PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
TRIBUNAS

ciberseguridadTIC
seguridad en informática y comunicaciones

Tai editorial

Año I Nº 5 Junio 2023

IA Generativa y sus ventajas en ciberseguridad

Joseph Carson, Delinea:
"La identidad es el área donde todavía tienes algún tipo de control"

John Shier, Sophos:
"No necesitas hacerlo solo. Hay un MDR detrás de ti"

José Manuel Canelada, Infoblox:
"Cada vez es más necesario utilizar elementos catalizadores como el DNS para seguridad"

Javier Abad, Nozomi:
"Ayudamos al cliente a entender qué riesgos tiene su entorno de OT"

IR A PÁGINA SIGUIENTE

ciberseguridadTIC
Tai editorial

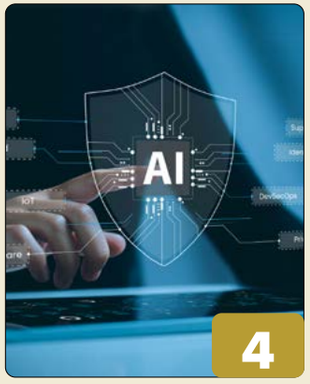
IA, ¿más artificial que inteligente?

Desde finales del año pasado, cuando OpenAI revolucionó al mercado con su ChatGPT, no hay semana, incluso día, que el tema de la Inteligencia Artificial en todas sus formas no salga a colación. Tanto da que hablemos de machine learning, de IA generativa, o de modelos de lenguaje. Ninguna de estas tecnologías es nueva, pero está más de moda que nunca. No cabe duda de que la Inteligencia Artificial tiene, y tendrá, un impacto importante en la vida de todas las empresas, y de todas las personas. Aún no hemos llegado al momento Skynet, la temida inteligencia artificial que lidera al ejército de las máquinas contra los hombres en la saga de películas Terminator, pero se están consiguiendo importantes avances en numerosos campos, incluido el de la ciberseguridad.

Hay personas preocupadas por el potencial de la IA para hacerse cargo de los trabajos que antes realizaban los humanos. También estamos lejos de eso. La frase que da título al editorial no es nueva, y tiene mucho de verdad. Estamos lejos del momento en que una IA realmente autónoma sea capaz de desplazar al hombre. Es indudable que los ordenadores tienen mejor memoria, que pueden recopilar información rápidamente de numerosas fuentes digitales, trabajar continuamente sin necesidad de dormir, que no cometen errores matemáticos y son mejores para realizar múltiples tareas y pensar varios pasos por delante que los humanos. Pero les falta imaginación, e intuición.

Me quedo con una historia escuchada en uno de tantos eventos o entrevistas. Frente al avance imparable de la IA un médico cuestionaba que fuera a ser sustituido por una inteligencia artificial; "no será sustituido por una IA, pero sí por otro médico capaz de utilizarla", fue la respuesta. Ahí está el camino, en ir de la mano. CST

SUMARIO



4

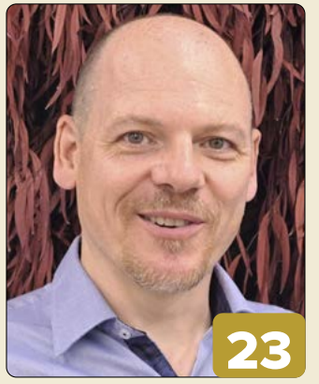
IA Generativa y sus ventajas en ciberseguridad

11

Netskope SASE Summit


17

Delinea: "La identidad es el área donde todavía tienes algún tipo de control o visibilidad"


23

Sophos: "No necesitas hacerlo solo. Hay un MDR detrás de ti"


30

Infoblox: "Cada vez es más necesario utilizar elementos catalizadores como el DNS para proporcionar seguridad"


35

Nozomi: "Ayudamos al cliente a entender qué riesgos tiene su entorno de OT"

39

Tribunas: Esta sección recoge opiniones de personas con experiencia y reconocimiento en el sector y donde se abordan las últimas tendencias o tecnologías que impactan en el mercado de ciberseguridad "

Directora:
Rosalía Arroyo
rosalia@taieditorial.es

Publicidad:
David Rico
david@taieditorial.es

Producción:
Marta Arias
marta@taieditorial.es

Edita:
T.A.I. Editorial, S.A.
(Técnicos y Asesores Informáticos Editorial, S.A.)
www.taieditorial.es
Avda. Fuencarral, 68
28108 Alcobendas (Madrid)
Tel. 91 661 61 02
e-mail: correo@taieditorial.es

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
TRIBUNAS

IA Generativa y sus ventajas en ciberseguridad

La inteligencia artificial, que lleva años utilizándose en los mercados de TO y ciberseguridad, y se ha visto revolucionada por la expansión de la inteligencia artificial generativa y los modelos de lenguaje grande, o LLM. En las últimas semanas se han ido sucediendo las noticias en torno a nuevos productos que prometen mejorar la detección de amenazas gracias a su uso mientras Europa está a punto de firmar la Ley de la Inteligencia Artificial.

