Número 105 | Agosto 2025

NTT DATA

Radar

El magazine de ciberseguridad

Deepfakes, IA y nuevas amenazas que exigen más conciencia

Por Francisco Javier García Lorente

La revolución tecnológica que vivimos, impulsada por la inteligencia artificial, ha abierto una nueva dimensión en el panorama de la ciberseguridad. Herramientas que hace unos años parecían ciencia ficción, como los generadores de imágenes sintéticas, las voces clonadas o los vídeos manipulados, hoy están al alcance de cualquier persona con conexión a Internet. Este avance, aunque fascinante, ha traído consigo amenazas emergentes que requieren algo más que medidas técnicas para ser combatidas: requieren una concienciación real de las personas.

Uno de los fenómenos más disruptivos es el de los *deepfakes*: contenidos audiovisuales generados por IA que suplantan rostros, voces o expresiones de individuos reales con una precisión alarmante.

En el ámbito de la ciberseguridad, esto se traduce en ataques de ingeniería social mucho más sofisticados, donde la apariencia de legitimidad es casi perfecta. Un simple vídeo aparentemente grabado por un CEO solicitando una transferencia urgente puede tener un impacto devastador si el receptor no está debidamente formado para detectar irregularidades sutiles.

A esto se suma el uso de modelos generativos de lenguaje que pueden crear correos de *phishing* sin faltas, con conocimiento del contexto y personalizados con datos obtenidos en redes sociales.

Ya no hablamos de correos mal redactados con errores evidentes, sino de mensajes que imitan el tono de una conversación previa o la firma de una persona conocida.

Esta “profesionalización” de los ataques exige un salto cualitativo en la formación del usuario, no solo para detectar amenazas evidentes, sino para aprender a dudar y verificar incluso lo aparentemente confiable.

Además, los ciberatacantes están combinando IA con automatización de ataques a gran escala. Por ejemplo, mediante *bots* que prueban millones de combinaciones de contraseñas (fuerza bruta), sistemas que identifican vulnerabilidades en tiempo real o *malware* que se adapta dinámicamente al entorno de la víctima para evitar su detección.

En este contexto, no basta con tener una solución antivirus: se necesita conciencia, criterio y hábitos seguros.

Aquí es donde la formación y la concienciación se convierten en un requisito estratégico. Las organizaciones deben entender que no se trata solo de dar una charla anual sobre buenas prácticas, sino de diseñar *ciberjourneys* continuos, con contenidos adaptados a los diferentes niveles de conocimiento, situaciones realistas y amenazas actuales.

El aprendizaje debe ser evolutivo, práctico y emocional: hay que conectar con el usuario, hacerlo sentir parte del sistema de defensa.

Es vital enseñar a todos, desde perfiles técnicos hasta administrativos, a reconocer señales de alerta: enlaces con URLs alteradas, peticiones urgentes de datos, cambios sutiles en el lenguaje, o incluso vídeos en los que “algo” no encaja.

Al mismo tiempo, hay que actualizar las políticas de uso de dispositivos, redes sociales y herramientas de comunicación, ya que el perímetro tradicional ha desaparecido con la movilidad, el teletrabajo y el BYOD (Bring Your Own Device).

La conclusión es clara: la inteligencia artificial ha elevado el nivel de las amenazas, pero también puede ser una aliada. Se pueden usar algoritmos para detectar patrones de fraude, automatizar respuestas y proteger la infraestructura.

Sin embargo, el eslabón más importante sigue siendo el humano. Una persona consciente, formada y empoderada es una barrera muy difícil de superar, incluso para la IA más avanzada.

Invertir en concienciación no es una opción, es una necesidad. Porque hoy, más que nunca, la seguridad comienza en cada uno de nosotros.

Francisco J. García Lorente
Cybersecurity Project Manager

Verano en llamas: la ciberseguridad bajo presión

Cibercrónica por Diego Turiegano y Juan Jose Rollán

Este verano, el calor no solo aprieta en las calles, sino que también se siente en el ámbito digital. Entre junio y julio de 2025, el ciberespacio ha sido escenario de una ola de ciberataques que han puesto en jaque a industrias clave, organismos públicos y millones de usuarios en todo el mundo. Desde plantas de producción detenidas hasta filtraciones masivas de credenciales, la temporada estival vuelve a demostrar que en ciberseguridad no existen las vacaciones. A continuación, repasamos los ciberincidentes más destacados de estas últimas semanas.

El pasado 8 de julio, Hero España confirmaba un ciberataque dirigido que afectó a su planta de producción en Murcia, obligando a interrumpir temporalmente su actividad industrial. Aunque la compañía no ha detallado el tipo de ataque, fuentes cercanas apuntan a un posible caso de *ransomware*.

La empresa activó su protocolo de contingencia para minimizar el impacto y garantizar el suministro a sus clientes. El incidente pone de relieve la creciente vulnerabilidad del sector alimentario, incluso en entornos con altos estándares tecnológicos y regulatorios.

También en julio, el ayuntamiento de Melilla sufrió un ciberataque de tipo *ransomware* que dejó fuera de servicio el 90% de sus servidores, afectando no solo a sistemas administrativos y judiciales, sino también a sus copias de seguridad.

El incidente, calificado de "crítico" por las autoridades, está siendo investigado por el CNI y el Centro Criptológico Nacional, que sospechan de un actor avanzado y con conocimientos especializados.

A escala internacional, un incidente ocurrido en Noruega generó gran preocupación. Un grupo de atacantes logró acceder al sistema de control remoto de una presa en el lago Risevatnet, simplemente explotando una contraseña débil.

Durante cuatro horas, abrieron una válvula de descarga sin que el equipo de operación lo detectara. Aunque no hubo daños materiales, el incidente evidencia la fragilidad de las infraestructuras críticas frente a errores básicos de seguridad digital.

En el plano financiero, el grupo de ciberdelincuentes Scattered Spider volvió a la escena este verano al atacar a la aseguradora Aflac.

Mediante técnicas de *vishing* (llamadas fraudulentas) y bombardeo de MFA (abuso de la autenticación multifactor), los atacantes lograron acceder a sistemas internos y exfiltrar datos confidenciales de empleados y clientes. Aunque no desplegaron *ransomware*, el daño reputacional ha sido considerable y ha generado inquietud en el sector asegurador, uno de los más golpeados este año.

