas sobre su autenticidad.

Otra noticia curiosa, ahora que está muy de moda el uso de las IAs, y en concreto chatGPT, es la que ha sacado a la luz Meta, que ha detectado en la red enlaces a apps que simulan ser ChatGPT con malware. Meta ha revelado algunas de las acciones tomadas durante el primer trimestre de 2023 para enfrentar las amenazas detectadas en sus aplicaciones dirigidas a personas y empresas. Estas amenazas incluyen campañas de malware en las que los delincuentes cibernéticos simulan aplicaciones de ChatGPT, así como la identificación de nueve redes antagónicas involucradas en operaciones de espionaje cibernético.

En su comunicado en el sitio web, Meta detalla que uno de los tipos de ataque más destacados durante este período han sido las campañas de malware en las que los ciberdelincuentes aprovechan temas populares, como la tecnología de Inteligencia Artificial (IA) generativa con ChatGPT, para llamar la atención de los usuarios. Específicamente, la compañía informa que, desde marzo, sus analistas han identificado alrededor de diez familias diferentes de malware que suplantan aplicaciones de ChatGPT y herramientas similares. También se han detectado campañas relacionadas con estafas criptográficas.

En estas campañas, los actores maliciosos creaban extensiones de navegador maliciosas disponibles en tiendas web oficiales, ofreciendo falsas herramientas relacionadas con la IA. En ocasiones, estas extensiones incluso incluían funciones reales de ChatGPT junto con el malware, para camuflarse y evitar levantar sospechas. Sin embargo, el equipo de investigadores de Meta logró bloquear más de mil extensiones maliciosas de estas campañas de malware para evitar que los usuarios las compartieran en sus aplicaciones. Asimismo, la empresa informó sobre estas campañas maliciosas a otras aplicaciones de intercambio de archivos de la industria, para que también tomen las medidas adecuadas.

También se ha detectado una nueva estafa que consiste en suplantar a la empresa FedEx para extraer los datos bancarios de los clientes. La estafa se realiza mediante el envío de un correo electrónico fraudulento en el cual, con la excusa de abonar un pago para recibir un paquete de FedEx, redirige por medio de un enlace a una encuesta y a dos formularios que solicitan datos personales y bancarios. Si el destinatario ha recibido un mensaje de correo electrónico supuestamente de FedEx, en el cual se le solicita realizar un pago para recibir un paquete, pero no ha compartido su información personal, es recomendable que el usuario marque dicho correo como spam y lo elimine de su bandeja de entrada.

© 2023 NTT DATA. Todos los derechos reservados. Prohibido su uso, copia, reproducción, divulgación, distribución, difusión o modificación, total o parcial, con fines comerciales sin autorización de su titular.

¿POR QUÉ LAS IAS PUEDEN AYUDAR EN EL TRABAJO DIARIO DE UN EMPLEADO DE CIBERSEGURIDAD Y QUÉ PAPEL TIENEN?

Por: NTT DATA Europe & Latam

La inteligencia artificial (IA) es una rama de la informática y la ciencia de la computación que se enfoca en desarrollar sistemas o programas que pueden realizar tareas que, en general, requieren inteligencia humana, como el aprendizaje, la percepción, el razonamiento y la resolución de problemas. Los sistemas de IA utilizan técnicas y algoritmos que les permiten aprender de la experiencia y mejorar su desempeño con el tiempo. Estas técnicas incluyen por ejemplo el aprendizaje automático (machine learning), el procesamiento del lenguaje natural (natural language processing), la visión por computadora (computer vision) y la robótica, entre otras muchas.

