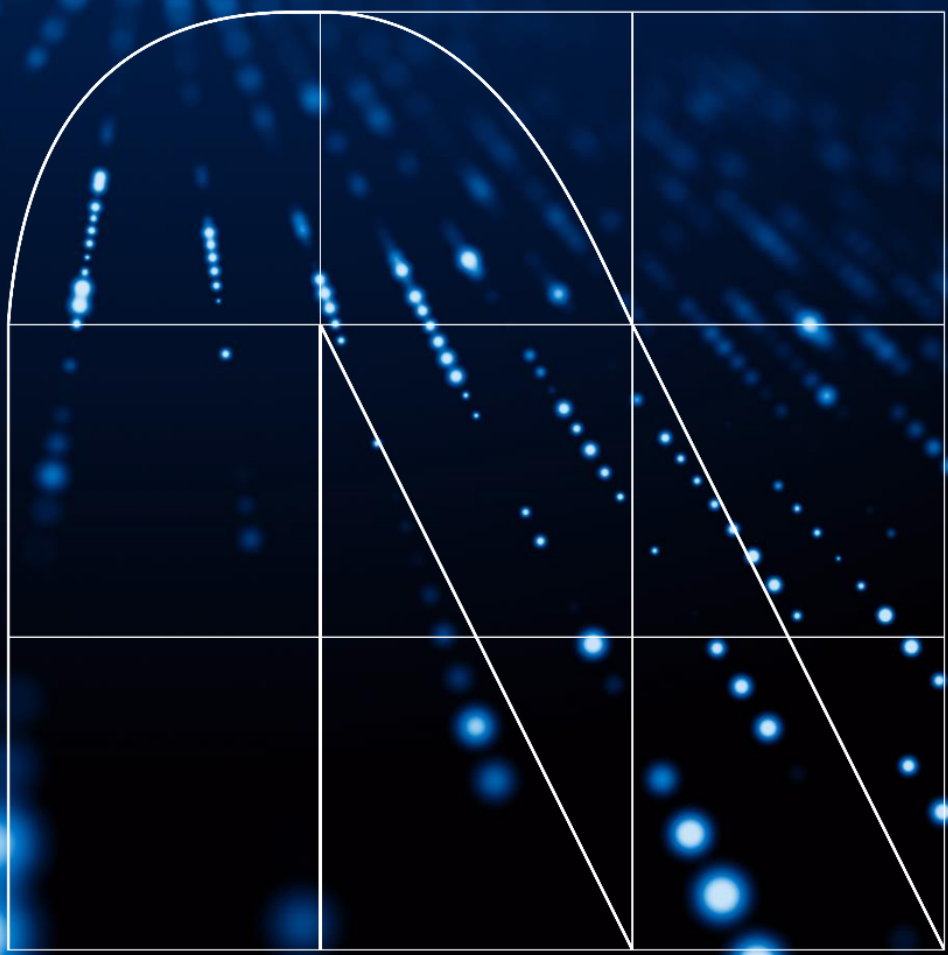
Número 102 | Mayo 2025

NTT DATA

Radar

El magazine de ciberseguridad



Navegando la Convergencia de la Ciberseguridad en IT y OT

Por Carlos Solano

En el panorama digital actual, la convergencia de la Tecnología de la Información (IT) y la Tecnología Operacional (OT) se ha convertido en un enfoque fundamental para las organizaciones de diversas industrias. A medida que las empresas dependen cada vez más de sistemas interconectados para impulsar la eficiencia y la innovación, la necesidad de una estrategia de ciberseguridad robusta que abarque tanto los entornos de IT como de OT nunca ha sido más crítica. Este editorial explora las estrategias más relevantes para gestionar eficazmente la ciberseguridad en este paisaje convergente.

La integración de IT y OT trae numerosos beneficios, incluyendo una mejor analítica de datos, una toma de decisiones más informada y operaciones más eficientes. Sin embargo, también introduce desafíos significativos en ciberseguridad. Los sistemas de OT, que controlan procesos físicos en industrias como la manufactura, la energía y el transporte, tradicionalmente estaban aislados de las redes de IT. Esta separación proporcionaba un nivel de seguridad, pero a medida que las organizaciones adoptan la transformación digital, las líneas entre IT y OT se están difuminando, creando nuevas vulnerabilidades y oportunidades para los atacantes.

Al crear un enfoque cohesivo entre ambos mundos, las organizaciones pueden asegurarse de que todos los equipos estén alineados en sus esfuerzos por proteger activos críticos.

Las organizaciones deben adoptar una visión holística de sus riesgos, considerando el impacto en las operaciones. Esta evaluación integral permite priorizar las medidas de seguridad, asegurando que los recursos se asignen de manera efectiva para mitigar las amenazas más significativas.

La implementación de la segmentación de redes es una estrategia crucial para proteger los sistemas de OT de posibles brechas que se originen en las redes de IT. Al aislar los entornos de OT mediante cortafuegos, redes de área local virtual (VLAN) y zonas desmilitarizadas (DMZ), las organizaciones pueden contener amenazas y limitar la capacidad de los atacantes para moverse lateralmente entre redes.

Establecer medidas estrictas de control de acceso es vital para salvaguardar sistemas críticos. Las organizaciones deben implementar controles de acceso basado en roles (RBAC) y autenticación multifactor (MFA) para garantizar que solo el personal autorizado pueda acceder a datos y sistemas sensibles.

Este enfoque reduce el riesgo de amenazas internas y mejora la postura de seguridad general.

Un plan de respuesta a incidentes unificado que aborde incidentes tanto de IT como de OT es esencial para una gestión efectiva de amenazas. Este plan debe delinear roles, responsabilidades y procedimientos para detectar, responder y recuperarse de incidentes de ciberseguridad. Una respuesta coordinada entre ambos dominios asegura que las organizaciones puedan actuar rápidamente para minimizar daños y restaurar operaciones.

Las soluciones de monitorización continua proporcionan visibilidad en tiempo real de los entornos de IT y OT, permitiendo a las organizaciones detectar amenazas potenciales antes de que escalen. Utilizar sistemas de gestión de información y eventos de seguridad (SIEM), sistemas de detección de intrusiones (IDS) y herramientas de detección de anomalías puede mejorar significativamente la capacidad de una organización para responder ante amenazas emergentes.