Pero quizá el episodio más inquietante por su alcance ha sido la revelación, a finales de junio, de un archivo masivo con más de 16.000 millones de credenciales filtradas.

Esta base de datos, recopilada a partir de múltiples brechas anteriores, ha sido difundida en foros clandestinos y contiene combinaciones de emails y contraseñas activas en servicios bancarios, redes sociales y plataformas corporativas.

Expertos de ESET han advertido que el material puede usarse para automatizar ataques de *phishing*, robo de identidad y accesos no autorizados. La recomendación: cambiar contraseñas de inmediato y activar la autenticación multifactor en todas las cuentas sensibles.

En definitiva, la sucesión de incidentes recientes pone de manifiesto que el panorama de la ciberseguridad atraviesa un momento de máxima exigencia.

La combinación de ataques dirigidos, filtraciones masivas y brechas en infraestructuras críticas confirma que la superficie de exposición sigue creciendo, al mismo ritmo que las capacidades de los ciberdelincuentes.

Lejos de ser un periodo de menor actividad, el verano ha demostrado ser un momento especialmente vulnerable, donde la relajación operativa y la falta de previsión pueden tener consecuencias graves.

La ciberseguridad, más que nunca, debe integrarse como un eje transversal y constante en la gestión de cualquier organización.

Diego Turiegano
Cybersecurity Analyst

Juan José Rollán
Cybersecurity Analyst

Llamada a la Concienci-acción

Artículo por Leire Cubo Arce

Trabajar como consultora de ciberseguridad dentro del equipo de Awareness me ha brindado una perspectiva única sobre la ciberseguridad. He tenido el privilegio de trabajar de cerca con diversas organizaciones y sus empleados, y a lo largo de esta experiencia, he podido observar una verdad fundamental: la concienciación efectiva en ciberseguridad no se construye sobre el miedo, sino sobre la comprensión y el empoderamiento.

Intentar asustar a la gente para que sea segura rara vez funciona a largo plazo. En cambio, cuando las personas comprenden por qué la ciberseguridad es relevante para ellas y se sienten capaces de actuar, se convierten en la primera línea de defensa más fuerte que lo que cualquier tecnología pueda ofrecer. Para ello, me guio por **tres claves principales**:

1. De lo personal a lo corporativo
2. Formación realista y no punitiva
3. A través del humor y sin miedo

De lo personal a lo corporativo

A menudo, un empleado no quiere escuchar sobre los **riesgos que enfrenta la empresa**, por muy reales que sean las amenazas y por mucho que estas puedan tener un impacto directo en su trabajo o incluso en su futuro. La realidad es que, por naturaleza, la mayoría de las personas tienden a **priorizar lo personal** antes que lo corporativo.

Por eso, una de las claves para una concienciación efectiva es **construir desde lo personal hacia arriba.** Algo que he aprendido es que, si logramos que una persona sea cibersegura en su casa, es muy probable que también lo sea en el trabajo. Al fin y al cabo, los malos hábitos no se quedan en la puerta de la oficina. Debemos partir de la base de que el empleado primero siempre se preocupará por sí mismo y su entorno más cercano.

Para ello, es crucial **aterrizar los ejemplos a su realidad diaria.** Los humanos, por naturaleza, somos un tanto egoístas; prestamos verdadera atención cuando el tema nos afecta directamente. Cuando comprendemos cómo un *phishing* puede afectar nuestras propias cuentas bancarias o cómo un virus puede dañar nuestro ordenador personal, el mensaje resuena de una manera mucho más profunda.

A partir de esa base de seguridad personal, es mucho más fácil conectar los puntos y mostrar cómo esas mismas prácticas y precauciones son cruciales para la **seguridad de la empresa.**

Formación realista y no punitiva

Otra de las cosas que he observado es que hay una gran brecha entre las organizaciones que se preocupan por la formación en ciberseguridad y las que no. Las más visionarias entienden que la ciberseguridad no es solo una cuestión tecnológica, sino también humana. Reconocen que un **empleado desinformado o no entrenado representa un eslabón débil** y un riesgo significativo. Lamentablemente, otras organizaciones ven la concienciación como una mera obligación, un control que deben cumplir para auditorías o normativas. Esta visión a corto plazo ignora el hecho de que la verdadera seguridad no se logra solo con herramientas, sino con **personas informadas y vigilantes.**

Veo la misma dicotomía reflejada en la percepción de los empleados. A menudo, lo que más temen no es la amenaza real de un ciberataque, sino las **políticas de "gestión de consecuencias"** que muchas empresas implementan. El miedo a la represalia por caer en una simulación de *phishing*, por ejemplo, puede generar ansiedad y una actitud defensiva, en lugar de fomentar un aprendizaje proactivo. Esta mentalidad de castigo desvía la atención del verdadero peligro.

Creo firmemente que debemos cambiar este chip. El verdadero miedo no debería ser el de una simulación fallida, sino la **posibilidad de que ese *phishing* hubiera sido real** y las devastadoras consecuencias que podría haber tenido para la empresa y para el propio empleado. Mediante el uso de ejemplos reales o enseñándoles que lo que escuchan en las noticias no es ficción (suelen decir que la realidad supera a la ficción) y podría afectarles, es como verdaderamente comprenderán la importancia de estar informados.

La formación, de cualquier tipo, nunca debe ser una herramienta de castigo, sino una oportunidad para **el desarrollo personal** y profesional. Los malos actores no dejarán de existir, por lo tanto, cada uno de nosotros debe convertirse en nuestro propio experto en ciberseguridad.

A través del humor y sin miedo

Pensando en todas las charlas de concienciación que he impartido, hay un factor que siempre funciona por encima de los demás. Para que la concienciación realmente cale, se necesita un enfoque mucho más humano y, sí, a menudo un poco travieso; **el humor es una herramienta poderosa** para romper el hielo y mantener la atención. De hecho, mis sesiones formativas son más exitosas cuando, de vez en cuando, les tiendo pequeñas "trampas": por ejemplo, les pido escanear un código QR que lleva a una página web con un mensaje "malicioso" (totalmente inofensivo y bajo mi control, claro está), y luego les guiño un ojo prometiéndoles que "no se lo contaré al jefe".

