Número 103 | Junio 2025

NTT DATA

Radar

El magazine de ciberseguridad

Footprinting: Lo que saben de ti antes de que te des cuenta

Por Alexis Martín García

Antes de que se produzca una intrusión, antes incluso de que una organización perciba que está siendo observada, ya se ha desencadenado un proceso meticuloso de recopilación de información. Este proceso, en apariencia pasivo y sin rastro técnico aparente, es la antesala de muchas de las campañas más exitosas de ataque dirigidas. Se trata del *footprinting*, una disciplina en sí misma, que explota todo aquello que una organización o sus empleados han expuesto voluntariamente, o a veces por desconocimiento, se ha expuesto involuntariamente al exterior, sin comprender del todo su valor operativo desde el punto de vista del adversario.

El atacante no necesita acceso privilegiado para comenzar. Le basta con inteligencia estructurada: nombres, correos corporativos, ubicaciones físicas, arquitectura de red, proveedores externos, tecnologías utilizadas, nombres de proyectos o incluso los patrones de comportamiento del personal clave. Toda esta información se encuentra dispersa en fuentes abiertas, ya sea páginas web, foros técnicos, redes sociales, documentos públicos y puede ser recolectada sin infringir una sola norma legal. Es la base silenciosa sobre la que se construyen campañas de suplantación, intrusión, manipulación o extorsión.

Aquí es donde el *footprinting* deja de ser un concepto técnico y se convierte en una preocupación estratégica. A medida que crece la dependencia de la digitalización en todos los niveles de una organización, también aumenta la superficie de exposición. Y, por tanto, crece el apetito de los actores de amenazas por esa exposición no gestionada.

Uno de los catalizadores más evidentes de este riesgo es la ingeniería social. Cuando un atacante dispone de información creíble, contextualizada y alineada con los procesos reales de la organización, sus probabilidades de éxito aumentan exponencialmente. Un correo de *phishing* genérico puede ser ignorado; pero si ese correo hace referencia a una reunión real, menciona a un compañero legítimo o replica un proceso interno, la posibilidad de que el destinatario interactúe con él deja de ser remota.

Esto no es una cuestión de errores humanos, sino de una ventaja estratégica construida a partir de inteligencia previa. Y es aquí donde entra en juego la disciplina de la Cyber Threat Intelligence (CTI). Lejos de ser una práctica reactiva, centrada únicamente en indicadores técnicos, la inteligencia de amenazas bien estructurada tiene el potencial de identificar patrones de observación externa, inferir intenciones y anticipar posibles escenarios de explotación antes de que el atacante pase a la acción.

El *footprinting*, desde la perspectiva del defensor, debe ser entendido como una herramienta doble: no solo para identificar lo que otros podrían explotar, sino también para establecer prioridades de protección basadas en lo que realmente es visible, accesible y valioso desde fuera.

En NTT DATA nuestros equipos de CTI tienen la capacidad de mapear la huella digital de una organización desde el punto de vista del adversario. Esta práctica a menudo subestimada, permite descubrir dominios abandonados que aún apuntan a servicios internos, documentos indexados por buscadores que revelan relaciones comerciales, perfiles personales que desvelan roles sensibles, o estructuras de red inferidas a través de información técnica inadvertidamente expuesta en foros especializados.

Y lo más preocupante, toda esta información es suficiente para que actores maliciosos desarrollen ataques altamente dirigidos sin necesidad de herramientas técnicas avanzadas. El ataque comienza en la mente del adversario cuando encuentra la narrativa que le permite encajar todas las piezas.

Por eso, hablar de *footprinting* e ingeniería social no debería reservarse únicamente a los equipos de Red Team o a simulacros internos. Debería formar parte de una conversación más amplia sobre resiliencia organizacional, gestión del riesgo informacional y modelado de amenazas basadas en inteligencia contextual.

El desafío no es evitar ser observado, algo prácticamente imposible en un mundo interconectado, sino controlar lo que se ve y entender el valor que esa exposición tiene para quien busca hacernos daño. Lo que está en juego no es solo la privacidad corporativa, sino la capacidad de resistir ataques que comienzan mucho antes de que se detecten en un SIEM.

Alexis Martin García
Cyber Threat Intelligence & Hacking Project Manager

OpenEoX y la gestión del *software* End of Life

Cibercrónica por Cayetano Valero y Ana Leticia Urbistondo

La gestión eficiente del ciclo de vida del *software* es una actividad fundamental para proteger a las organizaciones. Uno de los desafíos más significativos dentro de este ámbito es la gestión del *software* "End of Life" (EoL). Cuando un producto alcanza su fin de vida, deja de recibir actualizaciones y correcciones de vulnerabilidades. Al no contar con soporte continuado por parte del fabricante, el *software* EoL constituye un riesgo latente para las organizaciones (a nivel operativo y regulatorio), que aumenta la exposición a posibles amenazas tanto conocidas como futuras. En esta cibercrónica vamos a desarrollar las capacidades de este *framework* y explicar cómo trabaja con el *software* EoL.

Para ilustrar el impacto del *software* EoL, Qualys publicó un estudio en el que mostró que más del 50% de las instalaciones de la librería Log4j vulnerables a Log4Shell estaban fuera de soporte cuando se publicó la vulnerabilidad, y el 98% de los sistemas Windows 7 afectados por WannaCry ejecutaban versiones EoL de Windows.