La convergencia de IT y OT presenta tanto oportunidades como desafíos para las organizaciones. Al adoptar un enfoque integral hacia la ciberseguridad que incluya un marco de seguridad unificado, evaluaciones de riesgos, segmentación de redes y monitorización continua, las empresas pueden manejar eficazmente este complejo escenario. A medida que avanzamos, es imperativo que las organizaciones prioricen la ciberseguridad en sus estrategias de convergencia, asegurando la resiliencia y seguridad de sus operaciones en un mundo cada vez más interconectado. El futuro de las operaciones industriales depende de nuestra capacidad para proteger estos sistemas críticos de las amenazas en evolución.

Carlos Solano
Cybersecurity Manager

 © Copyright NTT DATA, Inc.

Privacidad en la IA: Un actor relevante habilitado que opera algunas veces sin los controles necesarios

Cibercrónica por Antonio Melo y Carlos Ortega

A medida que el panorama digital se vuelve más complejo, la ciberseguridad se posiciona como uno de los retos estratégicos más apremiantes para empresas, administraciones y ciudadanos. Tres noticias recientes evidencian la urgencia de reforzar las defensas: el alarmante incremento del 137% en ataques DDoS en Europa, el protagonismo de España como principal objetivo de ciberataques y las investigaciones en curso de Oracle sobre una posible brecha en entornos legados relacionada con la vulnerabilidad CVE-2021-35587.

Europa bajo ataque: DDoS en aumento

El último informe europeo de ciberseguridad revela que los ataques de denegación de servicio distribuido (DDoS) han experimentado un incremento del 137% en comparación con el año anterior.

Estos ataques, aunque son breves (algunos alcanzan su pico en apenas 10 a 60 segundos), tienen más sofisticación ya que utilizan técnicas combinadas –conocidas como ataques multivectoriales– para superar las medidas defensivas tradicionales.

La rapidez y precisión de estos ataques obligan a las organizaciones a adoptar soluciones de mitigación en tiempo real y sistemas basados en inteligencia artificial para detectar y bloquear flujos de tráfico malicioso antes de que logren interrumpir servicios críticos.

España, el blanco favorito de los ciberdelincuentes

En el ámbito nacional, declaraciones recientes del presidente de Indra, Ángel Escribano, han puesto de relieve que España encabeza la lista de países atacados en febrero, superando a potencias como Estados Unidos e Israel.

Según Escribano, la creciente relevancia tecnológica y económica de España, impulsada por un acelerado proceso de digitalización y la expansión de la infraestructura digital en sectores estratégicos, ha convertido al país en un objetivo prioritario para ciberataques dirigidos.

La exposición de una amplia base de pequeñas y medianas empresas, junto con una carencia relativa de profesionales especializados en ciberseguridad, agrava este panorama y demanda una respuesta coordinada entre el sector público y privado.

Oracle en la mira: Brecha en entornos legados

Por otro lado, Oracle ha iniciado una investigación sobre una posible brecha relacionada con la vulnerabilidad CVE-2021-35587 en entornos legados.

Aunque la vulnerabilidad fue identificada y parchada en 2021, se ha comprobado que algunos sistemas antiguos, que aún utilizan versiones obsoletas del Oracle Access Manager, permanecen expuestos.

Esta falla, con una puntuación CVSS de 9.8, permite a un atacante acceder sin autenticación a los sistemas a través de HTTP, comprometiendo la integridad, confidencialidad y disponibilidad de las aplicaciones afectadas.

Expertos en ciberseguridad instan a las organizaciones a actualizar inmediatamente sus entornos para evitar que esta brecha sea explotada, lo cual podría desencadenar consecuencias críticas y ampliar el alcance de los ciberataques.

Reflexiones y recomendaciones

El aumento vertiginoso de ataques DDoS en Europa, la consolidación de España como territorio vulnerable y la persistencia de brechas en sistemas legados como el de Oracle son una llamada de atención.

Estas amenazas subrayan la necesidad de que las organizaciones inviertan en tecnologías de detección y respuesta basadas en inteligencia artificial para anticipar y mitigar ataques en tiempo real.

Además, es necesario que se fortalezcan los protocolos de seguridad, actualizando de forma rigurosa y periódica sus sistemas, especialmente aquellos que operan en entornos *legacy*.

La cooperación entre el sector público y privado debe ser fomentada a través del flujo de información de amenazas y la coordinación de respuestas ante incidentes críticos.

En un mundo digital en constante evolución, la capacidad de adaptarse y mejorar las defensas será fundamental para garantizar la resiliencia de las infraestructuras críticas y la seguridad de la economía digital.

Con este escenario, la acción inmediata y coordinada se convierte en el pilar para contrarrestar los ciberataques, protegiendo tanto a las empresas como a los ciudadanos de las consecuencias de un entorno digital cada vez más hostil.

Antonio Melo
Cybersecurity Analyst

Carlos Ortega
Cybersecurity Analyst

Disponibilidad vs Seguridad en entornos industriales

Artículo por Miren Ordoñez de Arce

“Un hacker accedió al sistema de control de una planta de tratamiento de agua y provocó el envenenamiento masivo de la población de Oldsmar, Florida, en 2021”, “*Malware* dirigido a una planta petroquímica desactiva los mecanismos de protección ante fallas catastróficas y genera una explosión que causa la muerte de decenas de personas en Arabia Saudí” o “Ataque *ransomware* en una planta hidroeléctrica provoca el caos social debido a la interrupción de la energía en Sudamérica en 2022”. ¿Te suenan estos titulares? ¿No? Porque no ocurrieron. Pero podían haber sido una realidad.

En 2021, en Oldmsar, Florida, un ciberdelincuente obtuvo acceso remoto al sistema de control de la planta a través de TeamViewer y aumentó los niveles de hidróxido de sodio (conocido como lejía) a niveles peligrosos, más de 100 veces sus niveles normales; pudiendo haber envenenado el suministro de agua de la población. Sin embargo, un operario detectó en tiempo real los cambios que el hacker había realizado y los revirtió de forma manual, evitando el envenenamiento masivo, la saturación de los hospitales, y el elevado coste de descontaminación y restauración del sistema de agua.

En 2017, un *malware* denominado “Triton”, también conocido como “Trisis”, había sido desplegado en una planta petroquímica en Arabia Saudí, permitiendo a los ciberdelincuentes controlar los sistemas de seguridad de la fábrica de forma remota. Estos sistemas eran la última línea de defensa contra aquellos desastres que podían amenazar la vida de las personas. Funcionaban de tal forma que, si detectaban cualquier tipo de situación peligrosa, entrarían en acción, apagando los sistemas por completo, activando las válvulas de cierre y los mecanismos de liberación de presión. Si el *malware* hubiera tenido éxito, podría haber desactivado estos sistemas de seguridad permitiendo que otros ataques o fallos no detectados resultaran en explosiones o liberaciones tóxicas. Sin embargo, el ataque fue detectado cuando el *malware* provocó un fallo en los sistemas de seguridad, provocando un cierre seguro de las operaciones e impidiendo su movimiento así como daños mayores.