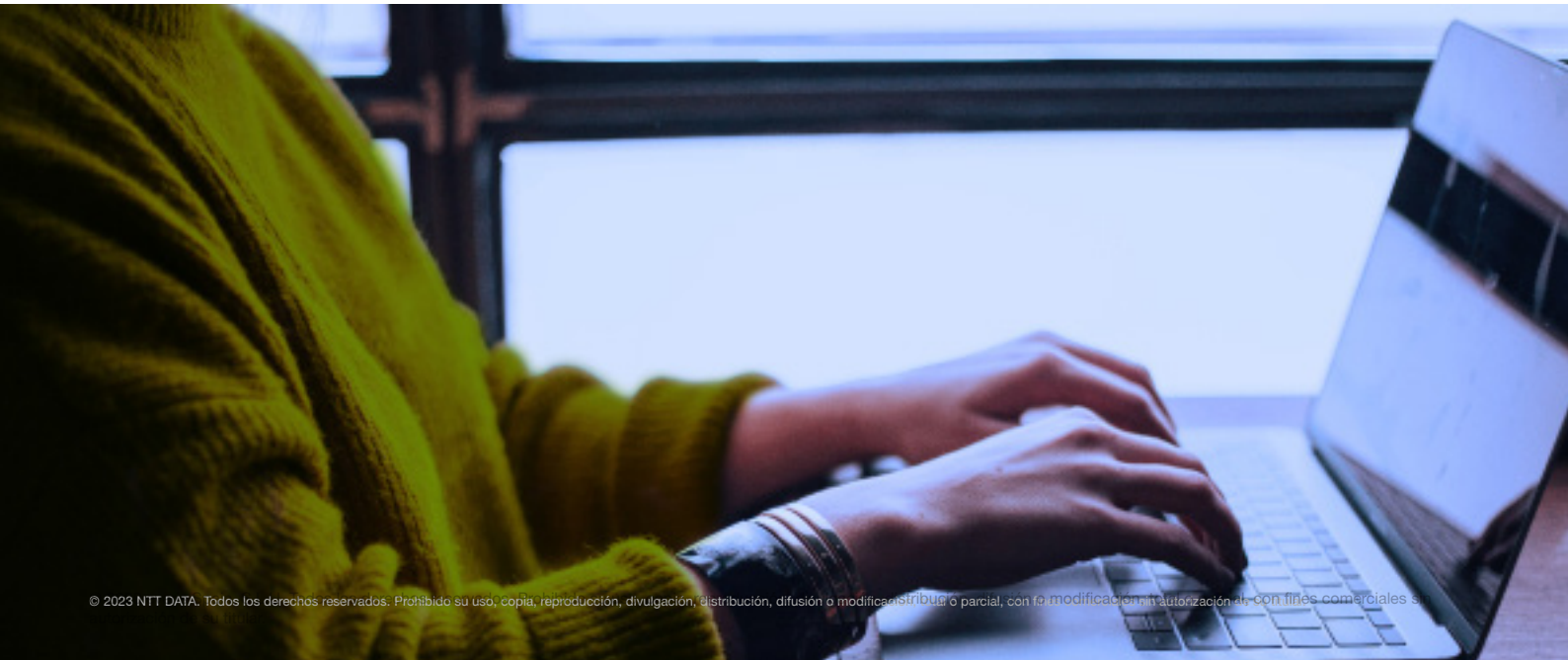
La IA se aplica en una amplia variedad de campos, como la medicina, la educación, la industria, el comercio y el entretenimiento. Su potencial para mejorar la eficiencia y la calidad de vida es enorme, aunque también plantea importantes desafíos éticos y sociales que deben ser abordados.

¿Qué tipos de IAs existen actualmente?

Aunque al pensar en las inteligencias artificiales se nos venga a la cabeza ChatGPT o DALL-E 2, lo cierto es que no son las únicas. Existen varios tipos de inteligencia artificial, cada uno con su propio enfoque y aplicación. Algunos de los tipos más comunes de IA incluyen:

- **Sistemas expertos:** son sistemas que utilizan conocimientos específicos de expertos humanos en un campo determinado para tomar decisiones y realizar tareas. Se utilizan en campos como la medicina, la ingeniería y la gestión empresarial.
- **Aprendizaje automático:** es un tipo de IA que utiliza algoritmos para permitir que los sistemas aprendan y mejoren a través de la experiencia. Se utiliza en aplicaciones como la detección de fraude, el reconocimiento de patrones y la toma de decisiones.
- **Redes neuronales:** son sistemas de IA que imitan la estructura y el funcionamiento del cerebro humano. Se utilizan en aplicaciones de reconocimiento de imágenes y de voz, así como en la toma de decisiones en tiempo real.
- **Procesamiento del lenguaje natural:** es un tipo de IA que permite a los sistemas comprender y responder al lenguaje humano. Se utiliza en aplicaciones como los chatbots y los asistentes virtuales.
- **Robótica:** es un campo de la IA que se enfoca en el desarrollo de robots inteligentes y autónomos que pueden realizar tareas físicas en entornos complejos.

Cada tipo de IA puede dar lugar a un sinfín diferentes aplicaciones ya que cada una puede ser entrenada para realizar funcionalidades distintas.



© 2023 NTT DATA. Todos los derechos reservados. Prohibido su uso, copia, reproducción, divulgación, distribución, difusión o modificación, distribución parcial, con o modificación, autorización ar, con fines comerciales s

¿Cómo están entrenadas en el ámbito de la ciberseguridad?

Las inteligencias artificiales (IA), como ChatGPT, no están necesariamente diseñadas específicamente para el ámbito de la ciberseguridad, pero pueden ser entrenadas para realizar tareas relacionadas con la seguridad informática.

El entrenamiento de una IA para la ciberseguridad implica enseñarle a reconocer patrones y anomalías en los datos, y a tomar decisiones basadas en esa información. Esto se logra a través de la alimentación de la IA con grandes cantidades de datos de seguridad, como registros de actividad de red, registros de eventos de seguridad, registros de aplicaciones y datos de amenazas conocidas.

Una vez que la IA ha sido entrenada en la identificación de patrones y anomalías, puede aplicarse a diversas tareas de ciberseguridad, como la detección de intrusiones, la identificación de malware, la monitorización de la actividad de red, la predicción de comportamientos maliciosos, y la respuesta automática a eventos de seguridad.

Para mantener una IA de ciberseguridad efectiva, es necesario que se actualice regularmente con nuevos datos y técnicas de amenazas. También es importante que las decisiones tomadas por la IA se supervisen y se ajusten según sea necesario para garantizar la precisión y la efectividad en la protección de los sistemas informáticos y los datos.