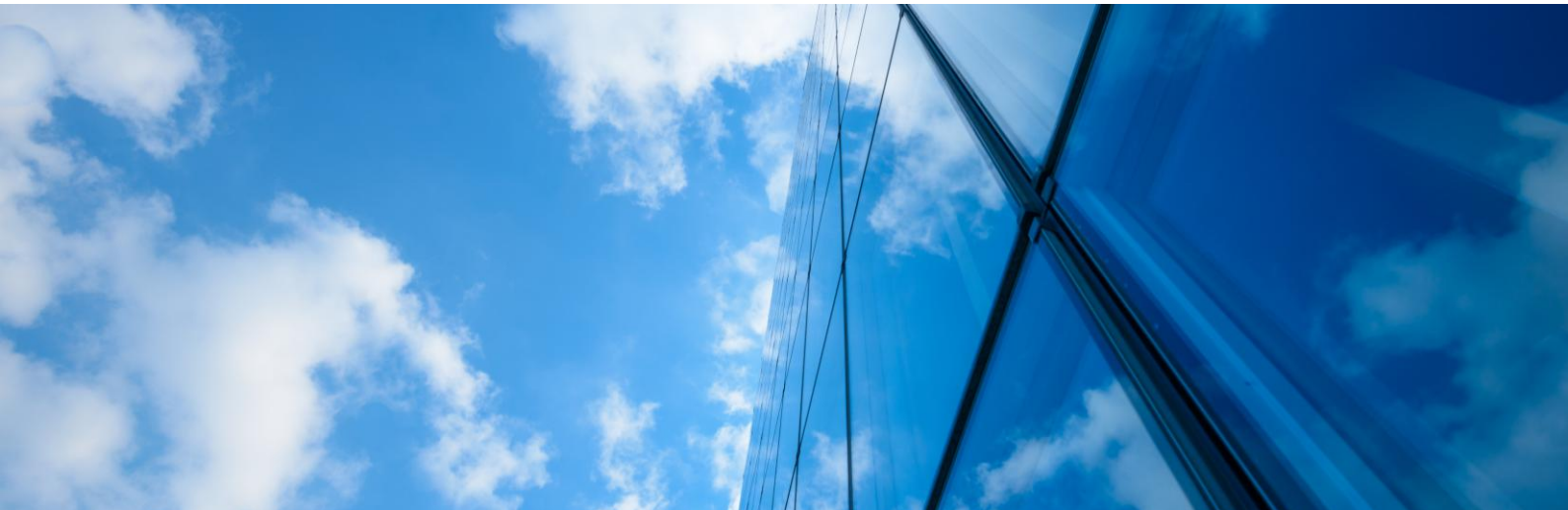
Debido al impacto que el *software* EoL puede tener en las organizaciones, identificarlo de forma temprana y eficaz se convierte en una clave del proceso de migración a una versión alternativa soportada antes de que se alcance el End of Life.

Recientemente, con el fin de mejorar la proactividad en la gestión del *software* EoL, ha surgido la iniciativa OpenEoX (Open End-of-Life Exchange), cuyo objetivo es establecer un *framework* para unificar la forma en que se comparte información sobre este tipo de *software* para identificarlo rápida y correctamente, permitiendo una actuación más eficaz frente a posibles amenazas que aprovechen las vulnerabilidades del *software* obsoleto. Bajo el soporte de empresas como Cisco, IBM o Microsoft, se ha desarrollado este marco de trabajo con el objetivo de proporcionar a los equipos de tecnología una fuente centralizada y fiable de información relacionada con el *software* no soportado, cubriendo puntos clave como: vulnerabilidades conocidas, soluciones de mitigación y mejores prácticas.

El *framework* OpenEoX ofrece claridad y consistencia en la gestión del ciclo de vida del *software* en tres aspectos principales:

- Transparencia: hacer que la información del ciclo de vida sea fácilmente accesible y comprensible.
- Eficiencia: agilizar el proceso tanto para los proveedores de información (proveedores, mantenedores) como para los consumidores (usuarios, organizaciones).
- Unificación: establecer un lenguaje común y una estructura de datos para las etapas del ciclo de vida como EoL, EoSSec y la información de EoS.

Dado que OpenEoX se basa en un esquema ligero y, además, modular, está diseñado para ser flexible y adaptable a distintos entornos, sin necesidad de realizar grandes cambios en los sistemas existentes. Adicionalmente, gracias a su especificación *machine-readable*, es posible integrar fácilmente OpenEoX a otros estándares como CSAF/VEX (Common Security Advisory Format/Vulnerability Exploitability eXchange) o SBOMs (Sofwate Bill of Materials). Esto permite que tanto fabricantes como responsables en el mantenimiento de *software* puedan comunicar de forma coherente y automatizada los hitos en el ciclo de vida de sus productos.



Este marco de trabajo proporciona tres beneficios clave:

1. Visibilidad temprana de los productos de *software* que pronto dejarán de recibir parches de seguridad.
2. Automatización de ciclo de vida a través de alertas programadas y acciones coordinadas.
3. Colaboración multisectorial mediante la compartición de una única fuente de datos sobre estados de soporte, compartida entre fabricantes y usuarios.

Para poder proporcionar estos beneficios a las organizaciones, tal como se ha mencionado anteriormente, el componente principal de este marco de trabajo se centra en la estandarización de los hitos en el ciclo de vida del software, proponiendo diferentes categorías especificadas que ayuden a definir el ciclo de vida de un producto de *software*:

- General Availability (GA) – Disponibilidad general: fecha en la que el producto se lanzó oficialmente al mercado.
- End of Sales (EoS) – Fin de ventas: último día en el que el producto se encuentra disponible para compra.
- End of Security Support (EoSSec) – Fin de Soporte de Seguridad: fecha en la que se deja de proporcionar actualizaciones y parches de seguridad para el producto.
- End of Life (EoL) – Fin de vida : última fecha en la que el producto deja de recibir cualquier tipo de soporte por parte del proveedor.

Con OpenEoX, no solo es posible llevar un mejor control del estado de los productos de *software* obsoletos en las organizaciones, sino que además ayuda a reducir el riesgo asociado a estos productos, anticipando la necesidad de migraciones de estos productos y mejorando las iniciativas de gestión de vulnerabilidades en las organizaciones al incorporar automatizaciones basadas en el ciclo de vida del *software*. Especialmente al considerar que una considerable cantidad de amenazas comienzan con la explotación de vulnerabilidades públicas asociadas a productos de software que se encuentran obsoletos.

Dado que la seguridad de los sistemas depende de una gestión eficaz de la deuda técnica, un marco de trabajo que permita implementar una gestión proactiva y homogénea de los riesgos tecnológicos asociados resulta fundamental, mejorando de forma significativa la planificación del mantenimiento del *software* y la transición hacia nuevas tecnologías.