Por último, en 2022, un *ransomware* cifró archivos críticos en los sistemas de control de una planta hidroeléctrica en Sudamérica, interrumpiendo las operaciones de la planta y exigiendo un rescate para liberar los datos.

En caso de éxito del *ransomware*, se podrían haber producido interrupciones prolongadas en el suministro de energía, afectando a millones de usuarios y causando pérdidas económicas significativas. Sin embargo, la planta contaba con protocolos de respuesta a incidentes correctamente establecidos, permitiendo una detección y contención temprana del ataque. Además, la implementación de copias de seguridad periódicas permitió la restauración de los sistemas afectados sin necesidad de pagar el rescate, minimizando el impacto del ataque.

Estos son simplemente algunos ejemplos de las consecuencias físicas, humanas, económicas y reputacionales que puede provocar un ciberataque en un entorno industrial; y todo ello tiene su origen en la salida a la luz de las redes industriales, que previamente se encontraban totalmente aisladas.

Aunque fue en 2014 cuando comienzan a verse las primeras fábricas inteligentes, no fue hasta 2016 cuando se empieza a escuchar el término “Industria 4.0”, encargada de integrar tecnologías avanzadas de producción y operación con tecnologías inteligentes que se comunican entre sí a lo largo de la cadena de suministro, logrando automatizar procesos, personalizar la producción y aumentar la eficiencia, entre otros.

Sin embargo, esto también ha provocado que las industrias sean un jugoso objetivo de ciberataques; principalmente debido a:

- El aumento de la conectividad: el uso de dispositivos IoT en los entornos industriales ha revolucionado la monitorización y el control de los activos, pero también ha creado múltiples puntos de entrada potenciales para ciberataques.
- La integración de tecnologías nuevas con antiguas: prácticamente la mayoría de industrias operan con sistemas *legacy* que no fueron diseñados con la seguridad moderna, dejando con ello agujeros de seguridad.

- La digitalización de procesos: el aumento de la automatización y capacidad de controlar sistemas de forma remota aumentan la superficie de ataque.
- La interacción humana: los empleados componen el eslabón más débil de la cadena y, en muchas ocasiones, no están suficientemente capacitados en prácticas de ciberseguridad, lo que conduce a ser objetivo de ataques de ingeniería social, descuidos y errores.
- El aumento de amenazas avanzadas: las infraestructuras críticas suponen un objetivo muy lucrativo en cuanto al daño causado, ya que en muchas ocasiones existe una interdependencia entre los sectores, lo que puede potenciar y multiplicar el impacto provocado.

Es bien sabido que en los entornos industriales la disponibilidad de los sistemas es una prioridad, por encima de la confidencialidad o la integridad; precisamente debido a la naturaleza crítica de las operaciones industriales.

En muchas ocasiones, las operaciones industriales funcionan de manera continua (como puede ser en una planta de energía), por lo que no pueden permitirse interrupciones. Además, las consecuencias de la inactividad se traducen en pérdidas económicas significativas o incluso pueden suponer riesgos de seguridad física.

Por otro lado, muchos sistemas industriales requieren de respuestas en tiempo real para el control de procesos críticos, lo cual se garantiza a través de la disponibilidad. También cabe mencionar que los propios sistemas, además de ser antiguos, fueron diseñados con un enfoque basado en la resiliencia, no en la seguridad. Por último, a menudo se observa que el riesgo de una interrupción es superior al riesgo de una violación de seguridad.

Todo esto no es novedad; tampoco es un hecho que se haya constatado hace un año, o cinco. Entonces, ¿por qué no se le da más importancia a la ciberseguridad industrial? ¿Es solo cuando se sufre un ciberataque cuando se toman medidas reales? ¿Tanto prima la disponibilidad de los sistemas?

A la hora de decidir si optar por la disponibilidad o la seguridad, las industrias a menudo se preguntan: ¿cuánto costaría detener las operaciones? ¿Podría alguien salir herido si se detiene el sistema? ¿Qué leyes o normativas deben cumplirse para operar de forma segura?

Supongamos una planta de producción de automóviles, que opera 24/7 para satisfacer la demanda global, un día normal como cualquier otro, sufre un ataque que interrumpe el software de control de producción, deteniendo la planta durante días.

Si la planta se ve obligada a detener su producción, cada hora de inactividad podría costar cientos de miles de euros, por no hablar de la pérdida reputacional y posibles penalizaciones adicionales por incumplimientos contractuales. Si la planta hubiera tenido en cuenta la seguridad, aunque el coste inicial de securizarla habría sido sustancial, habría podido evitar el ataque, o por lo menos, haber limitar el impacto.

Aunque los propios sistemas pueden fallar y generar un riesgo para los operarios, como puede por ejemplo ocurrir que una pieza de ensamblado quedase suspendida provocando una situación de riesgo por una interrupción, lo cierto es que esto también lo puede provocar un actor malicioso, como bien hemos comprobado con los ciberataques mencionados. Por lo tanto, a través del aumento de la seguridad se evitarían manipulaciones maliciosas.

Por último, cada vez se encuentran más normativas y estándares cuyo incumplimiento supone sanciones económicas cuantiosas, por lo que cumplir con ellas no sólo ayuda a asegurar la planta, los activos y la información, sino que también protege la reputación, mantiene la confianza de los clientes y fortalece la resiliencia operativa.

La ciberseguridad industrial, aunque al principio pueda parecer costosa, un impedimento para la disponibilidad de la planta e incluso una molestia, es como el héroe silencioso que mantiene el entorno en funcionamiento asegurando una mayor estabilidad y éxito del negocio. Por ello, tal vez conviene dejar de pensar qué prima más, si la disponibilidad o la seguridad, y empezar a tomar acciones que securicen el entorno mientras mantienen y aseguran la operativa.

Miren Ordoñez de Arce
Cybersecurity Lead Analyst

¿Qué perfiles se buscan para trabajar en tecnologías cuánticas?