Para ChatGPT, el modelo GPT-3.5 se entrena en una gran cantidad de datos no estructurados de diferentes fuentes, que incluyen páginas web, libros, artículos de noticias, foros y redes sociales, con el objetivo de aprender patrones y asociaciones en el lenguaje natural. A través de esta capacitación continua, el modelo se vuelve cada vez más preciso y efectivo en su capacidad para entender y generar lenguaje natural.

¿En que pueden ayudar a los perfiles de ciberseguridad estas IAs?

Las inteligencias artificiales pueden ayudar en múltiples formas a los perfiles de ciberseguridad, ya que permiten analizar grandes cantidades de datos de seguridad en tiempo real, identificar patrones y anomalías, y tomar decisiones automatizadas para detectar y responder a amenazas de seguridad.

A continuación, se presentan algunas formas en las que las inteligencias artificiales pueden ayudar a los perfiles de ciberseguridad:

1. **Detección de amenazas:** Las IA pueden analizar grandes cantidades de datos de seguridad en tiempo real y detectar patrones o comportamientos sospechosos en la actividad de la red o en los sistemas informáticos. Al identificar estos comportamientos, las IA pueden alertar a los equipos de seguridad para que investiguen y respondan a la amenaza.
2. **Análisis de vulnerabilidades:** Las IA pueden analizar sistemas y aplicaciones para detectar vulnerabilidades conocidas o desconocidas. Los equipos de seguridad pueden utilizar esta información para identificar y corregir las vulnerabilidades antes de que sean explotadas por atacantes.
3. **Identificación de malware:** Las IA pueden analizar patrones de comportamiento de software y detectar malware que se ha infiltrado en un sistema informático. Esto puede ayudar a los equipos de seguridad a identificar rápidamente la amenaza y tomar medidas para mitigarla.
4. **Gestión de incidentes de seguridad:** Las IA pueden ayudar en la gestión de incidentes de seguridad, proporcionando una respuesta rápida y automatizada a eventos de seguridad. Por ejemplo, las IA pueden tomar medidas para detener un ataque o bloquear un comportamiento sospechoso mientras el equipo de seguridad investiga el incidente.
5. **Monitoreo continuo:** Las IA pueden monitorear continuamente la actividad de red y los sistemas informáticos para detectar y responder a amenazas en tiempo real. Esto puede ayudar a los equipos de seguridad a mantener una postura de seguridad más proactiva y efectiva.

En resumen, las IA pueden ayudar a los perfiles de ciberseguridad en la detección de amenazas, análisis de vulnerabilidades, identificación de malware, gestión de incidentes de seguridad y monitoreo continuo. Al automatizar estas tareas y permitir una respuesta más rápida y precisa a los eventos de seguridad, las IA pueden mejorar significativamente la postura de seguridad de una organización.

© 2023 NTT DATA. Todos los derechos reservados. Prohibido su uso, copia, reproducción, divulgación, distribución, difusión o modificación, total o parcial, con fines comerciales sin autorización de su titular.

APLICACIONES DE LA INTELIGENCIA ARTIFICIAL EN LA CIBERSEGURIDAD

Por: NTT DATA Europe & Latam

La seguridad cibernética se ha convertido en una de las principales preocupaciones para individuos, empresas e instituciones gubernamentales de todo el mundo. Con la creciente cantidad de datos y dispositivos conectados a la red, la ciberdelincuencia ha aumentado de manera exponencial en los últimos años. Afortunadamente, la inteligencia artificial (IA) puede ser una herramienta valiosa en la lucha contra el crimen cibernético.

La IA tiene el potencial de revolucionar la ciberseguridad de muchas maneras. En primer lugar, los algoritmos de aprendizaje automático pueden analizar grandes cantidades de datos para identificar patrones y anomalías en el tráfico de red y en los registros de actividad. Estos patrones pueden ayudar y alertar a los profesionales de la seguridad antes de que ocurra un incidente que ponga en riesgo la infraestructura de la organización.

Además, la IA puede ser utilizada en motores de análisis de virus y para mejorar la detección de malware. Los algoritmos de aprendizaje automático pueden analizar el código de un programa y comparar la muestra con un conjunto de datos conocidos para determinar si se trata de software malicioso. Estos algoritmos pueden detectar patrones de comportamiento en los sistemas que indican una infección por malware.

Otra aplicación importante de la IA en la ciberseguridad es la identificación de amenazas internas. A menudo, los ataques informáticos pueden provenir de dentro de la propia organización, ya sea por negligencia o intencionalidad. La IA puede analizar los patrones de comportamiento de los empleados para detectar actividad sospechosa y alertar a los profesionales.

La IA también puede ser utilizada para mejorar la autenticación y la identificación de usuarios. Los sistemas de autenticación basados en la IA pueden analizar el comportamiento del usuario, como los patrones de tecleo y la forma en que interactúa con la interfaz de usuario, para determinar si un usuario es legítimo o impostor.