Cayetano Valero
Cybersecurity Lead Analyst

Ana Leticia Urbistondo
Cybersecurity Analyst

Surface Test: Radiografía Digital de la Exposición Corporativa

Artículo por Carlos Edalfo

En la era hiperconectada en la que vivimos, las organizaciones están más expuestas que nunca. Cada activo digital, cada empleado con presencia en redes sociales y cada línea de código publicada en Internet contribuyen a ampliar la superficie de ataque externa de una empresa. Esta realidad exige que los departamentos de Vigilancia Digital realicen un ejercicio sistemático y continuo de lo que se conoce como *surface test*, o prueba de superficie, una radiografía profunda de la huella digital corporativa.

Ingeniería social y digital *footprint*: el punto de partida

No se puede hablar de pruebas de superficie sin entender que el principal objetivo de los ciberdelincuentes es encontrar vulnerabilidades accesibles desde el exterior. La ingeniería social sigue siendo una de las armas más eficaces. Según datos de Splunk, el 98 % de los ciberataques se basan en técnicas de manipulación emocional o psicológica para obtener acceso a información confidencial.

¿Por qué es tan efectiva? Porque ataca al eslabón más débil: las personas. Y para explotar a las personas, los atacantes necesitan información previa: roles, estructuras internas, tecnologías usadas, nombres de dominio, subdominios, proveedores, contraseñas filtradas... Todo esto forma parte del *digital footprint* que una organización deja expuesta al mundo sin siquiera darse cuenta.

Estas son algunas de las tácticas más comunes:

- *Phishing*: consiste en enviar correos electrónicos o crear sitios web falsos que imitan a entidades legítimas para engañar al usuario y obtener datos personales o credenciales.
- *Shoulder Surfing*: técnica de observación en la que el atacante obtiene información sensible mirando directamente (o con herramientas) mientras la víctima la introduce en su dispositivo.
- *Dumpster Diving*: implica buscar en la basura corporativa documentos desechados que puedan contener información útil, como manuales internos, contraseñas impresas, organigramas o dispositivos antiguos.
- Juego de roles (*pretexting*): el atacante se hace pasar por una figura de confianza (como soporte técnico o un ejecutivo) a través de llamadas, correos o chats para persuadir a la víctima y obtener información sensible.
- Caballo de Troya: engaña a la víctima para que descargue e instale *software* malicioso que abre una puerta trasera en el sistema, otorgando al atacante control remoto del equipo.
- *Web Crawling*: los atacantes recopilan información de sitios web corporativos, redes sociales o foros para entender la estructura de la organización, identificar contactos clave y preparar ataques dirigidos más efectivos.
- Ingeniería Social Inversa: el atacante simula un problema en el sistema y se ofrece como la única solución confiable. Gana la confianza de la víctima al “ayudarla”, logrando así el acceso a información confidencial. Este enfoque combina sabotaje, marketing y soporte para crear dependencia en la víctima.

Reconocimiento externo: el primer paso del ataque (y de la defensa)

El proceso de *surface test* comienza igual que lo haría un actor malicioso: con reconocimiento pasivo. Utilizando técnicas de inteligencia de fuentes abiertas (OSINT), los analistas de CTI recopilan datos públicos sobre la organización desde múltiples frentes:

- Sitios web corporativos
- Redes sociales (especialmente de empleados)
- WHOIS y DNS
- Foros públicos y *deep/dark web*
- Ofertas de empleo y comunicados de prensa

Este reconocimiento revela activos que a menudo la propia organización desconoce que tiene expuestos, incluyendo:

- Servidores olvidados o heredados
- Puertos abiertos innecesarios
- Subdominios sin protección
- Aplicaciones no autorizadas por TI (*Shadow* IT)
- Credenciales corporativas filtradas
- Publicaciones en redes sociales con metadatos sensibles

OSINT como herramienta clave del *surface test*

Herramientas como Shodan o Censys permiten escanear la red pública para identificar servicios y dispositivos conectados: desde *routers* y cámaras hasta servidores de correo electrónico con configuraciones vulnerables.

No se requiere acceso privilegiado: todo es información abierta y disponible. Esto es precisamente lo que convierte al *surface test* en una herramienta tan poderosa y a la vez tan crítica: si nosotros podemos verlo, un atacante también puede.

El *surface test* como metodología no busca únicamente recopilar información, sino analizar, clasificar, priorizar y reportar riesgos. Se trata de construir un inventario preciso de los activos digitales accesibles desde internet, evaluar su criticidad y generar alertas ante cualquier exposición anómala o no autorizada.

En una organización moderna, el área de Vigilancia Digital no solo se encarga de monitorizar amenazas externas en fuentes abiertas o la *dark web*. También realiza tareas proactivas de *surface testing*, incluyendo:

- Descubrimiento de activos digitales no inventariados
- Identificación de credenciales expuestas
- Monitorización de menciones y fugas en plataformas clandestinas
- Evaluación de riesgos reputacionales y de marca
- Alertas sobre posibles campañas de ingeniería social o *spear phishing*

Estas capacidades permiten actuar antes que un incidente ocurra, transformando la postura de defensa reactiva en una defensa anticipada y basada en inteligencia.

Una máxima clave en ciberseguridad es: “no se puede proteger lo que no se ve.” El *surface test* revela justamente eso: lo que está expuesto pero invisible para la propia organización y es, precisamente, en empresas grandes con múltiples sedes, fusiones recientes o estructuras descentralizadas que existan activos huérfanos, configuraciones inseguras o servicios sin monitorización. Un simple entorno de pruebas dejado abierto por un desarrollador puede convertirse en la puerta de entrada para un ataque mayor.

De la teoría a la acción: gestionar la superficie de ataque

La gestión de la superficie de ataque externa (ASM, por sus siglas en inglés) es un proceso continuo, el cual implica:

1. Descubrimiento: inventariar todos los activos expuestos.
2. Clasificación: determinar el tipo de activo, su función y criticidad.
3. Análisis: buscar vulnerabilidades, configuraciones débiles o credenciales asociadas.
4. Priorización: definir el riesgo real y el impacto potencial.
5. Mitigación y seguimiento: coordinar con equipos de IT, SOC o desarrollo.