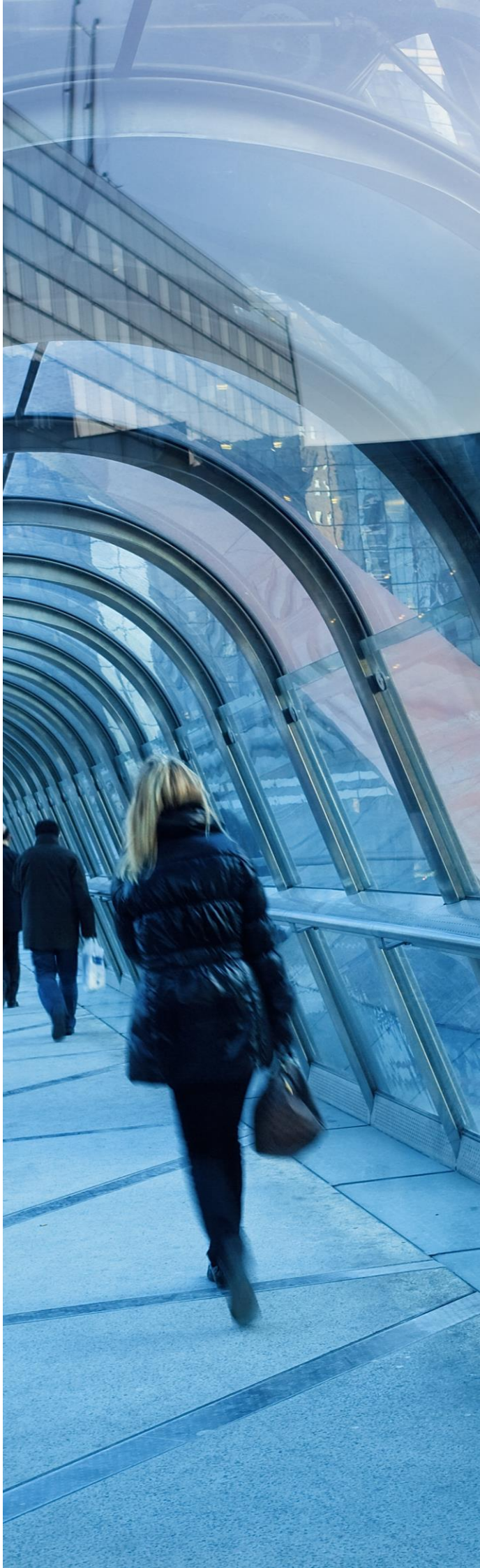
Espacio cuántico por María Gutiérrez

El campo de las tecnologías cuánticas está dejando de ser una promesa lejana para convertirse en un campo en rápida expansión que ya demanda profesionales cualificados. Computación cuántica, comunicaciones cuánticas, sensórica y metrología cuántica son las principales áreas que configuran esta nueva revolución tecnológica, y que requieren la colaboración estrecha de físicos, ingenieros matemáticos, informáticos, filósofos y expertos en ciberseguridad, entre otros. No se trata solo de saber cómo funcionan los sistemas cuánticos desde el punto de vista teórico sino de construir, operar y proteger dispositivos que se comportan de manera diferente a los clásicos.

Desde el equipo de cuántica de NTT DATA hemos definido lo que a nuestro entender son los perfiles llamados a formar parte de este nuevo equipo de trabajo cuántico y las competencias que se les requiere:

Quantum Business (QB) Especialista en identificar oportunidades de negocio en Tecnologías Cuánticas.

- Se requiere un pensamiento estratégico, así como la capacidad para visualizar cómo las tecnologías cuánticas pueden transformar modelos de negocio. También se debe controlar los análisis de negocio y viabilidad junto con la evaluación de la aplicabilidad y rentabilidad de soluciones cuánticas.
- Optimización de decisiones y uso de herramientas cuantitativas para priorizar inversiones en tecnologías cuánticas. Conocimiento de mercados emergentes y comprensión del impacto de la computación cuántica en diferentes industrias (finanzas, salud, logística, etc.). Además, es importante contar con la habilidad para comunicar conceptos cuánticos a *stakeholders* no técnicos.



 © Copyright NTT DATA, Inc.

Quantum Mathematics (QM) Especialista en modelado matemático y representación cuántica de problemas.

- Modelado matemático avanzado. Diseño de representaciones QUBO, Ising y modelos gráficos. Optimización combinatoria, aplicación de métodos cuánticos y clásicos para problemas NP-hard. Algoritmos cuánticos para simulación. Desarrollo de enfoques híbridos y algoritmos heurísticos. Análisis de rendimiento, evaluación de métricas de eficiencia y precisión en soluciones cuánticas. Teoría de la información cuántica.

Quantum Researcher (QR) Investigador especializado en el estudio y validación de algoritmos cuánticos para problemas complejos.

- Investigación y desarrollo. Exploración de nuevos enfoques en algoritmos cuánticos. Análisis comparativo, evaluación de eficiencia entre algoritmos clásicos y cuánticos, experimentación y validación, diseño de experimentos controlados para probar rendimiento de algoritmos cuánticos. Publicación científica, redacción y divulgación de avances en revistas y congresos especializados. Transformación de datos en representaciones adecuadas para Quantum Computing.

Quantum HW Engineering (QHE) Ingeniero especializado en el diseño, implementación y optimización de hardware cuántico para la ejecución de algoritmos y simulaciones.

- Arquitectura de hardware cuántico. Diseño y configuración de procesadores cuánticos y circuitos superconductores, programación de *hardware* cuántico, uso de lenguajes como Qiskit, Cirq y Ocean SDK. Optimización de ejecución en hardware, ajuste de parámetros y mitigación de ruido en cúbits.
- Electrónica y superconductividad, entendimiento de las propiedades físicas del hardware cuántico, integración de sistemas híbridos, comunicación entre hardware cuántico y sistemas clásicos.

Quantum Deployment Team (QDT) Equipo responsable de la implementación, optimización y despliegue de algoritmos cuánticos en entornos de producción IT.

- Optimización de código cuántico. Refinamiento de algoritmos cuánticos para ejecución eficiente en *hardware* y simuladores. Despliegue en *cloud* híbrido, implementación de soluciones cuánticas en plataformas como AWS Braket, IBM Quantum, Azure Quantum. Automatización de procesos IT, creación de flujos CI/CD para el mantenimiento de código cuántico en producción. Seguridad y fiabilidad en Quantum IT, implementación de estándares de seguridad y estabilidad en entornos cuánticos.

Quantum Developer (QD) Desarrollador especializado en la programación, optimización y validación de algoritmos cuánticos para resolver problemas específicos.

- Programación cuántica. Uso de lenguajes como Qiskit, Cirq, Ocean SDK y Pennylane, desarrollo de algoritmos cuánticos, implementación de algoritmos como QAOA, VQE y Quantum Annealing. Optimización de código cuántico, refinamiento de algoritmos para mejorar eficiencia y reducir errores. Análisis de datos cuánticos, transformación y preprocesamiento de datos para su uso en computación cuántica.