Este tipo de experiencias prácticas y un poco descaradas no solo consiguen mantener su atención, sino que les hace comprender que la formación no tiene por qué ser un tema pesado, ni tiene por qué ser impartida por “la típica ponente que viene a darnos la chapa”. Si consigues que los oyentes conecten contigo y se lo pasen bien mientras aprenden, la información permanecerá en sus mentes por más tiempo. Incluso puede que se dé el caso de que hablen con otros compañeros de dicha experiencia, llegando a muchas más personas de lo inicialmente planeado. Los adultos no somos más que niños en un cuerpo más maduro, y como niños que somos, nos encanta compartirle a todo el mundo las cosas que nos parecen interesantes.

La alegría, sonreír y tener una **actitud dinámica y positiva** siempre llegarán más lejos que una persona robótica, apesadumbrada y que únicamente da malas noticias. Que se lo digan a la Inteligencia Artificial y a los múltiples programas de concienciación en ciberseguridad que han comenzado a abusar de ella... ¿Cuántas veces has puesto los ojos en blanco cuando tu empresa te asigna el curso anual de “Security Awareness” que viene narrado por un avatar artificial? A los hechos me remito, que hasta yo misma tengo algunos cursos pendientes de realizar.

Inversión en Cultura de la Ciberseguridad: datos que hablan

Por supuesto, el primer paso para todo lo que os he contado hasta ahora, es poner un gigantesco foco en la inversión en programas de concienciación en ciberseguridad. Según un informe de **Statista de 2023**, se espera que el gasto global en servicios de ciberseguridad alcance los 267 mil millones de dólares para 2027, con un componente significativo destinado a la capacitación y concienciación.

Sin embargo, a pesar de estas cifras, muchas organizaciones todavía no priorizan la educación de sus empleados de manera efectiva.

Otro dato relevante, de un estudio de **Verizon (Data Breach Investigations Report 2024)**, señala que el **error humano sigue siendo un factor clave en la mayoría de las brechas de seguridad.** Esto subraya la importancia crítica de la concienciación. Las estadísticas varían, pero consistentemente muestran que las empresas con programas de concienciación robustos experimentan significativamente menos incidentes relacionados con el factor humano en comparación con aquellas que no los tienen.

Y hablando de programas de concienciación robustos, me gustaría hacer un pequeño énfasis en la importancia de elegir un **programa customizado o de creación humana** por encima de las plataformas de *learning* que ofrecen paquetes de formación listos para consumir. Han comenzado a proliferar en muchas compañías y no puedo evitar pensar en que la “fast-food-ificación” del aprendizaje ya está aquí. Si tus empleados no realizan esos cursos de formación que tienen pendientes desde hace meses, quizá es porque la calidad del contenido no invita a que quieran hacerlos.

Llamada a la concienci-acción

Mi llamado es claro: abandonemos la táctica del miedo, la negatividad y las palabras sombrías. En su lugar, abracemos un enfoque de **empoderamiento y educación**. Al fomentar una cultura de aprendizaje continuo, curiosidad y proactividad, podemos transformar a cada empleado en un defensor de la ciberseguridad, capaz de protegerse a sí mismo y a la organización de las amenazas del mundo digital.

¿Qué piensas tú sobre el papel del miedo en la concienciación en ciberseguridad? ¿Cómo crees que podemos empoderar mejor a nuestros empleados para que sean nuestros mejores defensores?

.

Leire Cubo Arce
Cybersecurity Analyst

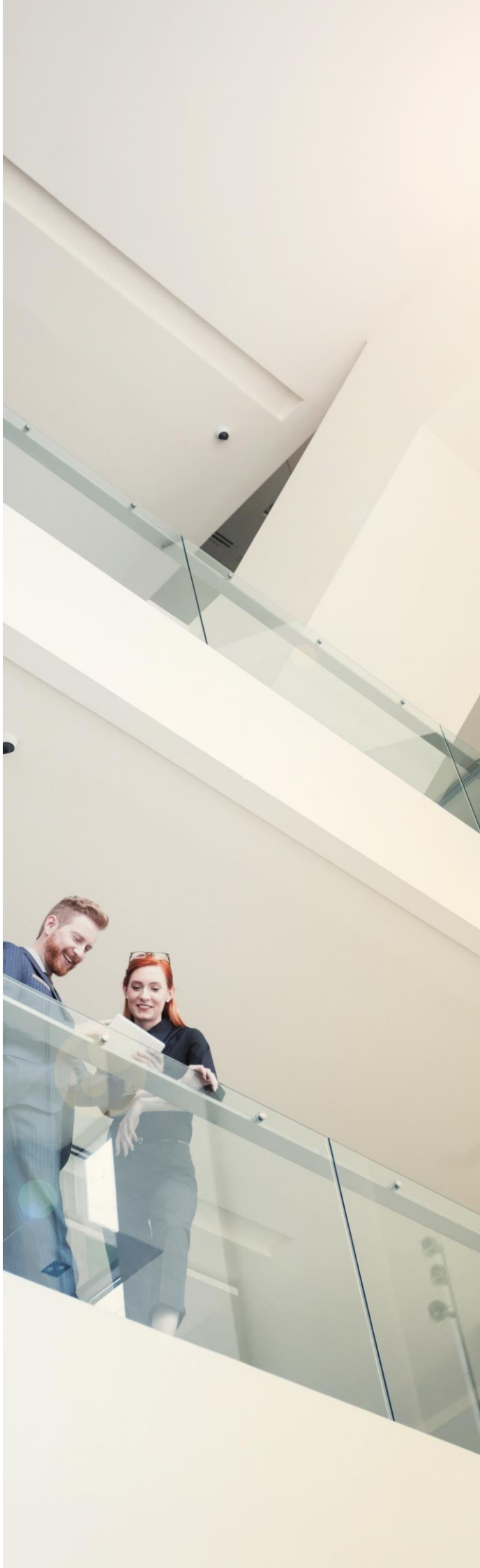
Simulación cuántica

Espacio cuántico
por María Gutiérrez

En los últimos años, la computación cuántica ha dejado de ser un concepto puramente teórico para empezar a aplicarse en sectores económicamente estratégicos. Esto es especialmente eficiente para resolver problemas complejos como la simulación de sistemas físicos, la optimización de procesos, el *machine learning* y la criptografía. Su impacto en diversas industrias es innegable, pero su integración en los negocios aún afronta múltiples obstáculos.