ciberseguridadTIC

Tai editorial

EN PORTADA

2023 pasará a la historia como el año de la IA Generativa. No porque no existiera antes, sino porque pocas veces el mercado se pone tan de acuerdo para hablar, analizar, desarrollar e invertir en lo mismo. Donde quiera que miremos y a cualquiera que preguntemos, queda claro que la IA Generativa está a punto de cambiar la industria, incluida la de ciberseguridad. Ya sea

Ya sea el Security Copilot de Microsoft, el LLM de Google centrado den ciberseguridad, el asistente de IA de Recorded Future, Charlotte AI de Crowdtrike, o Purple AI de Sentinel One, son muchas las empresas que aceleran para lanzar sus propuestas de inteligencia artificial para ciberseguridad, mientras la IA Act europea va camino de convertirse en Ley después de que el Parlamento Europeo haya aprobado por mayoría el último borrador de la legislación el 14 de junio de 2023.

En general, la industria observa el potencial defensivo de la IA generativa con una mezcla de escepticismo y entusiasmo. Un escepticismo que se basa en el recelo de que la publicidad exagerada está tergiversando lo que la tecnología realmente puede hacer, y la sensación de que la IA puede incluso introducir un nuevo conjunto de vulnerabilidades de seguridad poco conocidas.

Con la IA generativa, los profesionales de la seguridad ahora pueden crear modelos predictivos para identificar nuevas amenazas incluso antes de que surjan.

Respecto al entusiasmo, viene dado por las posibilidades que generan las técnicas de procesamiento del lenguaje natural, que pueden permitir que los humanos y las máquinas interactúen de nuevas formas con beneficios im-

EN PORTADA

predecibles. La integración de la IA y la seguridad ha estado evolucionando durante años, al menos conceptualmente. Con la IA generativa, los profesionales de la seguridad ahora pueden crear modelos predictivos para identificar nuevas amenazas incluso antes de que surjan.

Pero empecemos por el principio. ¿Qué es la IA Generativa? Es un tipo de inteligencia artificial que puede producir varios tipos de contenido, incluidos texto, imágenes o audio en función de patrones y datos con los que se ha entrenado. También puede transformar la forma en que detectamos y respondemos a las amenazas, pero solo si entendemos cómo aprovechar la IA correctamente.

Desde eWeek proponen varios casos de uso parala IA Generativa. Menciona la publicación la capacidad de crear correos electrónicos de phishing realistas u otros ataques, correos que se pueden utilizar en las campañas de formación y concienciación de los empleados con el fin de prevenir ataques y mejorar la postura general de seguridad.

> El modelo de lenguaje ELIZA debutó en 1966 en el MIT y es uno de los primeros ejemplos de un modelo de lenguaje de IA

Además de simular ataques, la AI Generativa puede utilizarse para simular entornos que imiten escenarios del mundo real, lo que permite probar y evaluar controles y respuestas de seguridad. Esto puede ayudar a identificar debilidades y mejorar la preparación general de la seguridad.

Otra aplicación valiosa de la IA generativa en ciberseguridad es la inteligencia de amenazas. Al analizar grandes volúmenes de datos, la IA generativa puede identificar patrones e indicadores de compromiso que se pueden usar para detectar y responder a las amenazas en tiempo real.

Por cierto, que los primeros modelos de lenguaje de IA datan de hace bastantes años. El modelo de lenguaje ELIZA debutó en 1966 en el

EN PORTADA

MIT y es uno de los primeros ejemplos de un modelo de lenguaje de IA. Todos los modelos de lenguaje se entrenan primero en un conjunto de datos y luego utilizan varias técnicas para inferir relaciones y luego generar nuevo contenido basado en los datos entrenados. Los modelos de lenguaje se usan comúnmente en aplicaciones de procesamiento de lenguaje natural (NLP) donde un usuario ingresa una consulta en lenguaje natural para generar un resultado. Un LLM es la evolución del concepto de modelo de lenguaje en IA que amplía drásticamente los datos utilizados para el entrenamiento y la inferencia.

Destacan los expertos que LLM tiene ventajas sobre la IA generativa al requerir menos poder de cómputo y capacidad de memoria

IA Generativa y LLM

Si bien ambos tipos de IA generan resultados, la IA generativa y el LLM (Modelo de lenguaje) son dos tecnologías relacionadas que se pueden utilizar para automatizar el servicio al cliente. A diferencia de otras formas de aprendizaje automático, que se basan en conjuntos de datos y algoritmos preexistentes para hacer predicciones o tomar decisiones, la IA generativa crea contenido nuevo desde cero, mientras que LLM se refiere a un tipo de modelo de aprendizaje automático que puede comprender y generar un lenguaje similar al humano.