Los perfiles que hoy empiecen a formarse en este ámbito estarán en una posición privilegiada para liderar el desarrollo de los próximos 5-10 años. Más allá de la formación académica, será clave desarrollar una mentalidad interdisciplinar y flexible, ¡porque trabajar en cuántica no es solo entender una nueva forma de computar es aprender a pensar de una manera radicalmente distinta!

Hiperconectividad

Tendencias por Alejandro García Muñiz y Raquel Gálvez Huertas

Actualmente es difícil imaginar un mundo sin comunicación constante a través de dispositivos tecnológicos y un intercambio continuo de datos. La hiperconectividad se ha convertido en un concepto omnipresente que define la sociedad actual. Por un lado, las organizaciones llevan por bandera la eficiencia y productividad, mientras que las personas quieren mayor bienestar y tiempo libre, en ambos casos la transformación digital parece el mejor aliado para buscar estas soluciones, dando como respuesta cada vez más interconexiones a través de la red. Por otro, esta crecientehiperconectividad y dependencia tecnológica también plantea un conjunto de nuevos desafíos, como la salud mental o la gran variedad de vulnerabilidades potencialmente explotables impulsadas por los riesgos y amenazas digitales, que requieren estrategias innovadoras para proteger la privacidad y seguridad de los usuarios en un entorno digital en constante evolución.

Explosión IoT, de cientos a millones

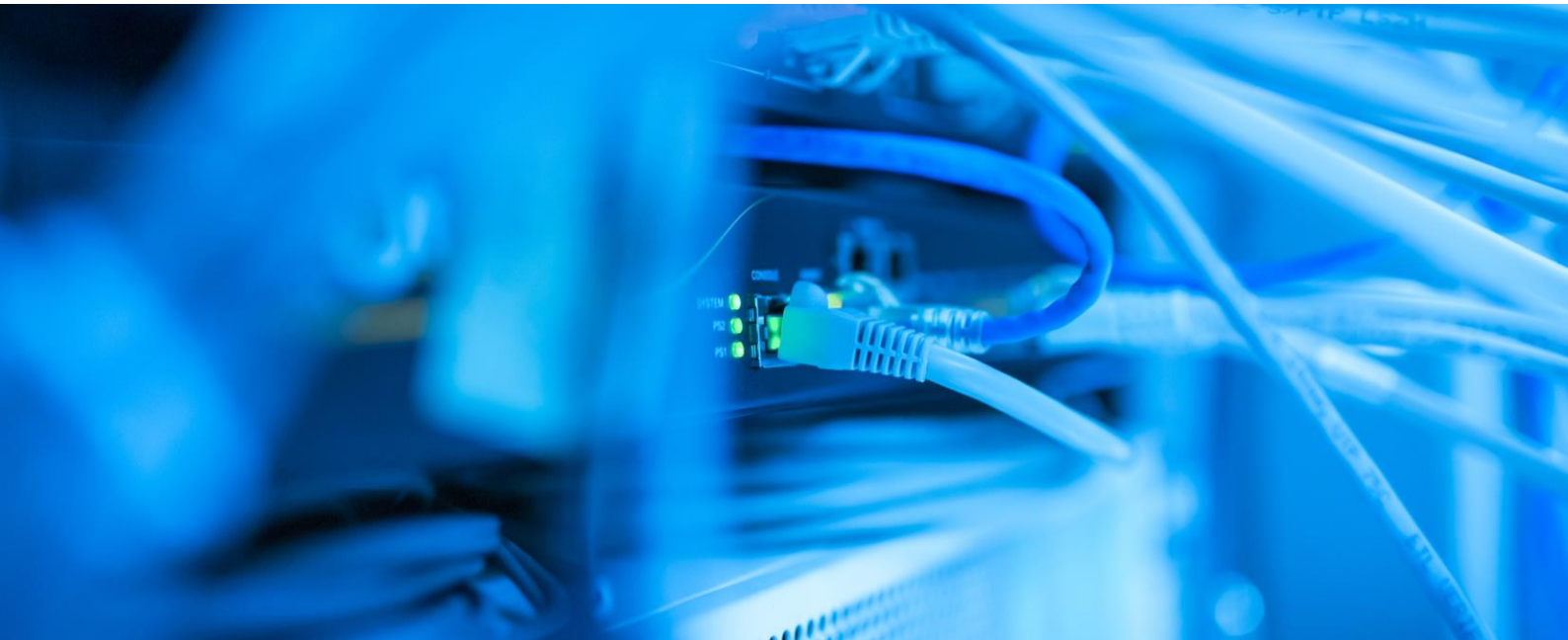
Desde el surgimiento de los primeros dispositivos IoT se ha presenciado un incremento exponencial en la cantidad de dispositivos interconectados, saliéndose de las expectativas estadísticas estimadas por los estudios y sorprendiendo por su rápido crecimiento a la industria. Mientras en 2015 se estimaba que un total de 3.5 billones de dispositivos estuviesen activos y conectados a internet, la cifra real osciló entorno a los 10 billones de dispositivos.

En esos mismos estudios se estimaba que en 2020 habría un total de 9.9 billones de dispositivos conectados, llegando a 21.5 billones en 2025, pero las cifras reales marcaron que un total de 11.7 billones de dispositivos se conectaron en 2020 y que, en 2025, oscilarán en torno a los 75 billones de dispositivos, lo que implicaría un crecimiento porcentual de más del 600%, siendo este crecimiento principalmente espoleado por los avances en IA y el 5G.

Vulnerables y peligrosos

Actualmente estos dispositivos se usan en todos los ámbitos sociales y sectores, desde la privacidad del hogar hasta grandes organizaciones que dan servicio a millones de usuarios: educación, sanidad, transportes, administraciones públicas, etc. La seguridad, desde el diseño, pasa a ser clave en el desarrollo de estos dispositivos IoT para mantener la confidencialidad, integridad y disponibilidad de la información que manejan, pues más del 50% tiene vulnerabilidades críticas por defecto que son explotadas por piratas informáticos antes de que puedan ser parcheadas. El *firmware* desactualizado potencia el 60% de ataques IoT que podrían prevenirse con actualizaciones automáticas y configuraciones de seguridad que garanticen que los dispositivos sean resilientes desde el inicio y estén preparados para enfrentar amenazas emergentes.

Asimismo, la integración de la IA y los LLM en los dispositivos IoT, incrementa la superficie de ataque al amplificar las vulnerabilidades inherentes de cada componente, lo que exige una mayor atención a las estrategias de seguridad.