En última instancia, la IA puede ayudar a mejorar la capacidad de respuesta ante incidentes de seguridad integrándolo con mecanismos de automatización. Los sistemas de IA pueden ser programados para tomar medidas inmediatas cuando se detecta un comportamiento sospechoso, como desconectar un dispositivo de la red o bloquear el acceso a una cuenta. Esto puede ayudar a prevenir el daño antes de que se produzca y limitar la propagación del ataque.

A pesar de los beneficios potenciales de la IA en la ciberseguridad, también hay preocupaciones sobre su uso. En particular, la privacidad y la ética son cuestiones importantes para tener en cuenta. La IA puede ser utilizada para recopilar y analizar grandes cantidades de datos sobre los usuarios, lo que plantea cuestiones de privacidad. Esto puede incluir la implementación de políticas claras y transparentes sobre el uso de la IA, así como la adopción de prácticas de privacidad y seguridad sólidas.

Otra preocupación es la posibilidad de que los atacantes utilicen la IA para llevar a cabo ataques cibernéticos más sofisticados.

Además, los sistemas de IA utilizados en la ciberseguridad deben ser rigurosamente probados y evaluados para garantizar su eficacia y fiabilidad. Los perfiles de seguridad deben trabajar en colaboración con los desarrolladores de IA para garantizar que los sistemas sean capaces de detectar una amplia gama de amenazas y adaptarse a los nuevos riesgos a medida que vayan surgiendo.

Existen diversas herramientas de ciberseguridad que utilizan inteligencia artificial para mejorar su eficacia en la detección y prevención de ataques cibernéticos. Algunos ejemplos de estas herramientas son los siguientes:

© 2023 NTT DATA. Todos los derechos reservados. Prohibido su uso, copia, reproducción, divulgación, distribución, difusión o modificación, total o parcial, con fines comerciales sin autorización de su titular.

1. **Darktrace:** esta herramienta utiliza algoritmos de aprendizaje automático para analizar los patrones de tráfico de red y detectar amenazas en tiempo real. Es capaz de detectar incluso las amenazas más sofisticadas, como ataques zero-day y amenazas internas.
2. **Cylance:** es una herramienta Endpoint Protection Platform (EPP) que utiliza inteligencia artificial para identificar y prevenir ataques de malware. La herramienta utiliza un motor de aprendizaje automático para analizar el código de los programas y determinar si son maliciosos o no.
3. **Palo Alto Networks:** puede utilizarse para mejorar la detección de amenazas y la prevención de ataques. La herramienta utiliza algoritmos de aprendizaje automático para analizar el tráfico de red y detectar patrones sospechosos.
4. **McAfee:** utiliza inteligencia artificial para mejorar la detección y prevención de ataques de malware y amenazas internas. La herramienta utiliza algoritmos de aprendizaje automático para analizar el comportamiento del usuario y detectar actividades sospechosas.

Es importante recalcar que la IA no es una solución perfecta para la ciberseguridad. Si bien puede ayudar a detectar y prevenir ataques, no puede reemplazar completamente a profesionales cualificados. Debe ser utilizada como una herramienta complementaria para mejorar la eficacia de la seguridad cibernética y no como una solución única.

TENDENCIAS

CIBERSEGURIDAD DEL INTERNET DE LAS COSAS (IOT)

Si bien en nuestra última edición explicamos algunas generalidades de ChatGPT (chatbot desarrollado por OpenAI) en cuanto a su definición, objetivo, pros y contras de cara al usuario común, se hace necesario también hablar del impacto que comienza a forjarse a nivel corporativo para su adopción y gracias a la evolución del modelo GPT.

Desde que se liberó su uso en noviembre 2022, ChatGPT ha sido el foco de un debate constante en materia de seguridad. Sin embargo, es importante hacer una retrospectiva para darnos cuenta de su progreso y el papel de tenerlo como aliado para darle ese tinte de confiabilidad en el ámbito empresarial.

Como es sabido por todos, OpenAI es una compañía gobernada por la organización sin ánimo de lucro -OpenAI Incorporated- pero además conformada por otra subsidiaria con fines de lucro -OpenAI Limited Partnership., Desde que comenzaron a desarrollar su idea en el 2015 fue solo hasta el 2019 cuando dieron inicio a su relación con uno de los gigantes tecnológicos -Microsoft- para entrenar sus modelos con tecnología Azure, facilitando de esta manera que OpenAI no renunciara a su propósito de investigación y por otro lado, Microsoft continuara madurando sus productos como su proveedor exclusivo en la nube hasta tal punto de llegar a implementar una interfaz de aplicaciones (API) que le permitiera su llegada tanto al mundo empresarial como a los desarrolladores para construir soluciones de una manera más segura sobre sus modelos GPT, CODEX y DALL-E

En términos sencillos, los definiremos:

- GPT, ejecuta una variedad de tareas de lenguaje natural, usado para ejecutar preguntas-respuestas, resúmenes de texto, traducción automática y conversación AI.
- CODEX, basado en GPT-3 convierte el lenguaje natural en código. No está diseñado para reemplazar el trabajo de los programadores, lo que busca es ayudarles en la codificación de ciertos fragmentos rutinarios u optimizar código existente.
- DALL.E, crea imágenes a partir de una descripción en lenguaje natural.