Esto requiere no solo tecnología, sino procesos, talento y visión estratégica. Y, sobre todo, un entendimiento claro de que la superficie de ataque no termina en el perímetro del firewall, sino que se extiende tanto como se extienden las huellas digitales de los empleados y los sistemas en Internet.

Realizar un *surface test* no es una acción puntual, sino una práctica estratégica. Es la base sobre la cual se construyen políticas de *hardening*, se priorizan parches, se fortalecen controles de acceso y se anticipan campañas de ingeniería social.

En el panorama actual, donde los ataques se dirigen cada vez más hacia las personas y no solo hacia los sistemas, comprender y anticipar el comportamiento del adversario se vuelve una prioridad. La ingeniería social, combinada con técnicas de reconocimiento como el *footprinting* y el uso de inteligencia de fuentes abiertas (OSINT), demuestra que los atacantes no necesitan vulnerar una infraestructura técnica si pueden explotar el eslabón más débil: el factor humano.

Desde los equipos de Vigilancia Digital, resulta fundamental no solo monitorizar la infraestructura digital expuesta, sino también adoptar una mentalidad ofensiva para detectar proactivamente vectores de ataque, huellas digitales no controladas, credenciales filtradas, presencia en la *dark web*, y señales tempranas de amenazas. La gestión de la superficie de ataque externa (EASM) y el análisis continuo del entorno digital son herramientas clave para anticipar riesgos, minimizar la exposición y proteger tanto los activos tecnológicos como la información crítica.

Solo comprendiendo cómo piensan y actúan los atacantes —y utilizando sus mismas herramientas y técnicas con fines defensivos— podremos construir estrategias de protección realmente eficaces. En este nuevo paradigma, la vigilancia digital deja de ser un complemento y se convierte en un pilar esencial de cualquier programa de ciberseguridad moderno.

Carlos Barrios
Cyber Threat Intelligence Lead Analyst

Tecnologías cuánticas

Espacio cuántico
por María Gutiérrez

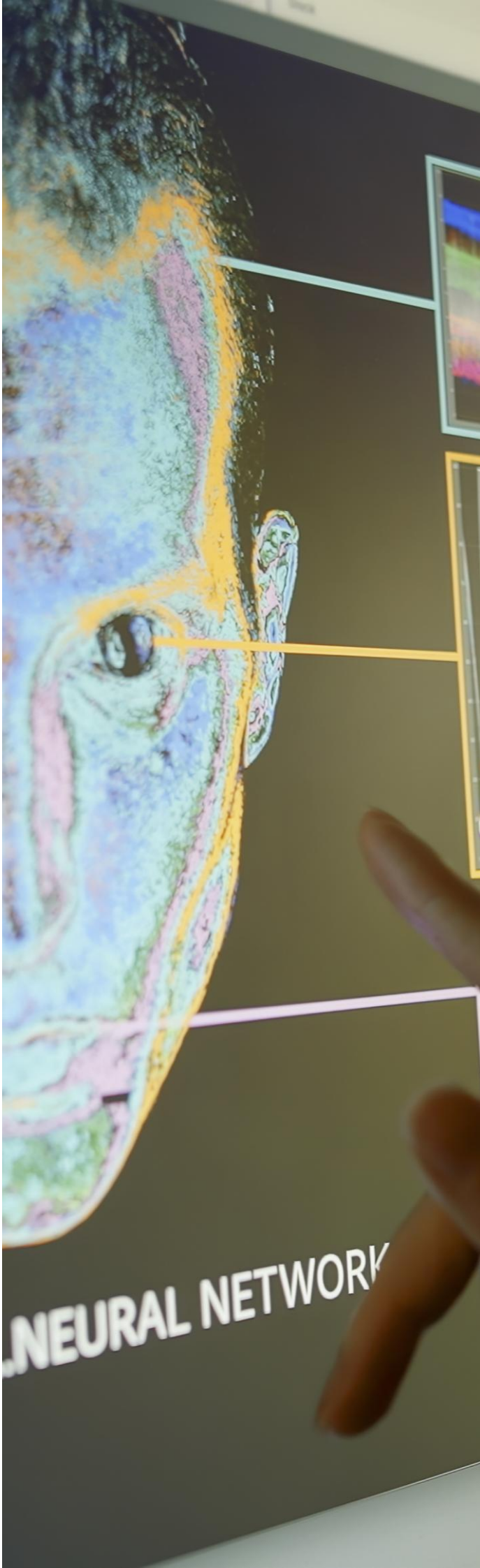
Como ya hemos comentado, el 2025 ha sido proclamado como Año Internacional de la Ciencia y la Tecnología Cuánticas por la ONU. Al leerlo, a casi todos se nos viene a la cabeza la computación cuántica, pero la industria cuántica abarca mucho más, de hecho, la categoría más amplia de tecnologías cuánticas aprovecha el comportamiento de las partículas para una amplia gama de aplicaciones, incluidas herramientas de navegación, tecnología de imagen mejorada y dispositivos de sincronización extremadamente precisos.

Nos vamos a centrar en este artículo en la “sensórica cuántica”, una aplicación de la tecnología cuántica que permite medir fenómenos físicos con una precisión, sensibilidad y resolución sin precedentes. Estos sensores pueden superar los límites de los dispositivos clásicos y ofrecer soluciones innovadoras a problemas industriales y sociales.

A diferencia de los sensores clásicos, los sensores cuánticos pueden registrar variaciones diminutas en el entorno (movimiento, campos electromagnéticos, etc.) aprovechando que los estados cuánticos son extremadamente sensibles a perturbaciones externas.

De este modo, logran resoluciones espaciales y sensibilidades extraordinarias que abren nuevas posibilidades en múltiples campos. Por ejemplo, en el sector sanitario y biomédico, la sensórica cuántica promete revolucionar las técnicas de diagnóstico por imagen y la monitorización de procesos fisiológicos, así como los magnetómetros de bombeo óptico (OPM), que son sensores cuánticos basados en átomos gaseosos que permiten realizar magnetoencefalografía (MEG) de forma más flexible que los sistemas convencionales.