Más conexiones que suman ataques

Hilado a lo anterior, estos problemas de seguridad desde el diseño, la cantidad de vulnerabilidades que afectan a los dispositivos y la necesidad de renovar constantemente los mismos, han generado una gran oportunidad para los actores de amenazas. En 2022 se registraron más de 112 millones de ataques a dispositivos IoT, cerca de un 200% más de ataques en comparación a los 32 millones de 2018. Pero el verdadero impacto se aprecia en las estadísticas aportadas por grandes fabricantes de AV en 2024, quienes afirmaron que, durante el primer semestre de 2024, se había registrado un promedio de más de 50 intentos de explotación semanales, incrementándose a nivel global la cantidad de ataques registrados en un 75%.

Nuevos dispositivos, nuevos atacantes

La era de la hiperconectividad ha transformado la manera de interactuar, pero también ha abierto la puerta a un conjunto de complejas amenazas. Para el año 2025, se espera que los actores de amenazas aprovechen tecnologías y tácticas avanzadas para explotar las vulnerabilidades del IoT.

Entre estos peligros destacan grupos como Volt Typhoon, RansomHub y Andariel, que actúan de manera sistemática para explotar vulnerabilidades a través de diversos sectores industriales y públicos. A su vez, Sandworm, con vínculos con la agencia de inteligencia militar de Rusia, dirige sus esfuerzos hacia los sistemas operativos de tecnología crítica.

Por otro lado, CYBERAV3NGERS, afiliados a Irán, dirigen sus ataques a infraestructuras críticas, incluyendo complejos sistemas de IoT. Y el grupo Qilin Ransomware Group se enfoca en interrumpir procesos industriales, tambaleando así la confianza y estabilidad de los sistemas integrados. En este contexto, la implementación de medidas de seguridad proactivas y el desarrollo de estrategias robustas para anticipar y mitigar estos ataques se convierten en imperativos para asegurar un ecosistema IoT seguro y resiliente.

¿El quién y el cómo?

El surgimiento de nuevos actores no es el único valor a considerar, y es que los actores ya conocidos siguen siendo una amenaza activa dado que las Tácticas, Técnicas y Procedimientos de ataque están en constante evolución, permitiendo a los actores adaptarse al entorno cambiante del IoT.

Entre las tácticas más empleadas desde 2024, los análisis revelan que el *deepfake*, el *phishing* avanzado, el *spoofing* y las aplicaciones maliciosas son las más empleadas para engañar a los usuarios e infectar los dispositivos. Dispositivos a través de los cuales los actores de amenaza consiguen ejecutar ataques de robo de credenciales almacenadas en los dispositivos, inserción de *malware* avanzado persistente e inclusión de los dispositivos en redes *botnet*.

El futuro de las amenazas interconectadas

Sumado a lo anterior, en 2025 se espera que las repercusiones de la interconexión de dispositivos IoT con dispositivos inteligentes, algunos de los cuales comenzarán a controlar de forma activa el funcionamiento de determinadas tecnologías a nivel público gracias a la evolución natural hacia las ciudades inteligentes, genere un incremento en el número de brechas de datos, fraudes financieros y robos de identidad potenciados por tecnología *deepfake*.

Estos ataques tendrán su nicho en el ciudadano común, pero también afectarán a las empresas, principalmente debido a las políticas de uso de dispositivos personales en el trabajo y uso de datos profesionales en dispositivos externos. Por otro lado, también se extenderá a los sectores industriales, que están en pleno proceso de digitalización incluyendo tecnologías IoT para automatizar tareas, lo cual conducirá irremediablemente a ataques de denegación de servicio que podrían paralizar la producción de fábricas enteras.

¿Compromiso de datos o de vidas?

Teniendo en cuenta todo lo anterior, y añadiendo los ámbitos de crecimiento en los que los Dispositivos IoT (DIoT) han tenido mayor impacto, puede verse que los sectores con mayor número de dispositivos conectados son algunos de los más críticos, como el sector sanitario, la administración pública o el sector industrial, seguidos por el sector energético, entre los que se encuentran algunas infraestructuras críticas como centrales nucleares, hidráulicas o eléctricas. Esto puede suponer un riesgo potencial mayor del que pueda considerarse a primera vista, dado que estos sectores representan el bienestar humano y marcan la sostenibilidad de los estados de bienestar en las metrópolis. Pudiendo considerar posibilidades desastrosas como el secuestro de salas de quirófano, denegaciones de servicio a infraestructuras energéticas críticas o el bloqueo de recepción de señales en aeropuertos, dejando líneas de vuelo completas sin visibilidad de tierra.

Conclusión

Ante esta perspectiva, los profesionales de la seguridad solo podemos concluir que la interconectividad de los dispositivos es un paso lógico e inevitable hacia un futuro cada vez más globalizado.

Sin embargo, cuando estos dispositivos no están adecuadamente protegidos, y los usuarios comparten datos y otorgan permisos sin una formación y conciencia previa, la adición de conexiones entre dispositivos IoT y tecnología inteligente amplifica el panorama de amenazas de manera significativa, comprometiendo tanto la seguridad pública como la privacidad individual.

En este punto, es evidente que lo que realmente separa a los usuarios y empresas de posibles ataques es una comprensión generalizada de la seguridad de los dispositivos, conexiones y aplicaciones móviles. Por ende, la educación y formación en ciberseguridad son cruciales.

Alejandro García Muñiz
Cybersecurity Analyst

Raquel Galvez Huertas
Cybersecurity Analyst

Vulnerabilidades

Múltiples vulnerabilidades en MongoDB

Fecha: 3 de abril de 2025
CVE: CVE-2025-3085 y 2 más

CVSS: 8.1

ALTA

Descripción

El proveedor de sistemas de base de datos de Linux, MongoDB, publicó en su portal web un aviso sobre diversas vulnerabilidades el pasado 3 de abril. El aviso de seguridad incluye vulnerabilidades entre las que se reconocen dos de criticidad alta:

- CVE-2025-3085: con un CVSS de 8.1, esta vulnerabilidad afecta a servidores Linux con TLS, donde se produce un error en la verificación el estado de los certificados intermedios, posibilitando una autenticación indebida.
- CVE-2025-3083: con un CVSS de 7.5, permitiría a un atacante no autenticado provocar la caída del servicio bajo mensajes específicos.

Solución

MongoDB ha publicado una serie de actualizaciones para corregir las vulnerabilidades mencionadas, así como otras vulnerabilidades de menor criticidad, los cuales se recogen en los siguientes puntos:

- CVE-2025-3083: actualizar a la versión 5.0.316.0.207.0.16.
- CVE-2025-3084: actualizar a la versión 5.0.316.0.207.0.168.0.4.
- CVE-2025-3085: actualizar a la versión 5.0.316.0.207.0.168.0.4.