Con todo el auge y las bondades del ChatGPT, algunos de estos modelos pueden pasar desapercibidos, aunque ya empiezan a cobrar relevancia en el entorno de las grandes compañías para aportar mejoras en los tiempos de respuesta, en efectividad y en la experiencia de usuario, factores que vienen siendo determinantes en los últimos años en la interacción de usuario con respecto a un producto o servicio.

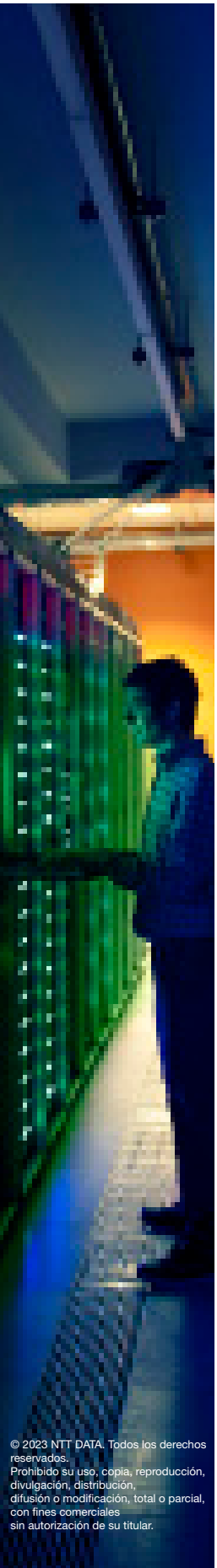
Finalmente, es sumamente importante aclarar que el simple hecho de contar con uno de estos módulos, no implica que todo funcionará como por arte de magia para la organización, hay que ser conscientes que solo forman una parte de la solución y alrededor de ellos habrá una pieza importante para trabajar sobre los controles a implementar en la comunicación de los servicios a ser definidos en el backend y asegurar que tanto los usuarios internos como externos que tengan acceso sean validados y reciban lo que sus funciones les permitan.

Para esto, se hace necesario no perder de vista dos conceptos que siempre irán de la mano y son complementarios en el éxito de una solución hoy, **seguridad** y **privacidad**. La **seguridad** orientada a protegerse contra las amenazas maliciosas mientras que la **privacidad** garantiza que solo aquellos usuarios que estén autorizados para acceder a los datos puedan hacerlo.

© 2023 NTT DATA. Todos los derechos reservados. Prohibido su uso, copia, reproducción, divulgación, distribución, difusión o modificación, total o parcial, con fines comerciales sin autorización de su titular.

VULNERABILIDADES

Reciba nuestro boletín completo de parches y vulnerabilidades suscribiéndose **aquí**.



Gitlab

CVE-2023-2478
Fecha: 05/05/2023

Descripción. El pasado 8 de mayo, Gitlab publicó una actualización de seguridad provocada por una vulnerabilidad crítica encontrada en múltiples versiones de Gitlab Community Edition (CE) y Gitlab Enterprise Edition (EE). Se ha asignado el identificador CVE-2023-2478 a esta vulnerabilidad. Mediante su explotación y si se cumplen ciertas circunstancias, un usuario de Gitlab podría utilizar un endpoint de GraphQL para adjuntar un ejecutable malicioso a cualquier proyecto. Este fallo de seguridad se produce debido a la asignación incorrecta de permisos para acceder recursos críticos del sistema.

Enlace: https://about.gitlab.com/releases/2023/05/05/critical-security-release-gitlab-15-11-2-released/#malicious-runner-attachment-via-graphql
https://www.incibe.es/incibe-cert/alerta-temprana/avisos/vulnerabilidad-en-community-edition-ce-y-enterprise-edition-ee-de-gitlab

Productos afectados. Esta vulnerabilidad afecta a las siguientes versiones de Gitlab Community Edition (CE) y Gitlab Enterprise Edition (EE).

- desde la 15.4 hasta la 15.9.7,
- desde la 15.10 hasta la 15.10.6,
- desde la 15.11 hasta la 15.11.2.

Solución: La solución principal para solventar esta vulnerabilidad consiste en actualizar a las últimas versiones, según corresponda:

- 15.11.2
- 15.10.6
- 15.9.7

Aruba

CVE-2023-22779,-22780,-22781,-22782,-22783,-22784,-22785,-22786,-22787,-22788,-22789,-22790,-22791
Fecha: 09/05/2023

Descripción. Se han descubierto un total de 13 vulnerabilidades en productos de Aruba, 8 de ellas de severidad crítica, 4 altas y una media. Las categorizadas con severidad alta se corresponden con múltiples vulnerabilidades de inyección de comandos de forma remota y una vulnerabilidad de denegación de servicio. Por otro lado, las 8 vulnerabilidades críticas consisten en un desbordamiento de búfer presente en múltiples servicios utilizados por el protocolo de gestión de puntos de acceso de Aruba (PAPI). Mediante su explotación, un atacante podría ejecutar código de forma remota con permisos de administrador. Por último, la vulnerabilidad de severidad media permitiría a un atacante la divulgación de información confidencial en una red Wi-Fi con una configuración específica. Sin embargo, los escenarios en los que puede producirse la explotación de esta vulnerabilidad son complejos y dependen de factores que escapan al control del atacante.