Si bien no existe una cifra universalmente aceptada sobre qué tan grande debe ser el conjunto de datos para la capacitación, un LLM generalmente tiene al menos mil millones o más parámetros. Los parámetros son un término de aprendizaje automático para las variables presentes en el modelo en el que se entrenó que se pueden usar para inferir contenido nuevo.

Destacan los expertos que LLM tiene ventajas sobre la IA generativa al requerir menos poder de cómputo y capacidad de memoria y, al mismo tiempo, lograr altos niveles de precisión en tareas como el reconocimiento de imágenes y el procesamiento del lenguaje natural.

El pasado mes de marzo, Microsoft anunció su servicio Security Copilot basado en los modelos de lenguaje grande (LLM), que impulsan aplicaciones como ChatGPT, y en la información de la inteligencia global de amenazas de la compañía, que recibe más de 65.000 millones de señales diarias.

Pero Microsoft no es el único que está aprovechando la IA generativa y los LLM en ciberseguridad. En abril SentinelOnel presentaba Purple AI, una IA generativa dedicada a la búsqueda, análisis y respuesta de amenazas que utiliza una variedad de modelos, tanto de código abierto como patentados, con el objetivo de aumentar la eficiencia de la organización al equipar a los analistas de seguridad con un motor de IA que puede ayudar a identificar, analizar y mitigar las amenazas mediante mensajes conversacionales y diálogos interactivos.

EN PORTADA

Purple AI permite que los cazadores de amenazas hagan preguntas sobre amenazas específicas y conocidas y obtengan respuestas rápidas sin necesidad de crear consultas manuales sobre indicadores de compromiso.

Nikesh Arora, CEO de Palo Alto, anunciaba durante los últimos resultados trimestrales de la compañía que está desarrollando su propio LLM, que se lanzará este año. Señaló que la tecnología mejorará la detección y la prevención, permitirá una mayor facilidad de uso para los clientes y ayudará a proporcionar más eficiencia.

También en abril anunciaba Google su Cloud Security AI Workbench, una primera plataforma extensible en la industria impulsada por un LLM especializado en seguridad, Sec-PaLM. Este nuevo modelo de seguridad está ajustado para casos de uso de seguridad, incorporando nuestra insuperable inteligencia de seguridad, como la visibilidad de Google en el panorama de amenazas y la inteligencia de primera línea de Mandiant sobre vulnerabilidades, malware, indicadores de amenazas y perfiles de actores de amenazas de comportamiento.

> En general, la industria observa el potencial defensivo de la IA generativa con una mezcla de escepticismo y entusiasmo

Veracode Fix es una IA especializada entrenada por aprendizaje automático profundo desarrollada específicamente para la reparación de código inseguro y reducir el trabajo y el tiempo necesarios para remediar fallos y vulnerabilidades.

Más recientemente, Cisco ha anunciado la incorporación de IA Generativa en sus soluciones de Seguridad y Colaboración. Ha sido durante el Cisco Live que se celebró a mediados de junio cuando la compañía ha explicado cómo está aprovechando los grandes modelos de lenguaje (LLM) integrados en sus porfolios de

EN PORTADA

Seguridad y Colaboración para ayudar a las organizaciones a impulsar la productividad de sus trabajadores.

Es probable que este sea solo el comienzo para las aplicaciones de seguridad basadas en LLM, que, como todo, no está exento de problemas. Aseguran varios expertos que los LLM son susceptibles a las alucinaciones, que es cuando los modelos generan contenido falso o engañoso, aunque parezcan convincentes.

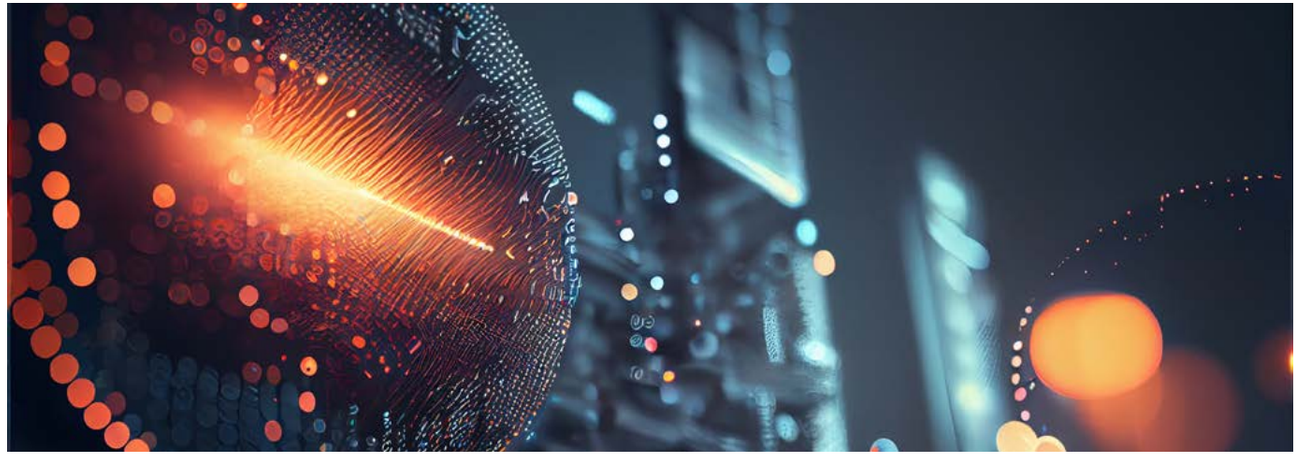
Se mencionan también algunos desafíos técnicos que pueden limitar el uso de LLM, como es la necesidad de una conectividad de red robusta, que podría representar un desafío para los dispositivos remotos o móviles; o la necesidad de un mantenimiento continuo para garantizar un rendimiento y una protección óptimos.