Ya existen cascos portátiles repletos de estos sensores OPM que registran los campos magnéticos producidos por la actividad cerebral, posibilitando que el paciente se mueva libremente durante el examen clínico.



Esto abre la puerta a estudios del cerebro en condiciones más naturales y a nuevas aplicaciones diagnósticas.

En el ámbito de la defensa, los sensores cuánticos ofrecen ventajas estratégicas en detección y navegación. Un área de gran interés es la navegación inercial cuántica, que permitiría a vehículos militares (submarinos, buques o aeronaves) orientarse con alta precisión sin depender de GPS.

Actualmente, si un submarino opera sumergido durante semanas, su sistema inercial convencional acumula error (deriva) y eventualmente debe salir a la superficie para recalibrar con GPS.

Con acelerómetros y giróscopos cuánticos basados en átomos fríos, esta deriva podría eliminarse, proporcionando navegación continua y segura incluso en entornos donde las señales satelitales estén bloqueadas o sean vulnerables a interferencias.

El espacio exterior por su lado es un entorno ideal para aprovechar la sensórica cuántica, por ejemplo, en exploración planetaria y astronomía. En condiciones de microgravedad, los interferómetros atómicos pueden alcanzar tiempos de medición más largos y, por tanto, mayor sensibilidad que en la Tierra. También permite desarrollar gravímetros cuánticos espaciales que midan con altísima resolución el campo gravitatorio de la Tierra u otros cuerpos celestes.

Por ejemplo, futuras misiones podrían mapear la distribución de masa de un planeta o luna detectando variaciones gravitatorias sutiles, ya que distintos materiales (agua, roca o hielo) producen ligeras diferencias locales en la gravedad.

En resumen, la sensórica cuántica está emergiendo como una tecnología disruptiva que traslada los extraños fenómenos de la física cuántica desde el laboratorio hasta aplicaciones del mundo real, y es que no solo de computación vive la cuántica.

La huella digital en la mira: análisis, riesgos y protección en 2025

Tendencias por Joel Pérez y Rodrigo Rey

En la era digital, todos dejamos un rastro en Internet: comentarios, fotos, perfiles sociales, registros públicos y más. A este rastro se le conoce como huella digital, y su análisis se ha vuelto una práctica clave tanto para la ciberseguridad como para los ataques. La disciplina de inteligencia de fuentes abiertas (OSINT) se encarga de recopilar y examinar información pública disponible en la web para convertirla en inteligencia útil. Esta información proviene de diversas fuentes: redes sociales, foros, blogs, registros gubernamentales o noticias, entre otros. Entender la huella digital propia o de una organización es vital: puede revelar reputación, relaciones y posibles vulnerabilidades.

Herramientas modernas para rastrear la huella digital

En los últimos años han surgido numerosas herramientas OSINT para facilitar el rastreo y análisis de la huella digital de personas y empresas. Por ejemplo, plataformas como Maltego o SpiderFoot permiten reunir datos dispersos y visualizar conexiones entre individuos, organizaciones y activos digitales.

Otras herramientas como Shodan actúan como motores de búsqueda especializados en dispositivos conectados a Internet. Shodan permite descubrir servidores, cámaras o routers expuestos públicamente, incluso identificando aquellos con contraseñas débiles o *software* desactualizado.

También existen buscadores enfocados en redes sociales (*social searchers*) que monitorizan menciones públicas en tiempo real, útiles para vigilar la reputación en línea. Estas herramientas automatizadas ahorran tiempo a analistas al recopilar información de múltiples fuentes, pintando un mapa detallado de la presencia online de un sujeto.

Vulnerabilidades expuestas mediante información pública

La huella digital no solo importa por lo que dice de nosotros, sino por lo que puede revelar en términos de seguridad. Mucha información aparentemente inocua puede ser aprovechada por atacantes.

Un caso común es el uso de búsquedas avanzadas tipo Google Dorks para localizar datos sensibles indexados por error, como documentos confidenciales en servidores públicos o listas de contraseñas expuestas.

Del mismo modo, herramientas OSINT como Shodan pueden destapar sistemas vulnerables accesibles desde Internet – por ejemplo, una cámara de seguridad sin credenciales robustas o un servidor corporativo con puertos abiertos indebidamente.

Otra utilidad popular es FOCA, una herramienta desarrollada en España que extrae metadatos de documentos públicos (PDF, Office, imágenes) para descubrir información oculta: nombres de usuarios, rutas internas de archivos, versiones de software e incluso posibles direcciones IP internas.

Toda esta información recopilada sin entrar directamente a ningún sistema permite a los profesionales (y también a los delincuentes) detectar puntos débiles. En auditorías de seguridad, el OSINT ayuda a identificar credenciales filtradas, configuraciones erróneas o datos personales expuestos que podrían facilitar un ataque. Con suficiente ingenio, los datos públicos se vuelven piezas de un rompecabezas que revela brechas de seguridad.

Ingeniería social potenciada por la huella digital

La ingeniería social es el arte de manipular a las personas para obtener acceso o información confidencial, y se ha visto profundamente reforzada por la abundancia de datos en línea. Los atacantes emplean técnicas de OSINT para recopilar todo dato disponible de sus víctimas y así personalizar sus engaños.

¿El resultado? Ataques más creíbles y dirigidos. Un ejemplo claro es el *spear phishing* o *phishing* dirigido: en lugar de enviar correos genéricos, el delincuente investiga a su objetivo en redes sociales y otras fuentes, averiguando su nombre, cargo, compañeros de trabajo, gustos o hábitos.

Con esa información, redacta un correo electrónico muy convincente, quizá aparentando provenir de un colega o un servicio que la víctima utiliza, mencionando detalles específicos para ganar su confianza. De hecho, hoy en día cada intento de *phishing* sofisticado aprovecha datos detallados para que el mensaje parezca legítimo y único.

Si la víctima suele publicar sobre sus viajes, el gancho puede ser una falsa confirmación de vuelo; si es un directivo, puede recibir un correo aparentemente de RR.HH. con información interna. Esta personalización dificulta enormemente distinguir el engaño.