Enlace: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04454en_us
https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt

Productos afectados.

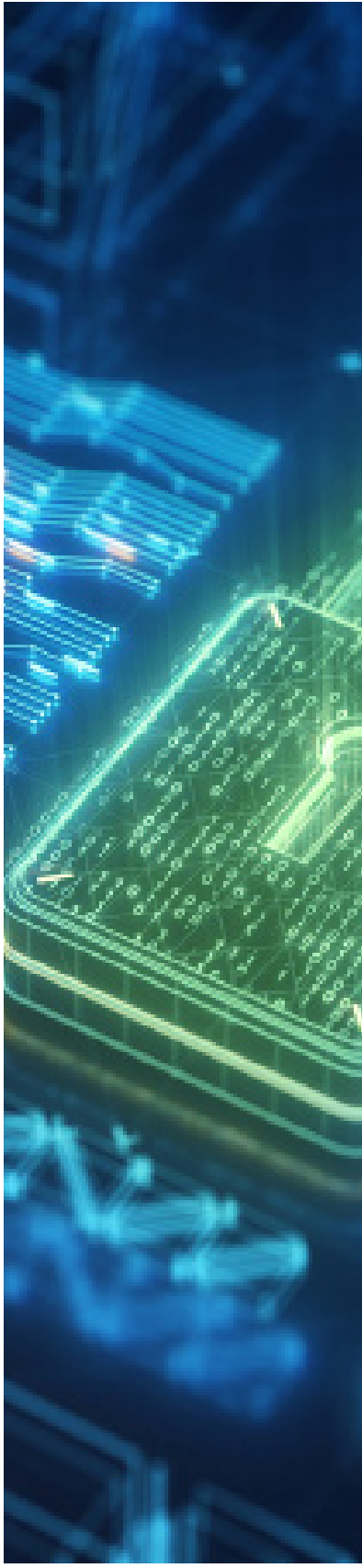
Aruba Access Points con el software InstantOS y ArubaOS 10:

- ArubaOS 10.3.x: versiones 10.3.1.0 y anteriores;
- Aruba InstantOS 8.10.x: versiones 8.10.0.4 y anteriores;
- Aruba InstantOS 8.6.x: versiones 8.6.0.19 y anteriores;
- Aruba InstantOS 6.5.x: versiones 6.5.4.23 y anteriores;
- Aruba InstantOS 6.4.x: versiones 6.4.4.8-4.2.4.20 y anteriores.

Solución: Aruba Network ha emitido actualizaciones de seguridad para los productos afectados, por lo que se recomienda actualizar a la última versión disponible.

© 2023 NTT DATA. Todos los derechos reservados.
Prohibido su uso, copia, reproducción, divulgación, distribución, difusión o modificación, total o parcial, con fines comerciales
sin autorización de su titular.

PARCHES



Microsoft

Fecha: 09-05-2023

Descripción. Microsoft ha publicado una serie de actualizaciones de seguridad correspondientes al mes de mayo de 2023 donde corrige un total de 38 vulnerabilidades conocidas: 6 críticas de ejecución de código remoto, 33 altas, 1 moderada y 9 sin calificación de gravedad. Entre ellas, se encuentran tres zero-day, dos de ellas explotadas activamente:

- CVE-2023-29336: esta vulnerabilidad presente en el Kernel Win32k, permite a un atacante obtener los permisos SYSTEM, el mayor nivel de privilegios dentro de un sistema Windows.
- CVE-2023-24932: mediante esta vulnerabilidad, un atacante con permisos de administrador o acceso físico al equipo podría instalar una política de arranque maliciosa. Este tipo de malware, denominado UEFI bootkits, resulta invisible a las herramientas de seguridad, debido a que se ejecuta en la etapa inicial del arranque del equipo.
- CVE-2023-29325: esta vulnerabilidad permitiría a un atacante ejecutar código de forma remota en el equipo mediante correos electrónicos especialmente diseñados.

Enlace:
https://cve.report/CVE-2023-20078
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP#details

Productos afectados:
Algunos de los productos afectados son: Microsoft Bluetooth Driver;Microsoft Edge (Chromium-based); Microsoft Office Excel; Microsoft Office SharePoint; Microsoft Office Word; Microsoft Teams; Visual Studio Code; Windows Secure Boot;Windows Win32K. La lista complete de productos afectados se puede consultar en el siguiente enlace: https://msrc.microsoft.com/update-guide

Solución: Actualizar los parches de seguridad publicados por el fabricante del dispositivo correspondiente.

SAP

Fecha: 09-05-2023

Descripción. Apple ha publicado un reporte de seguridad en el que se indican múltiples actualizaciones para sus dispositivos iPadOS, iOS y macOS Estos parches solucionan las vulnerabilidades: CVE-2023-23531, con severidad critica, CVE-2023-23530, con severidad alta.