Ley de Inteligencia Artificial

Presentada en abril de 2021, la Ley de IA tiene como objetivo regular estrictamente los servicios de IA y reducir el riesgo que plantea. El primer borrador, que incluía medidas como agregar salvaguardas a la explotación de datos biométricos, sistemas de vigilancia masiva y algoritmos policiales, anticipó el aumento en la adopción de herramientas de IA generativa que comenzó a fines de 2022.

La ley asigna tres categorías de riesgo a las aplicaciones de Inteligencia artificial. En primer lugar, se prohíben las aplicaciones y los sistemas que crean un riesgo inaceptable, como la calificación social administrada por el gobierno del tipo que se usa en China. En segundo lugar, las aplicaciones de alto riesgo, como una herramienta de escaneo de CV que clasifica a los solicitantes de empleo, están sujetas a requisitos legales específicos. Por último, las aplicaciones que no están explícitamente prohibidas o catalogadas como de alto riesgo quedan en gran parte sin regular.

EN PORTADA



Además de simular ataques, la AI Generativa puede utilizarse para simular entornos que imiten escenarios del mundo real

Asegurando que la IA afecta muchas partes de tu vida, se busca que la ley de IA tenga un impacto similar al que tuvo el Reglamento General de Protección de Datos (GDPR) de la UE de 2018. De forma que la Ley de IA de la UE podría convertirse en un estándar global. El último borrador de la Ley, presentado en mayo de 2023, introdujo nuevas medidas para incluir un enfoque escalonado para los modelos de IA, desde prácticas de IA de "riesgo bajo y mínimo" hasta prácticas de IA de "riesgo limitado", "alto riesgo" y "riesgo inaceptable".

Las herramientas de IA de "riesgo bajo y mínimo" no estarán reguladas, mientras que las de "riesgo limitado" deberán ser transparentes. Sin embargo, las prácticas de IA de "alto riesgo" estarán estrictamente reguladas. La UE requerirá una base de datos de sistemas de inteligencia artificial de uso general y de alto riesgo para explicar dónde, cuándo y cómo se implementarán en la UE.

ENLACES DESTACADOS

Palo Alto lanzará su propio ChatGPT el próximo año

ChatGPT es un LLM

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
TRIBUNAS

Netskope SASE Summit

Netskope celebraba en mayo su segundo SASE Summit en España con récord de asistentes, más de 250 personas, y la presentación de Miguel Ángel Martos, director general de la compañía para la región de Iberia. Recordaba el directivo que Netskope ha despertado el interés de todo el mundo sin haber salido a bolsa y que el cuadrante SSE de Gartner posiciona a la compañía como "líder entre los líderes".

Hablaba también Martos de un año "tremendamente exitoso" en el que se han conseguido cien clientes nuevos, se ha multiplicado por cuatro la facturación, se cuenta con un equipo de más de 50 personas y se sigue trabajando con el canal. Repetía el directivo una frase que se está convirtiendo en lema: "Es el momento de Netskope", y lo es porque es el momento de una transformación digital que implica transformar la red y transformar la seguridad. Para ello nada mejor que una arquitectura SASE en la que la compañía es un referente que además acaba de presentar Borderless SD-WAN, una propuesta en la que confluyen la seguridad de confianza cero con la optimización de la red y que amplía una propuesta de seguridad y red

ACTUALIDAD

como servicio “para acelerar tu transformación digital”, aseguraba Miguel Ángel Martos.

Bob Gilberts, VP de estrategia y evangelista de Netskope, siguió a Martos para hablar de las capacidades críticas que hacen diferente a la compañía. Mencionaba existencia de una plataforma unificada y la mayor visibilidad, contexto y control que ofrece; una propuesta de protección de datos y DLP, asumidos como “el ADN de Netskope; su mayor velocidad y resiliencia gracias a Netskope NewEdge, una de las grandes inversiones de la compañía que les permite estar “entre diez y 15 milisegundos de la mayoría de la población mundial”. Estos cuatro elementos diferenciadores permiten a Netskope poder reducir los riesgos de seguridad un 85 %, incrementar la agilidad del negocio un 19 % y reducir los costes de ancho de banda un 51 %.