En el caso concreto de su uso en simulaciones, es verdad que siguen existiendo grandes retos, como el ruido y errores cuánticos, la escalabilidad y la hibridación con métodos clásicos, pero no deja de ser una de las aplicaciones más prometedoras. La cuántica permite modelar problemas complejos con una eficiencia inalcanzable para los sistemas clásicos, como ejemplo el estudio realizado por Multiverse Computing, una empresa pionera asociada al sector financiero en colaboración con Crédit Agricole. Juntos han desarrollado un modelo basado en redes tensoriales neuronales inspirado en computación cuántica para optimizar el *pricing* de productos financieros complejos.

¿Cuál es el problema que pretendían resolver? En el mundo de las finanzas calcular el precio justo de un producto financiero (el llamado *pricing*) es una tarea crítica, especialmente para productos derivados o estructurados, cuya valoración depende de múltiples variables y escenarios de mercado. Tradicionalmente, estos cálculos se realizan mediante simulaciones de Monte Carlo, un método estadístico que requiere una enorme capacidad de cómputo y tiempo, especialmente cuando se buscan simulaciones precisas bajo múltiples condiciones de mercado (what-if scenarios). En el caso de Crédit Agricole, el reto era encontrar una forma más rápida y eficiente de realizar estos cálculos sin comprometer la precisión, permitiendo además una mejor personalización del *pricing* para distintos clientes y condiciones de mercado. Es aquí donde entra en juego la simulación cuántica.



Multiverse Computing no utilizó un ordenador cuántico físico, sino que aplicó un enfoque de simulación “quantum inspired”, es decir, modelos matemáticos que imitan algunas de las estructuras y ventajas de la computación cuántica, pero se ejecutan en ordenadores clásicos. En particular, aplicaron una técnica basada en redes tensoriales neuronales cuánticas, un tipo de arquitectura de inteligencia artificial que permite manejar representaciones muy complejas con gran eficiencia.

Las redes tensoriales provienen de la física cuántica, donde se usan para describir sistemas con múltiples partículas entrelazadas. En inteligencia artificial, estas redes se adaptan para manejar grandes volúmenes de datos con interdependencias múltiples como las que existen en los mercados financieros. En este caso, se aplicaron a un modelo de *pricing* de derivados financieros permitiendo reducir el número de simulaciones necesarias, así como mantener una alta precisión en los resultados, acelerar el tiempo de cálculo respecto a los métodos tradicionales y hacer análisis de sensibilidad casi en tiempo real.

El impacto del proyecto fue notable. El banco puede mejorar la eficiencia de su sistema de *pricing* reduciendo el uso de recursos computacionales y aumentando su capacidad para personalizar productos. Además, este enfoque permite una mejor toma de decisiones al poder simular múltiples escenarios en tiempos mucho más breves. Esto tiene un enorme valor estratégico en un entorno financiero donde las condiciones pueden cambiar en cuestión de minutos.

Este caso demuestra cómo la simulación cuántica, sobre sistemas “quantum inspired”, puede transformar sectores complejos como las finanzas hoy mismo, sin esperar a que existan ordenadores cuánticos comerciales plenamente operativos.

E-mails a Valmont 2.0

Artículo por David Contel

La innovación pedagógica ha sido clave en la consolidación del área de Awareness y el desarrollo de acciones suficientemente imaginativas para, por un lado, lograr los objetivos de aprendizaje y, por el otro, lograr un buen *engagement* con colectivos de usuarios acostumbrados a la constante evolución en el consumo de contenidos. A veces (y por sistema), no nos paramos a pensar de un modo crítico qué medios estamos utilizando y por inercia dejamos que las tendencias tecnológicas y nuevas herramientas docentes nos marquen el rumbo. El resultado puede acabar siendo el de enarbolar la bandera de un formato novedoso por defecto, dejando en un segundo plano qué se quiere contar.

En este artículo queremos invitar a reflexionar sobre los estilos y medios de comunicación clásicos, y cómo estos, lejos de ser una herramienta caduca, pueden ser utilizados de un modo efectivo para los objetivos de concienciación.

Partamos de esta pregunta, ¿qué son un hilo de mensajes de correo, de SMS o entradas en un foro de discusión? Simplemente cartas. Y la historia de la literatura lo llama novela epistolar.

Vemos un ejemplo de como un clásico estilo literario puede transformarse en una poderosa pieza de concienciación. Las conclusiones se las dejamos al lector.

Extractos del diario de un CIO de finanzas

Lunes 18 de agosto. 11:15 AM

He visto el Instagram del CEO. Parece que se lo está pasando en grande esquiando en Argentina. Subo de inmediato a mis redes algunas cosas de estos días. Esa foto donde salen las niñas con el cartelito de felicitación a mi madre “Tamara y Cayetana te queremos. Felicidades yaya” es de lo más tierno que he visto. Cuando lo haya posteado a todos mis seguidores, me hago un video para TikTok con el nuevo hit de verano de Karol G.

Viernes 22 de agosto. 18:13 PM

Me he pasado con las caipiriñas y el servicio de canguros del hotel termina a las 19:00 horas. Justo cuando sale del spa mi mujer. Me tomo un refresco y dos ibuprofenos. Las publicaciones en mis redes de ayer han triunfado. Tengo más likes que Leticia Sabater y el waka, waka. Perdón. ¿O era Shakira? Mejor tres ibuprofenos. ¿Y esa notificación? Es verdad. Toca foto para el Be Real.

Lunes 25 de agosto. 15:24 PM

En dos días volvemos a casa. He tenido tentaciones de abrir el correo del trabajo. Por suerte, Tadeo, el barman colombiano tiene el punto perfecto cogido a los mojitos. Nos hemos hecho colegas.

Es super gracioso. Son geniales las anécdotas de su empresa familiar: Exportaciones Escobar. Me alegra mucho que la empresa superara con éxito la muerte de su CEO, en un accidente aéreo. Le he dado mi correo electrónico para que me pase algunas fotos que nos ha hecho.

Lunes 1 de septiembre. 10:32 AM

Después de dos semanas en Copacabana (Brasil) de vacaciones con la familia, vuelvo al trabajo. Necesito ya unas vacaciones de estas últimas vacaciones. Menos mal que en un mes tenemos el congreso corporativo internacional en Tijuana. Mi estado anímico se hunde aún más cuando veo la bandeja de entrada del Outlook. Estoy por pedirle a mi *assistant* que se encargue de filtrar los más importantes. Bueno, me pondré luego, después de las primeras reuniones.