- CVE-2023-23531: esta vulnerabilidad permitiría a un atacante la ejecución de código arbitrario en el equipo mediante la explotación de las expresiones de NSPredicate las cuales podían saltarse la validación realizada por el componente NSPredicateVisitor lo cual permite al atacante saltarse cualquier tipo de validación.
- CVE-2023-23530: En el caso de esta vulnerabilidad un atacante podría mediante la explotación de las listas negras utilizadas por NSPredicate, las cuales impedían la utilización de ciertas clases o métodos que podían poner en entredicho la seguridad del dispositivo. El borrado de estas listas podría permitir a un atacante la ejecución de código arbitrario en el equipo.

Enlace: https://onapsis.com/blog/sap-patch-day-may-2023
https://www.incibe.es/incibe-cert/alerta-temprana/avisos/actualizacion-de-seguridad-de-sap-de-mayo-de-2023

Productos afectados:
Los productos afectados son los siguientes:
SAP 3D Visual Enterprise License Manager, versión 15; SAP BusinessObjects Intelligence Platform, versiones 420 y 430; SAP AS NetWeaver JAVA, versiones SERVERCORE 7.50, J2EE-FRMW 7.50 y CORE-TOOLS 7.50; SAP IBP EXCEL ADD-IN, versiones 2211, 2302 y 2305; SAP PowerDesigner (Proxy), versión 16.7; SAP Commerce, versiones 2105, 2205 y 2211; SAP GUI for Windows, versiones 7.70 y 8,0; SAP Commerce (Backoffice), versiones 2105 y 2205; SAPUI5, versiones SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757 y UI_700 20.

Solución: Se recomienda actualizar los productos a la última versión disponible según indica el fabricante: https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html según indica el fabricante: https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html

© 2023 NTT DATA. Todos los derechos reservados. Prohibido su uso, copia, reproducción, divulgación, distribución, difusión o modificación, total o parcial, con fines comerciales sin autorización de su titular.

EVENTOS

XII Simposium de Seguridad GAP

22 - 29 de mayo de 2023 |

El grupo Aeroportuario (GAP) con apoyo de Segurilatam, y la colaboración de la agencia federal de aviación (AFAC) a organizado el XII Simposium de seguridad GAP en Guadalajara, México. Este aforo tendrá una limitación presencial de 300 plazas, y cuya asistencia es exclusiva por invitación personal. Los asuntos por tratar en este congreso van a ser sistemas AVSEC, protección perimetral, servicios privados de seguridad y ciberamenazas.

Enlace: https://www.segurilatam.com/agenda/xii-simposium-de-seguridad-gap_20230303.html

III Congreso de Seguridad Digital y Ciberinteligencia: C1b3rwall

20 - 22 de junio 2023 |

El III Congreso de Seguridad Digital y Ciberinteligencia (C1b3rwall) comienza el 20 de junio en formato presencial, y durara hasta el 22 de este mismo mes. El evento está organizado por la Universidad de Salamanca y por la Policía Nacional en la Escuela Nacional de Policía de Ávila. Este congreso nació en 2019, y la pasada edición congrego a más de 5000 profesionales relacionados con la tecnología de la información y comunicación, fuerzas y cuerpos de seguridad, fuerzas armadas, docentes universitarios y estudiantes.

Enlace: https://c1b3rwall.policia.es/congreso

‘Cyber Security International Radar’(CSI Radar)

12 - 16 de junio de 2023 |

La compañía Medina Media Events organizara el evento Cyber Security International Radar’(CSI Radar) en Sevilla. Este evento será desde el 12 al 16 de junio, donde se dará visibilidad a todos los proyectos y soluciones a nivel nacional e internacional para mejorar la seguridad en empresas, instituciones e individuos. Esta agenda es hibrida, con dos días presenciales (Palacio de Exposiciones y Congresos de Sevilla) y tres virtuales, agrupando más de 40 ponenticas.