Productos afectados

Esta vulnerabilidad afecta a las siguientes versiones de MongoDB:

- Versiones 5.0X anteriores a 5.0.316.0.207.0.16.
- Versiones 5.0X anteriores a 5.0.316.0.207.0.168.0.4.

Referencias

- csirt.telconet.net
- cert.gov.py

TLP:WHITE

Vulnerabilidades

Vulnerabilidad crítica en Fortinet FortiSwitch GUI

Fecha: 8 de abril de 2025
CVE: CVE-2024-48887

CVSS: 9.3

CRÍTICA

Descripción

Se ha identificado una vulnerabilidad crítica en Fortinet FortiSwitch GUI (CVE-2024-48887), que permite, mediante un cambio de contraseña no verificada en la interfaz gráfica de FortiSwitch, que un atacante remoto no autenticado pueda cambiar las contraseñas de administrador utilizando una solicitud diseñada especialmente para este propósito.

El descubrimiento ha sido interno, realizado por Daniel Rozenboom, que forma parte del equipo de desarrollo de la interfaz de FortiSwitch. Por el momento, no se han encontrado evidencias de que esta vulnerabilidad haya sido explotada, pero se recomienda aplicar los parches de remediación lo antes posible.

Solución

Para mitigar los riesgos asociados, se recomienda realizar las siguientes acciones:

- FortiSwitch 7.6.0 (actualizar a la 7.6.1 o superior).
- FortiSwitch 7.4.0 a 7.4.4 (actualizar a la 7.4.5 o superior).
- FortiSwitch 7.2.0 a 7.2.8 (actualizar a la 7.2.9 o superior).
- FortiSwitch 7.0.0 a 7.0.10 (actualizar a la 7.0.11 o superior).
- FortiSwitch 6.4.0 a 6.4.14 (actualizar a la 6.4.15 o superior).

Además, Fortinet recomienda deshabilitar el acceso HTTP/HTTPS y restringir el acceso al sistema a dispositivos de confianza.

Productos afectados

Las versiones afectadas son las siguientes:

- FortiSwitch 7.6.0.
- FortiSwitch 7.4.0 a 7.4.4.
- FortiSwitch 7.2.0 a 7.2.8.
- FortiSwitch 7.0.0 a 7.0.10.
- FortiSwitch 6.4.0 a 6.4.14.

Referencias

- nvd.nist.gov
- fortiguard.fortinet.com
- thehackernews.com

 © Copyright NTT DATA, Inc.

Boletín de seguridad de abril de Android corrige vulnerabilidades críticas

Fecha: 7 de abril de 2025
CVE: CVE-2024-45551 y 58 más

Crítica

Descripción

El boletín de seguridad de Android de abril de 2025 aborda un total de 59 vulnerabilidades, incluidas cuatro críticas. Tres de ellas pueden ser utilizadas para la elevación de privilegios sin necesidad de interacción del usuario (CVE-2025-22429, CVE-2025-26416 y CVE-2025-22423).

También destaca la vulnerabilidad crítica CVE-2024-45551, donde un subcomponente de Qualcomm puede realizar incorrectamente la verificación del pin o contraseña.

Además, también hay dos vulnerabilidades de criticidad alta que han sido explotadas activamente, pero de forma dirigida:

- CVE-2024-53150
- CVE-2024-53197

Productos afectados

Los componentes afectados por estas vulnerabilidades son:

- Framework
- Sistema
- Kernel
- Componentes de Terceros:
  - Arm
  - Imagination Technologies
  - MediaTek
  - Qualcomm

Además, se indica que es posible que los dispositivos con Android 10 y versiones posteriores también reciban actualizaciones de seguridad.

Solución

Se han publicado varios parches de seguridad en este boletín, por lo que se recomienda a todos los usuarios de Android actualizar a la versión más reciente para solucionar las vulnerabilidades.

Referencias

- android.com
- nvd.nist.gov

 © Copyright NTT DATA, Inc.

Actualizaciones de seguridad de Microsoft de abril de 2025

Fecha: 8 de abril de 2025
CVE: CVE-2025-29824 y 124 más.

Crítica

Descripción

Microsoft ha publicado su parche mensual de corrección de vulnerabilidades del mes de abril, donde se corrigen un total de 125 fallas de seguridad, de las cuales 11 son de severidad crítica.

Entre estas vulnerabilidades, existe una vulnerabilidad (CVE-2025-29824) *zero-day* con una puntuación de 7.8. Esta vulnerabilidad está enfocada a la escalada de privilegios, donde una explotación exitosa permitiría a un usuario estándar obtener privilegios elevados (administrador), afectando al sistema de archivos de registro común (CLFS).

Esta vulnerabilidad ha sido corregida para el sistema operativo Windows 11, mientras que para Windows 10 aún no se ha solventado.

Solución

Microsoft recomienda encarecidamente a sus clientes actualizar sus sistemas operativos a la última versión disponible, actualmente son:

- Actualización acumulativa para Windows 11 Versión 24H2 (versión KB5055523).
- Actualización acumulativa para Windows 11 Versión 24H2 (versión KB5055528).

Productos afectados

Los productos/versiones afectadas por estas vulnerabilidades son:

- Versiones anteriores a la actualización de seguridad de abril. La lista completa de productos afectados está disponible en el portal de Microsoft.

Referencias

- support.microsoft.com
- thehackernews.com
- incibe.es

 © Copyright NTT DATA, Inc.

Eventos

RSA Conference
28 abril – 1 de mayo

La RSA Conference 2025 es uno de los eventos más destacados en el ámbito de la ciberseguridad. Este encuentro reúne a expertos, innovadores y líderes de la industria para explorar las últimas tendencias, tecnologías y estrategias frente a los desafíos de seguridad actuales. Además de conferencias y talleres interactivos, los asistentes tendrán la oportunidad de establecer conexiones valiosas, descubrir soluciones innovadoras y participar en actividades como el concurso de innovación "Innovation Sandbox".

Enlace

Cybersecurity & Data Innovation Summit
29 de abril

La 6ª edición del Cybersecurity & Data Innovation Summit 2025 se celebrará el 29 de abril en Madrid, posicionándose como un evento clave en el ámbito de la ciberseguridad. Este encuentro ofrece oportunidades exclusivas de *networking* con líderes del sector y debates sobre temas como las directivas NIS2, estrategias DORA, innovaciones en IA aplicada a la ciberseguridad, combate contra el *ransomware* y más.