Lunes 1 de septiembre. 12:32 PM

La tercera reunión ha sido con el CISO. Nos ha introducido los cambios en las políticas de seguridad. Ahora tendremos que usar contraseñas de 12 caracteres y no podemos reutilizarlas. Hasta final de año utilizaré “Copacaban@2025”, que no habrá quien la descifre. Pero lo que realmente me fastidia son los cambios de seguridad que implementarán en la red. No sé por qué nos bloquean ChatGPT. Por otro lado, nos ha presentado a la nueva manager de GRC. Me ha parecido super competente. La convocaré tan pronto como sea posible para que me explique exactamente cual el su trabajo.

Miércoles 10 de septiembre. 10:32 AM

Ya he cambiado la contraseña de mi mail corporativo por “Copacaba@2025” después de la reunión con la nueva manager de GRC. Me ha explicado cuáles son sus líneas de trabajo y objetivos para el nuevo ejercicio. Voy a necesitar diversas reuniones más para entenderlo todo. Pero, por lo que me ha parecido entender, tenemos que estar atentos a la implementación de cambios derivados de esa NIS2. Antes de investigarlo con más profundidad tengo que atender algo urgente. Me dicen que el responsable de pagos está sufriendo un ataque de pánico y ha intentado ahorcarse con el cable del microondas.

Miércoles 10 de septiembre. 10:55 AM

¡De esta no sale nadie vivo! Pero será mameluco, pedazo de ectoplasma, zafio y patán. Pero ¿cómo se le ocurre transferir dos millones de euros? Y a otra cuenta. ¿Qué no sabe que hay procedimientos para hacer esos cambios? Y el muy troglodita me dice que se lo he pedido yo desde mi cuenta personal de correo, y que ha hablado con mi abogado. Ahora sí que voy a necesitar un abogado. Pero penalista. Si no se ahoca con el cable del microondas, lo haré yo mismo con mis manos.

Miércoles 10 de septiembre. 13:35 PM

Hoy voy a empezar a creer en otro Ser Superior. Nos han llamado del banco para pedirnos confirmación de la transferencia. Les ha resultado extraño que quisiéramos pagar una cantidad tan elevada a una nueva cuenta, y de un banco chino. Hemos podido anular la transferencia. Que suerte hemos tenido. Ha faltado poco para no sobrevivir a la hecatombe. Voy a cerrar un par de temas, tomarme el quinto Diazepan, e ir al hospital a visitar al responsable de pagos. Cuando se lo ha llevado la ambulancia se hablaba de un posible ictus.

Miércoles 11 de septiembre. 8:57 AM

Ya hemos realizado todas las acciones después del incidente de seguridad. El CISO y su equipo han analizado las fases del ataque y realizado el informe. Además, prepararán una formación específica para usuarios críticos para mejorar la cultura de ciberseguridad. Si lo llego a saber antes, lo patrocino yo mismo. En cualquier caso, todos estamos más tranquilos. Me ha alegrado tener noticias de Tadeo, el barman colombiano. Me ha escrito un correo super agradable. Ese chico es un encanto. Pero estaba seguro de que le había dado mi cuenta personal de correo y no la corporativa. En cualquier caso, me ha contado las últimas novedades del resort y me ha pasado unas fotos. Acabo de ver el enlace a su drive personal. Le doy clic y me descargo las fotos de inmediato. Seguro que hoy serán un gran día.

Extractos del diario de un ciberdelincuente

Martes 19 de agosto. 14:25 PM

Continúo con el seguimiento en redes del CIO de finanzas de la empresa objetivo. Como cualquier persona con vocación a la grandeza, solo hoy ha publicado 5 post en Instagram, 2 vídeos en TikTok, y 9 entradas en Facebook. Será "boomer" el tío. Las fotos que ha publicado con sus hijas Tamara y Cayetana, confirman que sigue pagando en vano la cuota del gimnasio. Es lo que tiene preferir una inversión en Cruzcampo que en el Metropolitan.

Sábado 23 de agosto. 11:25 AM

El objetivo sigue publicando información. Ese último *selfie* para Be Real que se ha hecho con el barman, no aporta apenas datos, aparte que, en unos años necesitará un trasplante de hígado. Hoy ya es tarde, pero mañana averiguaré cuál es su aseguradora médica y les vendo ese dato.

Lunes 28 de agosto. 21:25 PM

He ganado acceso a la cuenta de correo personal del objetivo. Estoy contento. No ha sido necesario utilizar un diccionario de palabras para descubrir la contraseña. Al tercer intento, el servidor de correo ha aceptado el *password.* TamarayCayetana2025. Revisaré si se ha enviado información corporativa más tarde. Por la madre Rusia. ¿Quién es ese Tadeo Escobar que le envía fotos de Sofía Vergara?

Lunes 1 de septiembre. 12:01 PM

Confirmado. El objetivo tenía información corporativa en su correo personal. Es especialmente interesante la referente a los próximos pagos de equipos informáticos. Tengo datos exactos de los interlocutores, los asuntos que tratan habitualmente, e incluso de los chascarrillos que tienen entre ellos. Tengo que investigar quien es ese Albert Rivera y su perro Lucas. Con todos estos datos podré montar un ataque mediante el *Business email compromiso (BEC)*.

Martes 9 de septiembre. 10.48 AM

He diseñado ya la estrategia de ataque del BEC. Lanzaré el mail al responsable de pagos desde el mail personal del CIO. Para hacerlo más creíble entrará en el hilo su abogado personal. Si todo va según lo planeado me saco unas buenas comisiones. Le he pasado el informe a mi superior y le ha gustado tanto que me ha regalado una botella de vodka. Me ha dicho que si lo consigo me da un ascenso.

Miércoles 10 de septiembre. 10:48 PM

El ataque ha sido todo un éxito. El responsable de ventas ha actuado según lo esperado. Después de pedir el cambio de cuenta urgente y la transferencia inmediata, y una amenaza sutil, a través de la cuenta personal del CIO, lo ha ejecutado en seguida. En unas horas tendríamos que recibir la confirmación del ingreso en nuestra cuenta. Cambiaré la contraseña de la cuenta de correo para bloquearla. Mi jefe estaba tan contento, que parecía Boris Yeltsin en un *afterwork* con Bill Clinton.

Miércoles 10 de septiembre. 11:16 PM

Mientras todavía estamos esperando la confirmación del ingreso, estoy matando el tiempo eligiendo dónde me voy a gastar el bonus. Aunque Benidorm siempre es una garantía de turismo de calidad, quizá visito a unos amigos en Hackerville. Rumanía en verano es preciosa.