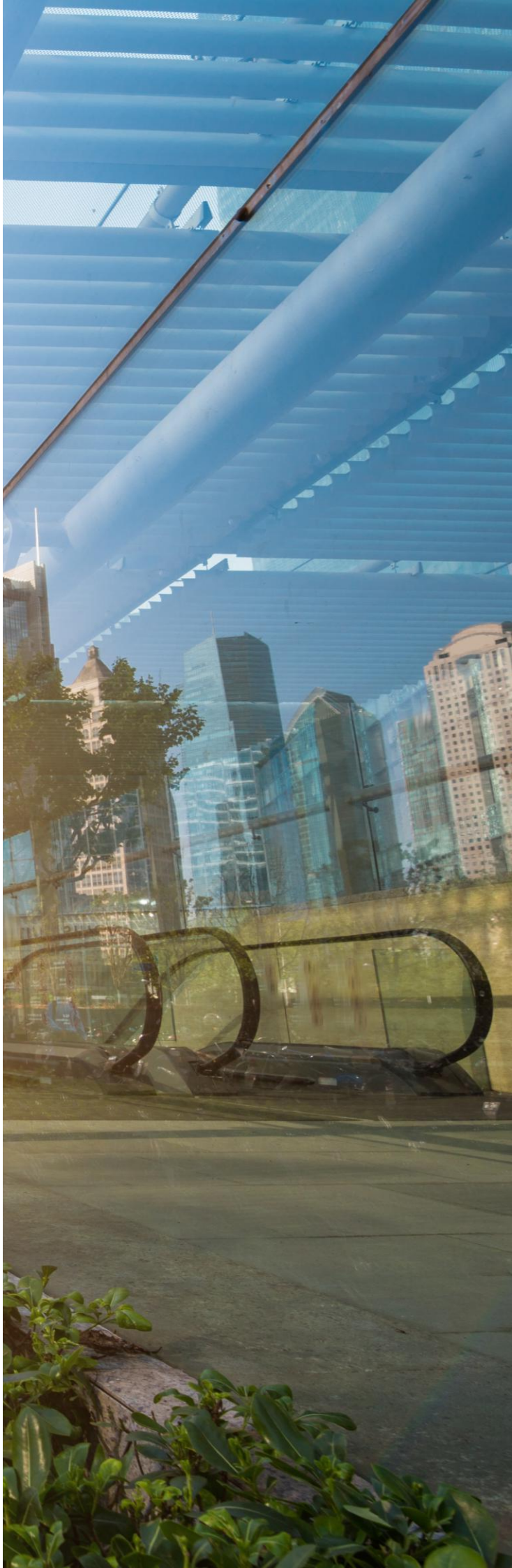
La situación se ha vuelto más compleja con la irrupción de la inteligencia artificial (IA) en estas tácticas. Herramientas de IA generativa pueden producir mensajes en el estilo y tono exactos que usaría una empresa o persona, automatizando la creación de correos fraudulentos a gran escala. Incluso se han reportado estafas donde se clonó la voz de un ejecutivo mediante *deepfake* de audio, para ordenar transferencias millonarias por teléfono con una voz que sonaba auténtica. En resumen, la huella digital de una persona (sus datos públicos) es usada como munición para ataques de ingeniería social sumamente convincentes.

Tecnologías emergentes de protección

Frente a estos riesgos, también han surgido herramientas y prácticas innovadoras para proteger la identidad digital y mitigar amenazas basadas en OSINT. Por un lado, los expertos recomiendan fortalecer los fundamentos: limitar la información personal que compartimos públicamente, configurar adecuadamente la privacidad en redes sociales y mantener contraseñas seguras (idealmente apoyadas con autenticación multifactor). Medidas como la autenticación en dos pasos (2FA/MFA) añaden una capa extra que ha demostrado reducir significativamente la efectividad de ataques basados solo en credenciales robadas.

Por otro lado, existen plataformas especializadas de monitorización de la huella digital. Por ejemplo, servicios comerciales de protección de identidad ofrecen rastrear continuamente Internet y la *dark web* en busca de datos personales del cliente (números de documento, correos o contraseñas filtradas).

Un caso es Bitdefender Digital Identity Protection, que analiza hasta el último rincón de la red en busca de cuentas comprometidas, contraseñas expuestas u otra información sensible, alertando al usuario en cuanto detecta una vulneración social y otras fuentes abiertas para detectar intentos de suplantación de identidad o filtraciones de información en tiempo real.



De igual forma, herramientas gratuitas como Have I Been Pwned permiten a cualquier persona verificar si su correo electrónico o número de teléfono ha aparecido en brechas de datos conocidas.

Las empresas, por su parte, pueden recurrir a soluciones como ZeroFOX, que monitorizan redes.

Incluso se están desarrollando algoritmos de IA capaces de analizar videos y audios para identificar *deepfakes* y otras falsificaciones digitales, con el fin de frenar fraudes sofisticados antes de que se consumen.

Finalmente, la concienciación y formación siguen siendo una de las defensas más efectivas. Programas de capacitación en ciberseguridad enseñan a empleados y usuarios a reconocer señales de *phishing* y técnicas de ingeniería social. Mediante simulaciones de ataques controlados, plataformas educativas (por ejemplo, KnowBe4 en el ámbito corporativo) refuerzan buenos hábitos de seguridad en las personas. Con una combinación de tecnología puntera y educación, es posible reducir considerablemente el riesgo que representa la explotación de nuestra huella digital.

Joel Pérez
Lead Architect

Rodrigo Rey
Lead Architect

Vulnerabilidades

Vulnerabilidad crítica en AWS Amplify Studio

Fecha: 5 de mayo de 2025
CVE: CVE-2025-4318

CVSS: 9.5

CRÍTICA

Descripción

Amazon ha detectado esta vulnerabilidad crítica (CVE-2025-4318) que afecta a AWS Amplify Studio, una interfaz visual para desarrollar aplicaciones web y móviles.

Esta vulnerabilidad provoca un problema de validación de entrada en las propiedades del componente de interfaz de usuario de AWS Amplify Studio, concretamente en el paquete “aws-amplify/amplify-codegen-ui”.