Enlace

Cloud Summit 2025
26 – 28 de mayo

El European AI and Cloud Summit es un evento destacado de inteligencia artificial y tecnologías en la nube que contará con la asistencia de 3.000 participantes. Reunirá a líderes, innovadores y expertos para explorar los últimos avances en áreas como *generative* AI, OpenAI, Microsoft Azure y aplicaciones de inteligencia artificial en diversas industrias. Entre los temas clave estarán el escalado de startups de IA y herramientas avanzadas de visualización de datos, con empresas como SquaredUp presentando soluciones innovadoras en el evento, ubicado en el Booth 36.

Enlace

Recursos

➢ Burp AI

Burp AI es una herramienta integrada en Burp Suite Professional que utiliza inteligencia artificial para mejorar la seguridad web. Ofrece análisis automatizados para validar vulnerabilidades, reduce falsos positivos y simplifica configuraciones como las de inicio de sesión. Agrega explicaciones de forma clara sobre tecnologías web y permite integrar funciones avanzadas mediante extensiones de IA, garantizando siempre la privacidad de los datos.

Enlace

➢ OpenNHP

Herramienta de código abierto diseñada para implementar seguridad de confianza cero en infraestructuras, aplicaciones y datos. Utiliza protocolos avanzados de criptografía para ocultar detalles de la infraestructura de red, como puertos y direcciones IP, protegiendo así los recursos de accesos no autorizados. Además, asegura la privacidad de los datos mediante algoritmos de cifrado, reduciendo la superficie de ataque y fortaleciendo la defensa contra amenazas cibernéticas

Enlace

➢ Dalfox

Herramienta de código abierto diseñada para detectar automáticamente vulnerabilidades de XSS (Cross-Site Scripting). Ofrece un motor de pruebas avanzado que permite analizar parámetros, realizar escaneos rápidos o análisis detallados, y verificar vulnerabilidades. Incluye características como modos de escaneo flexibles, análisis de parámetros reflejados, almacenados y basados en DOM, y opciones de personalización con *payloads* y listas de palabras remotas.

Enlace

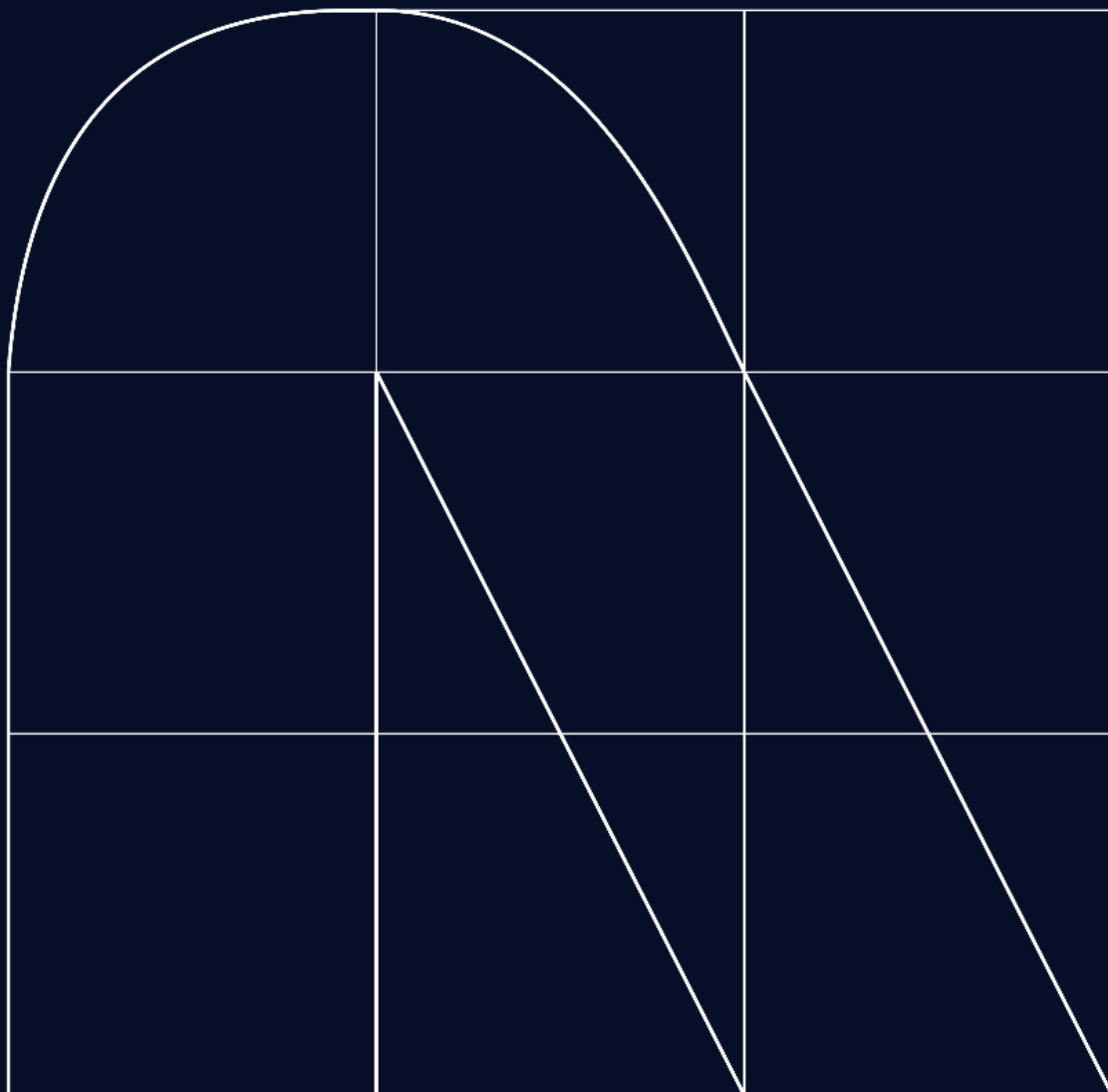
➢ OpenCTI

Plataforma de código abierto diseñada para gestionar inteligencia de amenazas cibernéticas. Permite estructurar, almacenar, organizar y visualizar información técnica (y no técnica) sobre amenazas cibernéticas utilizando el estándar STIX2. Incluye una interfaz moderna basada en GraphQL y puede integrarse con herramientas como MISP, TheHive y MITRE ATT&CK. Facilita la exportación e importación de datos en varios formatos, ayudando a los analistas a extraer conocimiento significativo de los datos brutos.

Enlace

Suscríbete a RADAR
up.nttdata.com/suscribetearadar

 © Copyright NTT DATA, Inc.



Powered by the cybersecurity NTT DATA team

es.nttdata.com