Miércoles 10 de septiembre. 15:23 PM

Los controles del banco se han activado y el objetivo ha logrado anular la orden de transferencia. Era una posibilidad, pero me siento muy frustrado. Ya había estado fantaseando con la compra de un apartamento en Marina d'Or. Pero el verdadero problema lo tengo con mi superior. Está convencido que ha sido error mío por no haber pensado mejor las posibles contingencias. Me ha llamado traidor. Ha comparado esta afrenta con la marcha a Moscú de Yevgeny Prigozhin, y amenazado con desterrarme a un *gulag* si no lograba resultados. Cuando se ha calmado, le he explicado otro plan que he diseñado y me ha dado otra oportunidad. Pero me ha dejado claro que, si vuelvo a fallar, lo considerará una traición aun mayor al nivel de la perpetrada por Joan Garcia. Procedo a lanzar el ataque sin más demora. El barman Tadeo Escobar y sus fotos será mi caballo de troya. He preparado ya en enlace directo al ejecutable del *ransomware*, simulando ser un drive personal de almacenamiento de fotos. Esta vez todo irá según lo planeado

David Contel
Cybersecurity Senior Consultant

Enfoque de las actividades de concienciación sobre ciberseguridad en las organizaciones

Tendencias por Gerard Marín Raventos

La ciberseguridad no es, para la mayoría de empresas y organizaciones, la finalidad en sí de su actividad e incluso, su existencia. No obstante, a estas alturas ya no hay ninguna duda de que la ciberseguridad se ha convertido en un aspecto crítico para cualquier organización. Como no es la finalidad, pero si necesaria y crítica, se hace imprescindible que tanto la empresa como las personas que la integren tengan interiorizada una cultura de ciberseguridad.

Esto implica que las actividades de concienciación sobre ciberseguridad deben ser diseñadas de manera estratégica, considerando que estas organizaciones deben priorizar su enfoque en sus operaciones centrales mientras integran la seguridad como un valor añadido.

Para empezar, es esencial que la concienciación sobre ciberseguridad se aborde de forma pragmática.

En lugar de saturar a los empleados con información técnica compleja, las actividades deben ser accesibles y relevantes para sus funciones diarias. Por ejemplo, se pueden realizar talleres breves que se enfoquen en cómo aplicar prácticas seguras en sus tareas cotidianas, como el manejo de información sensible o el uso de contraseñas robustas.

Además, las actividades de concienciación deben ser interactivas y atractivas. Utilizar metodologías como la *gamificación*, donde los empleados participan en juegos o simulaciones relacionados con la ciberseguridad, puede ser muy efectivo.

Por ejemplo, una empresa puede organizar un "escape room" virtual, donde los equipos deben resolver acertijos de ciberseguridad para "escapar" de un entorno simulado. Este tipo de actividad no solo es entretenida, sino que también promueve el trabajo en equipo y refuerza el aprendizaje práctico.

También es fundamental que la alta dirección participe y respalde estas iniciativas. Cuando los líderes de la organización muestran su compromiso con la ciberseguridad, los empleados son más propensos a tomar en serio las actividades de concienciación.

El dicho “los jóvenes cierran las orejas a los consejos y abren los ojos a los ejemplos” también se puede aplicar a los adultos. Las comunicaciones regulares sobre la importancia de la ciberseguridad, acompañadas de ejemplos concretos, incluso de la propia organización, pueden aumentar la percepción de riesgo y la necesidad de actuar.

La concienciación debe ser continua y no un evento único. Implementar un programa de formación recurrente, en el que se aborden diferentes aspectos de la ciberseguridad a lo largo del año, ayudará a mantener a los empleados informados y preparados ante nuevas amenazas.

Finalmente, la medición de la efectividad de estas actividades es crucial. Realizar encuestas o evaluar el desempeño de los empleados en simulaciones de seguridad permitirá ajustar los programas según sea necesario y demostrar el impacto de las iniciativas de concienciación en el entorno laboral.

En conclusión, aunque la ciberseguridad no sea el *core business* de una organización, es esencial que las actividades de concienciación se integren de manera efectiva en la cultura corporativa. Al adoptar un enfoque práctico, interactivo y continuo, las organizaciones pueden fortalecer la seguridad sin desviar su atención de sus objetivos principales.

Gerard Marín Raventos
Cybersecurity Consultant

Vulnerabilidades

Vulnerabilidad crítica encontrada en Sudo

Fecha: 30 de junio de 2025
CVE: CVE-2025-32463

CVSS: 9.3

CRÍTICA

Descripción

Esta vulnerabilidad, con identificador CVE-2025-32463, hace referencia a la detección de un fallo de diseño que permite que un atacante pueda invocar Sudo con la opción -R o *–chroot*, aprovechando la resolución de rutas antes de la evaluación correcta de los permisos, permitiendo cargar un archivo /etc/nsswitch.conf malicioso que apunte a su vez a bibliotecas compartidas aleatorias que conduzcan a la ejecución de código malicioso como *root*.

Esta falla permite una escalada de privilegios en el sistema y la ejecución de código como *root,* incluso con cuentas de usuario que no se encuentren en el archivo *sudoers*.

Solución

No existen parches oficiales que corrijan esta falla, pero solo algunas versiones de Sudo se encuentran afectadas, por lo que se recomienda utilizar las siguientes versiones:

- Sudo 1.9.17p1 o superior

Además, se recomienda deshabilitar reglas *sudo* que permitan el uso de las opciones –R o *–chroot* en entornos donde no sean necesarios, o temporalmente hasta la aplicación de la actualización, así como la limitación de permisos de ejecución de archivos desde rutas como */tmp* o */var/tmp*.

Productos afectados

Esta vulnerabilidad crítica afecta a varios productos sudo, entre los que destacan los siguientes:

- Sudo (1.9.14 a 1.9.17)
- Sudo (1.8.8 a 1.8.32)

Referencias

- nvd.nist.gov
- www.incibe.es
- access.redhat.com
- thehackernews.com
- thehackernews.com

Vulnerabilidades

Vulnerabilidad de severidad crítica en Chrome

Fecha: 2 de julio de 2025
CVEs: CVE-2025-34090

CVSS: 9.3

CRÍTICA

Descripción

La vulnerabilidad CVE-2025-34090 afecta a Google Chrome e involucra una debilidad en el cifrado de *cookies* mediante AppBound.