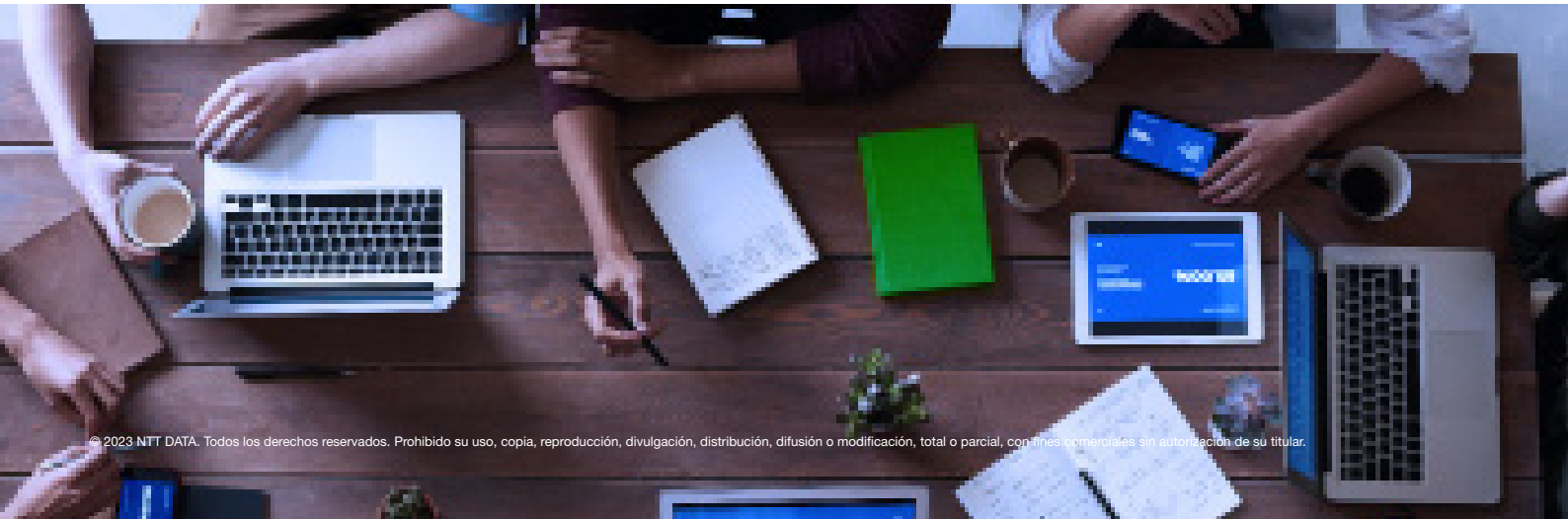
Enlace: https://csiradar.com/

15 Encuentro de la Seguridad Integral (Seg2)

24 - 27 de abril de 2023 |

Este encuentro organizado por las revistas Red Seguridad y Seguritecnia tendrá lugar el 22 de junio. EL evento estará bajo el título “El nuevo paradigma de seguridad: La respuesta a los desafíos geopolíticos”. Este evento será en formato TV experiencia. Algunos de los tópicos que se van a tratar son, la guerra de Ucrania y la guerra digital, peligros del ciberespacio, regulaciones (5G, NIS2…) inspecciones y gestión.

Enlace: https://www.seguritecnia.es/agenda/15-encuentro-de-la-seguridad-integral-seg2_20230104.html



© 2023 NTT DATA. Todos los derechos reservados. Prohibido su uso, copia, reproducción, divulgación, distribución, difusión o modificación, total o parcial, con fines comerciales sin autorización de su titular.

RECURSOS

BGP Boofuzzer

Es una herramienta de código abierto para encontrar vulnerabilidades en la implementación de BGP. Esta herramienta permitirá a las empresas evaluar la seguridad de las suites BGP que utilizan internamente, así como utilizarla para descubrir nuevas vulnerabilidades en las implementaciones de BGP por parte de los investigadores.

Enlace: https://noticiasseguridad.com/tutoriales/bgp-boofuzzer-herramienta-para-encontrar-vulnerabilidades-en-la-implementacion-de-bgp/

Goose Tool

Es una herramienta gratuita que puede ayudar a los defensores de la red a identificar posibles actividades maliciosas en los entornos de Microsoft Azure, Azure Active Directory y Microsoft 365. La herramienta proporciona nuevos métodos de autenticación y recopilación de datos para usar en el proceso de defensa de los mencionados entornos

Enlace: https://noticiasseguridad.com/tutoriales/la-mejor-herramienta-gratuitita-para-la-deteccion-de-incidentes-ciberneticos-en-microsoft-azure-azure-active-directory-y-microsoft-365/

Microsoft anuncia Security Copilot

Es una herramienta de ciberseguridad que utiliza inteligencia artificial para detectar y responder a las amenazas en el mundo digital. Su propósito es simplificar los procesos y potenciar las capacidades de los equipos de seguridad de las organizaciones. La herramienta buscará aprender y mejorar continuamente para adaptarse al cambiante panorama de amenazas, y permitir a los equipos de seguridad estar preparados y actualizados para afrontarlos de manera efectiva

Enlace: https://cybersecuritynews.es/microsoft-anuncia-security-copilot-una-solucion-con-ia-para-dar-respuesta-ciberamenazas/

Cigent Secure SSD+

Se trata una unidad SSD que, gracias a un sistema de IA, cuenta con una sólida e infranqueable protección contra todo tipo de ransomware. Su uso podría significar la protección final de todos los archivos que se almacenen en su interior, lo que lo cambiaría todo para organizaciones, gobiernos y usuarios.

Enlace: https://www.adslzone.net/noticias/seguridad/adios-malware-unidad-ssd-ia-evita-infecciones-ransomware/

© 2023 NTT DATA. Todos los derechos reservados. Prohibido su uso, copia, reproducción, divulgación, distribución, difusión o modificación, total o parcial, con fines comerciales sin autorización de su titular.


NTT DATA
Trusted Global Innovator
powered by the
cybersecurity NTT DATA team
nttdata.com