Planteó el directivo los principales cinco casos de uso de la propuesta SASE de la compañía.

1. Entender el uso y riesgo del SaaS

Que una organización tenga una media de

Miguel Ángel Martos,
Country Manager de **Netskope**

> “Netskope ha despertado el interés de todo el mundo sin haber salido a Bolsa”

2.400 aplicaciones en la nube representa un gran desafío cuando se trata de amenazas que entran en la organización y de datos que pueden exfiltrarse fuera, comentaba Bob Gilbert.

Por eso “obtener una visión de lo que está sucediendo a través del riesgo y lo que significa para la organización es una gran fortaleza de Netskope”. La compañía cuenta con una base de datos de más de 63.000 aplicaciones a las que se asigna un grado de confianza de cero a 100. Se trata de una base de datos viva que modifica la puntuación de una aplicación en función de si, por ejemplo, ha sufrido una brecha de seguridad. Permite la compañía ver la cantidad de aplicaciones en la nube que se han utilizado en los últimos 30 días.

2. Coaching de usuario activo

El segundo caso de uso tiene que ver con la actuación de los usuarios, que siguen siendo el eslabón más débil. El *coaching* de usuario activo de Netskope es capaz de identificar actividades y comportamientos de riesgo en tiempo real; “interrumpe las actividades y lleva al usuario a través de un flujo de trabajo de entrenamiento avanzado. Y lo que eso le permite hacer es entrenar al usuario, moldear el comporta-

ACTUALIDAD

miento, crear buenos ciudadanos digitales", explicaba el directivo.

Se trata de una herramienta que no se limita a bloquear. Por diferentes motivos, como tener que hacer un estudio, puede una empresa tener que realizar actividades que podrían considerarse sospechosas, "¿por qué no tener un flujo de trabajo diferente para los usuarios que necesitan acceso?". Es una forma diferente de pensar en los controles de seguridad porque está haciendo que un usuario sea parte de una solución en lugar de solo parte de un problema, aseguraba el VP de Netskope.

3. Control contextual Zero Trust

La Confianza Zero no trata solo del dispositivo y la identidad. Explicaba el directivo que cuando se observa el comportamiento del usuario no sólo hay que mirar cómo está realizando determinada actividad porque en base a su pasado, a su comportamiento histórico", podemos entenderle y "es posible que sepa que el empleado se marcha antes que Recursos Humanos".

ACTUALIDAD

Hablaba Bob Gilberts de “una forma diferente de pensar en los controles de seguridad que no verá con ningún otro proveedor de seguridad porque es una política inteligente que pone en contexto”. Mencionaba el directivo dos formas de tratar o identificar a los usuarios de riesgo. “Una es utilizar nuestro análisis de comportamiento del usuario para identificar el comportamiento pasado”; otra forma es crear un grupo llamado ‘Empleados que salen” y sincronizarlo con el proveedor de identidades y acceso y con Netskope para impedir que acceda a información sensible. “Una vez más, una política inteligente que va más allá de una pasarela web segura o un cortafuegos”, comentaba el directivo.

4. Ver y controlar el movimiento de los datos

Evitar que la información privilegiada salga de la empresa requiere de una tecnología “que vaya más allá de mirar tipos específicos de datos cargados en destinos específicos.

Debe poder cubrir todo, desde la nube hasta el punto final y utilizar técnicas avanzadas”, comentaba Bob Gilberts durante su ponencia, para explicar las diferentes maneras que tiene la compañía de detectar movimientos sospechosos de información.

Bob Gilberts,
VP de estrategia y evangelista de **Netskope**

> “Evitar que la información privilegiada salga de la empresa requiere de una tecnología que vaya más allá de mirar tipos específicos de datos cargados en destinos específicos”

5. Jubilación de la VPN, o ZTNA Next

El quinto caso de uso propuesto por Bob Gilberts tiene que ver con la VPN, una tecnología con décadas de historia, cuyo uso se multiplicó en tiempos de pandemia al mismo ritmo que demostraba su obsolescencia.

Implementadas en todas las organizaciones, aseguraba el directivo que son vulnerable a los ataques una vez que otorga acceso a la red. “Aquí es donde Netskope tiene la capacidad de retirar efectivamente la VPN de las organizaciones. Y tenemos un enfoque único”, decía Bob Gilberts haciendo referencia a ZTNA Next, la evolución de la propuesta de ZTNA de la compañía y donde convergen Netskope Private Access (NPA) ZTNA con Netskope Endpoint SD-WAN “para una seguridad y conectividad óptimas cuando se actualiza desde las VPNs. CST

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
TRIBUNAS

Netskope Borderless SD-WAN

La compañía aprovechaba también su SASE Summit para destacar las ventajas de Borderless SD-WAN, una propuesta anunciada el pasado mes de febrero que ofrece una arquitectura en la que convergen los principios de confianza cero y el rendimiento garantizado de las aplicaciones para proporcionar una conectividad segura y de alto rendimiento sin precedentes para cada ubicación, nube, usuario remoto y dispositivo IoT...