Un atacante local puede llevar a cabo un *COM hijacking* (secuestro de componentes de Windows) para forzar que Chrome use DPAPI del usuario en lugar de AppBound, lo que supone un método menos seguro de cifrado.

Una vez que el atacante logra degradar el cifrado, puede realizar un ataque de tipo Padding Oracle, aprovechando los mensajes de error del sistema al descifrar datos. Esto le permite descifrar *cookies* cifradas byte por byte, sin privilegios elevados, y obtener acceso a sesiones web activas.

Solución

Actualmente, la vulnerabilidad CVE-2025-34090 en Google Chrome no cuenta con un parche oficial disponible.

Por ello, es fundamental tomar precauciones para minimizar riesgos, como limitar el acceso a las claves CLSID en el registro de Windows para evitar ataques de COM *hijacking*.

Productos afectados

Esta vulnerabilidad crítica afecta a:

- Google Chrome versiones anteriores a la 129.
- Otros navegadores basados en Chromium que usen mecanismos similares de cifrado de cookies.

Referencias

- cyberark.com
- nvd.nist.gov

Citrix parchea una vulnerabilidad crítica que afecta a NetScaler ADC y NetScaler Gateway

Fecha: 25 de junio de 2025
CVE: CVE-2025-5777

Crítica

Descripción

La vulnerabilidad CitrixBleed 2 (CVE-2025-5777) afecta a los dispositivos Citrix NetScaler ADC y Gateway, permitiendo a los atacantes recuperar contenidos de la memoria enviando solicitudes POST malformadas durante los inicios de sesión. CitrixBleed 2 puede ser explotada contra utilidades de configuración usadas por los administradores y para robar *tokens* de sesión.

Según los investigadores, cada solicitud filtra 127 bytes, lo que permite a los atacantes realizar solicitudes HTTP repetidas para extraer contenido de memoria adicional hasta encontrar los datos que buscan.

Citrix ha afirmado que la vulnerabilidad no ha sido explotada, aunque existen informes que demuestran lo contrario.

Solución

Citrix recomienda en su boletín de seguridad a sus clientes instalar a la mayor brevedad posible las nuevas versiones corregidas de sus productos NetScaler ADC y NetScaler Gateway.

Además, Citrix recomienda finalizar todas las sesiones activas de ICA y PCoIP, así como revisar las sesiones existentes para detectar cualquier actividad sospechosa.

Productos afectados

- NetScaler ADC y NetScaler Gateway 13,1 (versiones previas a 13.1-58.32), 14.1 (versiones previas a 14.1-43.56)
- NetScaler ADC 12.1-FIPS (versiones previas a 12.1-55.328-FIPS), 13.1-FIPS y NDcPP (versiones previas a 13.1-37.235)

Referencias

- netscaler.com
- bleepingcomputer.com
- horizon3.ai

Parches de seguridad de Microsoft de julio para corregir 130 vulnerabilidades

Fecha: 9 de julio de 2025
CVE: CVE-2025-47981 y 129 más

Crítica

Descripción

Microsoft publica su parche mensual de julio 2025 corrigiendo un total de 130 vulnerabilidades, de las cuales 10 son consideradas de severidad crítica. Las vulnerabilidades más relevantes identificadas son las siguientes:

- CVE-2025-47981 (CVSS 9.8): esta vulnerabilidad crítica en SPNEGO / NEGOEX, permitiría la ejecución remota de código (RCE) sin interacción del usuario, afectando a versiones de Windows que tienen una determinada *GPO* habilitada por defecto.
- CVE-2025-49719 (CVSS 7.5): se trata de una vulnerabilidad en SQL Server que permite acceder a información sensible sin autenticación previa. Fue divulgada públicamente antes del parche, y cuenta con una prueba de concepto pública (PoC) disponible.

También destaca la siguiente vulnerabilidad:

- CVE-2025-49735 (CVSS 8.8): es una vulnerabilidad en Kerberos (servicio de política de clave - KPSSVC) que permitiría a un atacante ejecutar código remoto en el sistema afectado.

Según Microsoft, estas vulnerabilidades no han sido explotadas activamente.

Productos afectados

Estas vulnerabilidades impactan en una amplia gama de productos de Microsoft. Para ver todos los productos afectados, consulta el siguiente enlace:

- msrc.microsoft.com

Solución

Microsoft recomienda aplicar el parche de seguridad publicado para corregir las vulnerabilidades detectadas.

Referencias

- msrc.microsoft.com
- thehackernews.com

Eventos

DEF CON 33
7 - 10 agosto

Se celebrará del 7 al 10 de agosto de 2025 en Las Vegas Convention Center – West Hall (EEUU), y promete ser una experiencia intensa, diversa y profundamente técnica. Este evento no es solo para hackers: también es ideal para investigadores, defensores, desarrolladores, analistas y curiosos del mundo digital. El tema de este año: "Access Everywhere" aborda cómo hacer que la información y los servicios sean accesibles para todos, sin importar el dispositivo, ubicación o capacidades.
El evento consta de:

- *Villages* temáticos: espacios dedicados a áreas específicas como *IoT*, *biohacking*, redes, *hardware*, inteligencia artificial, y más.
- Charlas y *keynotes*: presentaciones de expertos globales sobre vulnerabilidades, técnicas de ataque, defensa y análisis forense.
- Competiciones CTF (Capture The Flag): retos técnicos para equipos de todo el mundo, desde principiantes hasta profesionales.
- Demo *Labs*: donde los creadores muestran herramientas de *hacking*, defensa y análisis en vivo.
- Workshops: talleres prácticos de 4 horas sobre temas como *reversing, pentesting*, OSINT, y más.
- Eventos sociales y *meet-ups*: Desde karaoke hacker hasta grupos de radioaficionados, pasando por fiestas temáticas y *networking* informal.

Enlace

International Conference on computer Science, Programming and Security ICCSPS
14 - 15 de agosto

El objetivo es reunir académicos, investigadores y profesionales del sector para compartir experiencias y avances en áreas como la informática, programación segura, protección de datos y ciberseguridad. El encuentro se celebrará en Barcelona (España) los días 14 y 15 de agosto.

Enlace

BSides Bournemouth
16 de agosto

Cada BSides es un marco impulsado por la comunidad para crear eventos para y por los miembros de la comunidad de seguridad de la información. Crea oportunidades para que las personas presenten y participen en un ambiente íntimo que fomenta la colaboración. Es un evento intenso con discusiones, demostraciones e interacción de los participantes.