Esto podría provocar que un usuario autenticado con permisos para crear o modificar componentes pueda ejecutar código JavaScript arbitrario durante el proceso de renderizado y compilación de componentes.

Solución

Para corregir dicha vulnerabilidad se recomienda actualizar a la versión 2.20.3. de AWS Amplify Studio.

Además, es importante asegurarse de que se actualiza la versión para cualquier código relacionado, y de esta forma incorporar los nuevos cambios.

Productos afectados

Esta vulnerabilidad afecta a la versión 2.20.2 del paquete “aws-amplify/amplify-codegen-ui” de AWS Amplify Studio y a sus versiones anteriores.

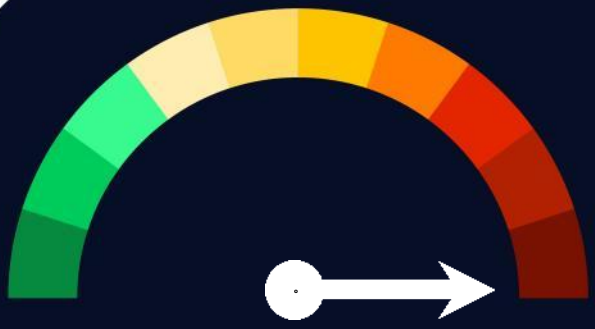
Referencias

- incibe.es
- aws.amazon.com

Vulnerabilidades

Vulnerabilidad de severidad critica en Cisco IOS XE

Fecha: 7 de mayo de 2025
CVE: CVE-2025-20188



CVSS: 10.0

CRÍTICA

Descripción

Cisco ha publicado una vulnerabilidad crítica presente en su controlador inalámbrico IOS XE. Esta vulnerabilidad únicamente afecta a aquellos sistemas que tengan habilitada la función de descarga de imágenes de AP fuera de banda.

La empresa ha indicado en su comunicado que esta vulnerabilidad se debe a la presencia de un *token* web JSON expuesto abiertamente en el código de los sistemas afectados.

Mediante su explotación, un atacante remoto no autenticado podría cargar archivos al sistema afectado, cambiar de directorio y ejecutar comandos con privilegios de *root*.

Solución

Se recomienda actualizar los productos a la última versión publicada por el fabricante.

Por otro lado, para determinar si un dispositivo puede estar afectado por esta vulnerabilidad, Cisco recomienda ejecutar el siguiente comando:

```
> show running config | include ap
upgrade
```

En caso de que este comando devuelva 'ap upgrade method https', el sistema se vería afectado por la vulnerabilidad.

Productos afectados

Algunos de los productos afectados son:

- Controladores inalámbricos Catalyst 9800-CL para la nube.
- Controlador inalámbrico integrado Catalyst 9800 para conmutadores de las series Catalyst 9300, 9400 y 9500.

Referencias

- incibe.es
- sec.cloudapps.cisco.com

Parche de seguridad para corregir vulnerabilidad crítica en SAP NetWeaver

Fecha: 9 de mayo de 2025
CVE: CVE-2025-31324

Crítica

Descripción

Se ha descubierto una vulnerabilidad crítica en SAP NetWeaver Visual Composer (CVE-2025-20188), en el componente Metadata Uploader, con una puntuación CVSS de 10.0.

Este componente no cuenta con una protección adecuada, por lo que un atacante remoto sin autenticación podría cargar archivos arbitrarios con código ejecutable.

La vulnerabilidad ya ha sido explotada, permitiendo la instalación de *web shells* y otras herramientas, y ha sido atribuida a actores vinculados a grupos de origen chino, lo que resalta la necesidad inmediata de aplicar contramedidas para mitigar el riesgo.

Productos afectados

Esta vulnerabilidad afecta a SAP NetWeaver Visual Composer en su versión 7.50, concretamente al componente Metadata Uploader.

Los sistemas comprometidos son utilizados por organizaciones en diversos sectores, como en energía, farmacéutica o manufactura.

Solución

Se recomienda aplicar la actualización de emergencia publicada por SAP que corrige la vulnerabilidad, así como desactivar el componente Visual Composer, a menos que sea estrictamente necesario.

Referencias

- thehackernews.com
- incibe.es

TLP:WHITE

Parches de seguridad de mayo para productos Android

Fecha: 5 de mayo de 2025
CVE: CVE-2025-27363 y 45 más

Alta

Descripción

Google ha publicado su parche de seguridad mensual del mes de mayo, donde se corrigen un total de 46 vulnerabilidades, entre ellas una de severidad alta (CVE-2025-27363) que se encuentra bajo explotación activa.

Esta vulnerabilidad se encuentra en la librería de código abierto de representación de fuentes FreeType y se debe a un fallo de escritura fuera de límites. Esto podría resultar en una ejecución de código de forma remota al parsear TrueType GX y ficheros de fuentes variables.

Por otro lado, el parche corrige otras vulnerabilidades que podrían facilitar ataques de escalada de privilegios, denegación de servicio y divulgación de información confidencial.

Solución

La vulnerabilidad afecta a los siguientes componentes de Android:

- Android Open Source Project (AOSP): versiones 13, 14 y 15.
- Componentes de Arm, MediaTek, Imagination Technologies y Qualcomm.

Productos afectados

Google recomienda actualizar sus dispositivos a la última versión de *software* disponible para solucionar las vulnerabilidades.

Referencias

- thehackernews.com
- source.android.com

Eventos

Infosecurity Europe
3 - 5 junio

Infosecurity Europe, que se celebrará este año en Londres, es el evento líder en el ámbito de la ciberseguridad donde los profesionales del sector se reunirán para discutir y explorar los desafíos actuales y futuros de la seguridad en el mundo digital. Entre las conferencias destacadas se encuentra "AI Attacks LIVE", donde se tratarán ciberataques impulsados por Inteligencia Artificial y su mitigación. Además, el evento explorará la implementación de estrategias eficaces de gestión de riesgos, seguridad en la nube, y las últimas tendencias en protección de infraestructuras críticas.