El encargado de hablar de ella, Parag Thakore, vicepresidente senior y máximo responsable de esta área, publicaba hace unos meses un contenido en el que aseguraba que proteger y optimizar la conectividad de usuarios, ubicaciones y dispositivos hacia los recursos corporativos y de la nube no tiene por qué ser difícil. “Todo lo que se necesita son la estrategia y la plataforma adecuadas”. La arquitectura Borderless SD-WAN de Netskope ofrece una seguridad de confianza cero y un rendimiento de las aplicaciones coherente.

Parag Thakore,
vicepresidente senior de **Netskope**

ENLACES DESTACADOS

Netskope Endpoint SD-WAN permite sustituir las VPN sin necesidad de hardware

Estrategia de gasto en una economía restrictiva

utimaco®

SOLUCIONES de CIBERSEGURIDAD

Con las más prestigiosas **certificaciones internacionales de seguridad**

EMEA
UTIMACO IS GmbH
Germanusstrasse 4
52080 Aquisgrán,
Alemania
+49 241 1696 200
hsm@utimaco.com

América
UTIMACO Inc.
900 E Hamilton Ave., Suite 400
Campbell, CA 95008,
EE.UU.
+1 844 UTIMACO
hsm@utimaco.com

APAC
UTIMACO IS Pte Limited
6 Temasek Boulevard, #23-04
Suntec Tower Four
Singapore 038986
+65 6993 8918
hsm@utimaco.com

UTIMACO España
C/ Infanta Mercedes, 90,
4th floor
28020, Madrid
+34 91 449 03 30
info@realsec.com

UTIMACO México
Av. Jaime Balmes 8, M6-A
Colonia Los Morales, Polanco
11510 Miguel Hidalgo, México City
+52 (55) 44 35 00 45
infomexico@realsec.com

BANCA | FINTECH | INFRAESTRUCTURAS CRÍTICAS | AUTOMOCIÓN | INDUSTRIA 4.0 | RETAIL | TELCO

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

“La identidad es el área donde todavía tienes algún tipo de control o visibilidad”

Dice Joseph Carson, Chief Security Scientist y Advisory CISO de Delinea, que cuando se trabaja en diferentes entornos con diferentes tecnologías y diferentes pilas, se pierde el control de quién accede a qué, cuándo y cómo; que la visión de Delinea es hacer que PAM (Privileged Access Management) sea lo más transparente y automatizado posible y que *Passwordless* no es la desaparición de la contraseña, sino una nueva experiencia en la que la contraseña pasa a un segundo plano.

Joseph Carson, *Chief Security Scientist y Advisory* CISO de **Delinea**

La marca Delinea solo tiene un año, pero acumula la experiencia de dos grandes compañías del mercado de gestión el acceso privilegiado, Thycotic y Centrify, fusionadas al amparo de TPG Capital. Nos lo cuenta Joseph Carson, Chief Security Scientist y Advisory CISO de Delinea durante un reciente viaje a Madrid.

Explica que las empresas tienen usuarios remotos, proveedores externos o administradores que en algún momento necesitan realizar actualizaciones o cambios en la configuración de las instalaciones, y que lo que hace Delinea es “proporcionar una forma segura de utilizar ese acceso”. Añade que lo que hace la compañía es garantizar que las empresas midan, monitoricen y aseguren ese acceso, y que Delinea “es la empresa que llevó el acceso privilegiado al modelo de entrega en la nube”; también es la empresa que ha democratizado la gestión del acceso privilegiado, levándolo a organizaciones de todos los tamaños.

Como Chief Security Scientist y Advisory CISO de Delinea, la responsabilidad de Joseph Carson dentro de la compañía es “comprender cuáles son los métodos de ataque existentes y cómo tienen éxito los ciberdelincuentes”. Después de hacer esa investigación, “analizo cuál

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

es la mejor manera de mitigar o reducir el riesgo de esos ataques", y todo este conocimiento se convierte en material educativo, desde documentos técnicos a seminarios o la participación en eventos.

Preguntado sobre el elemento diferenciador de Delinea, dice que es llevar la tecnología a organizaciones de todos los tamaños "y asegurarnos de cómo encajamos en esas organizaciones sin obligarlas a tener que cambiar sus procesos comerciales para trabajar con nuestras soluciones", lo que significa "un retorno del valor mucho más rápido". Añade además que, a diferencia de otros proveedores, con Delinea los clientes "pueden obtener implementaciones mucho más completas".