Enlace

Conferencia GRC 2025
18 - 20 de agosto

ISACA y The IIA reunirán en Nueva York (EEUU) a las mentes líderes en gobernanza, gestión de riesgos y control (GRC) para proporcionar a profesionales dedicados contenido de clase mundial, ideas innovadoras y orientación práctica.

Los asistentes obtendrán información crítica y conocimientos prácticos en una variedad de temas diseñados para enfrentar los desafíos y oportunidades actuales.

Las sesiones de este año están seleccionadas para empoderar a los profesionales con herramientas prácticas, estrategias innovadoras e ideas con visión de futuro para sobresalir en sus roles y avanzar en sus organizaciones.

Enlace

Recursos

➢ Vastav AI: detección de *deepfakes* y desinformación

Vastav AI interviene con una solución poderosa: usar aprendizaje automático forense y análisis de metadatos. Analiza el contenido visual y de audio en busca de manipulación. Sus intuitivos mapas de calor y puntuaciones de confianza facilitan a investigadores, periodistas y analistas la rápida detección de manipulaciones.

Enlace

➢ Vectra AI: inteligencia de señales de ataque en la red y la nube

Vectra proporciona monitorización continua mediante IA para detectar comportamientos ocultos de atacantes, como movimientos laterales, abuso de privilegios y actividades de comando y control, antes de que se produzcan daños. Su verdadero poder reside en reducir la fatiga de alertas al priorizar las amenazas reales de alto riesgo.

Enlace

➢ PentestGPT: asistente de *pentesting* impulsado por IA

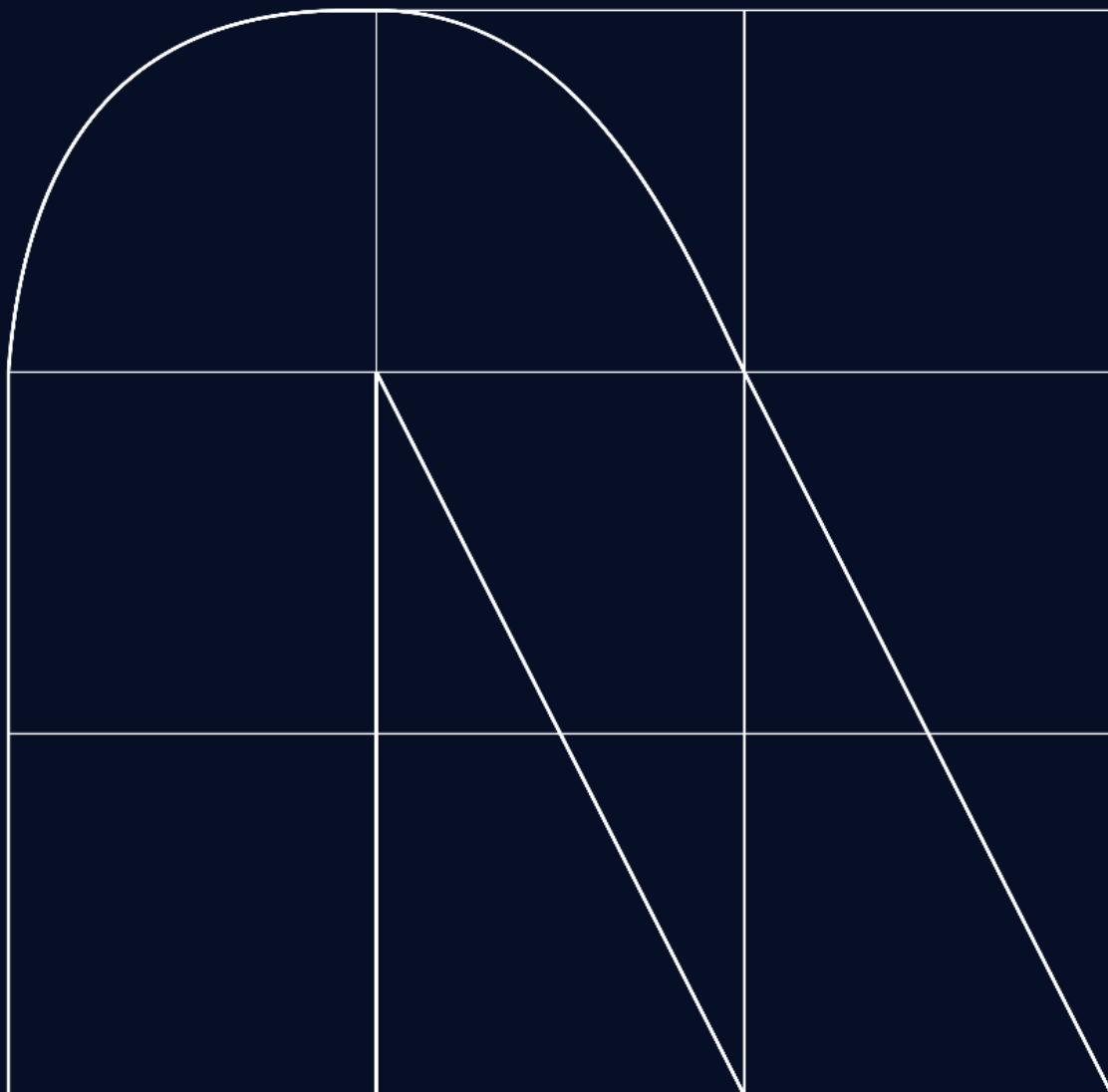
PentestGPT es un asistente de pruebas de penetración basado en IA y basado en modelos GPT que ayuda a los *hackers* éticos a optimizar su flujo de trabajo. En lugar de dedicar horas al reconocimiento manual o a la redacción de informes.

Los usuarios pueden delegar estas tareas a PentestGPT, que ofrece exploraciones guiadas, genera informes de vulnerabilidad estructurados, e incluso crea *scripts* personalizados adaptados a su compromiso.

Perfecto para *pentesters* solitarios, cazadores de errores y equipos rojos que quieren acelerar tareas comunes y repetitivas sin comprometer la calidad ni la minuciosidad.

Enlace

Suscríbete a RADAR
up.nttdata.com/suscribetearadar



Powered by the cybersecurity NTT DATA team

es.nttdata.com