Enlace

JNIC 2025
4 - 6 de junio

Las X Jornadas Nacionales de Investigación en Ciberseguridad (JNIC), en colaboración con INCIBE, se celebrarán en la Universidad de Zaragoza. Este congreso científico reúne a la comunidad académica, profesional y empresarial para discutir avances y enfoques innovadores en ciberseguridad. Además, se entregarán los Premios RENIC de Investigación en Ciberseguridad a trabajos destacados. El evento se centrará en la investigación, transferencia y formación en ciberseguridad.

Enlace

EuskalHack Security Congress VIII
20 – 21 de junio

La octava edición del EuskalHack Security Congress, que se celebrará en Donostia, destaca como un foro de referencia en ciberseguridad en el País Vasco. Este congreso se centra en la divulgación y el intercambio de experiencias entre expertos del sector, abarcando temas punteros como el uso de inteligencia artificial en ciberseguridad, la seguridad en aplicaciones web, análisis de *malware* y estrategias de vigilancia digital. Los asistentes tendrán la oportunidad de participar en conferencias impartidas por profesionales de la industria y acceder a talleres prácticos que fortalecen la colaboración y el aprendizaje en nuevas técnicas de protección y reacción ante ciberataques.

Enlace

Recursos

➢ CAIDO

Es una herramienta que tiene que como objetivo facilitar los análisis web en las auditorías de seguridad. Busca ofrecer una alternativa moderna y eficiente a otras herramientas más tradicionales como Burp Suite.

Enlace

➢ YES3 Scanner

YES3 Scanner es una herramienta de código abierto que escanea y analiza los diferentes elementos de configuración de los contenedores S3 de AWS para detectar riesgos de seguridad y así poder reducirlos como los accesos públicos, tipos de encriptación, protección contra *ransomware* o el plan de recuperación de datos entre muchos otros.

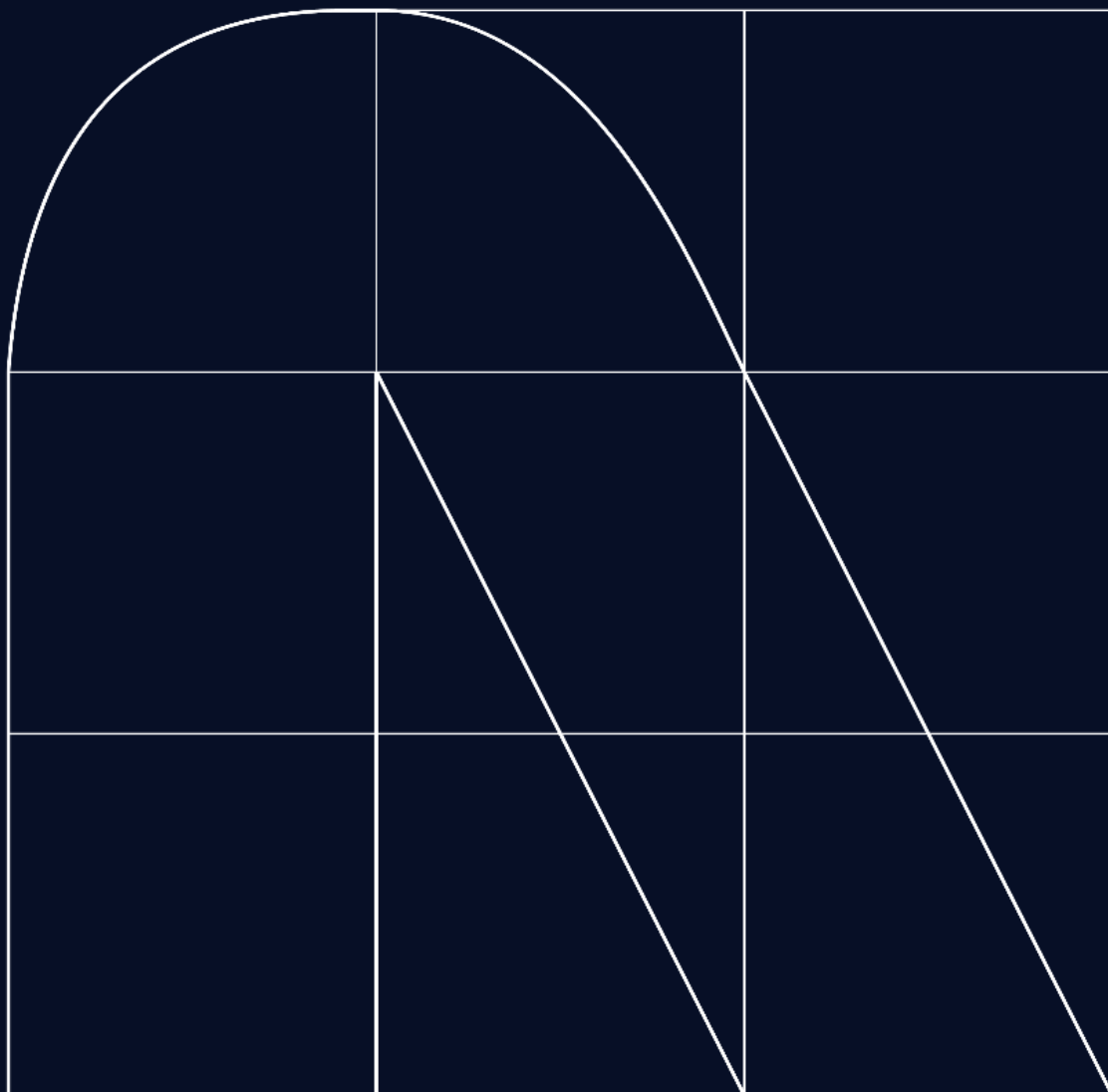
Enlace

➢ Sniffnet

Sniffnet es una herramienta de código abierto diseñada para la monitorización y análisis de tráfico de red en tiempo real. Su principal objetivo es capturar, visualizar y analizar el tráfico de red de una manera sencilla y accesible en comparación con otras más famosas como Wireshark.

Enlace

Suscríbete a RADAR
up.nttdata.com/suscribetearadar



Powered by the cybersecurity NTT DATA team

es.nttdata.com