Impulsores

En opinión de Joseph Carson lo que definitivamente está impulsando el mercado de seguridad de la identidad en su sentido más amplio es la nube. El trabajo y los servicios son remotos gracias a la nube, a lo que se suma que el

> "Delinea trajo el acceso privilegiado al modelo de entrega en la nube"

BYOD diluye el control sobre los dispositivos. En este entorno, "la identidad es el área donde todavía tienes algún tipo de control o visibilidad. Por eso la gestión de acceso a la identidad y el gobierno de la identidad se han acelerado", comenta el directivo añadiendo que ve dos categorías separadas: autenticación y autorización.

El primero, la autenticación, corre a cargo de proveedores de servicios de identidad "y son los responsables de cosas como el aprovisionamiento, los derechos, etc.". Delinea se posi-

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

> "Somos la parte de la solución real que determina a qué debe tener acceso, cuánto tiempo debe tener acceso y qué privilegios tiene cuando tiene ese acceso"

ciona en el lado de la autorización; "somos la parte de la solución real que determina a qué debe tener acceso, cuánto tiempo debe tener acceso y qué privilegios tiene cuando tiene ese acceso". Añade el directivo que entre la autenticación de la identidad y la autorización normalmente hay una parte de verificación, que no es otra cosa que la autenticación multifactor. "Tenemos la capacidad de comprender qué nivel de confianza deberíamos brindar una vez que se ha establecido el proceso de autenticación y luego brindamos controles de seguridad más consistentes en las organizaciones. Es algo beneficioso, especialmente si tiene un entorno de nube híbrida", porque cuando se trabaja en diferentes entornos, con diferentes tecnologías y diferentes pilas, "se pierde el control de quién accede a qué, cuándo y cómo". Añade Joseph Carson que para mantener una visibilidad consistente el acceso privilegiado y la autorización de la autenticación tienen que ponerse en primera línea.

ITDR - Identity Detection and Response

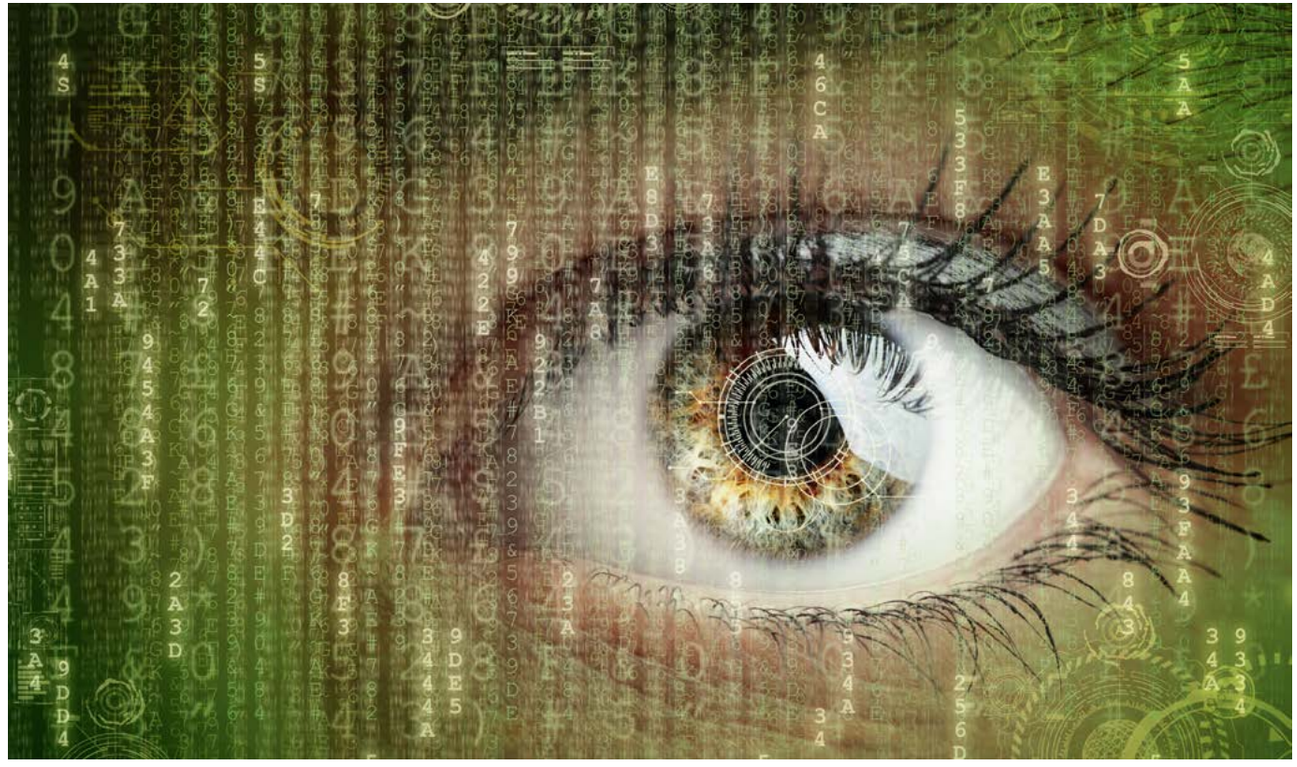
Identity Threat Detection and Response, o ITDR, es una nueva categoría de productos creada por Gartner para describir las soluciones que protegen los sistemas de identidad como Active Directory (AD) y Azure AD. Tras señalar que los atacantes utilizan principalmente el uso indebido de credenciales para obtener acceso privilegiado a los sistemas de información de una organización y manipular sus sistemas de administración de acceso e identidad (IAM), se propone que las soluciones de ITDR se centren en la infraestructura de identidad en sí, en lugar de los usuarios administrados por esa infraestructura.

Sobre esta nueva categoría de producto dice Joseph Carson que la visión de Delinea es hacer que PAM (Privileged Access Management) "sea lo más transparente y automatizado posible". Utiliza el directivo la analogía de una orquesta para explicar que todos los instrumentos deben trabajar juntos; "necesitas saber que todos están en sintonía. La gestión del acceso privilegiado es la parte que asegura que las API tengan acceso para realizar la comunicación que necesitan, y que las personas tengan acceso a lo que requieren para tomar decisiones vitales para el negocio. Somos un área clave en toda esa interoperabilidad y esa es realmente nuestra estrategia: asegurarnos de que sea lo más fluido posible, que funcione en segundo plano y, en muchos casos, eliminando el sufrimiento de las contraseñas de muchas personas".

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

ENTREVISTAS

> "Cuando se trabaja en diferentes entornos, con diferentes tecnologías y diferentes pilas, se pierde el control de quién accede a qué, cuándo y cómo"



Passwordless, Zero Trust e IA

Hablando de las contraseñas... "siguen siendo un gran problema para muchas organizaciones", dice el CISO de Delinea explicando que la compañía ayuda a los empleados a no perder el tiempo cambiando contraseñas y a obtener acceso a los sistemas que necesitan a tiempo con una mayor eficiencia. "Nuestros clientes exigen una integración más unificada", asegura, y eso supone no tener que implementar, no tener que esperar. "Los clientes solo quieren que la solución funcione, y quieren que funcione sin problemas y quieren que esté unificada porque las organizaciones tienen que ser eficientes hoy, y esa unificación es la única forma en que pueden ser eficientes", asegura.

En opinión de Joseph Carson, "*passwordless* no es la desaparición de la contraseña, sino una nueva experiencia en la que la contraseña pasa a un segundo plano porque todavía hay una llave, un secreto que se intercambia. A veces, esa clave puede ser una clave persistente, otras una clave temporal, pero aun así hay un intercambio".

Sobre *Zero Trust*, o Confianza Cero, dice Carson que son muchos los que piensan que es un producto, pero en realidad es "una mentalidad sobre cómo desea operar su negocio de manera segura. Es una capacidad operativa y no una capacidad tecnológica". Planificar una estrate-

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

gia de *Zero Trust* supone "priorizar también una estrategia de *Zero Friction*, lo que significa que cuando piensas en la seguridad, tiene que ser mejor que cualquier cosa que hayas usado antes. Tiene que ser siempre mejor que la experiencia anterior".

La IA "puede convertirse en algo increíble en el futuro, pero estamos al principio", más artificial que inteligente. "Me gusta pensar en ello como una inteligencia más aumentada que me ayuda a tomar decisiones más rápidas", dice el directivo, añadiendo que los dos términos que mejor la representan son: reducción matemática, que consiste en tomar gran cantidad de información y reducirla lo más rápido posible, y texto predictivo. "La pieza de reducción matemática y luego la pieza predictiva buscan posibles sugerencias sobre cuáles serán mis próximas acciones. Pero no es mi máquina cobrando vida y no tiene un cerebro por sí mismo. Eso no es lo que va a pasar, al menos no en un futuro próximo".

> "La visión de Delinea es hacer que PAM (Privileged Access Management) sea lo más transparente y automatizado posible"

Apuesta más por el aprendizaje automático y aprendizaje profundo para comprender los datos y darles sentido mucho más rápido. Lo que marca la diferencia, asegura es la comprensión del lenguaje natural y el procesamiento del lenguaje natural, que hace que sea importante formular la pregunta de una manera que proporcione la mejor respuesta posible; "así que las preguntas son la parte más crítica cuando te metes en esas áreas".

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

ENTREVISTAS

Ciberseguridad como servicio

Hablamos también con Joseph Carson sobre el informe Cybersecurity versus the Business, una encuesta global que muestra una clara desconexión entre la estrategia de ciberseguridad y de negocio en las empresas y que recoge que solo el 40 % de las organizaciones se sienten preparadas para enfrentar los ciberataques. ¿A pesar de que las inversiones en ciberseguridad crecen? "Sí. Pero hay que tener en cuenta que la mayoría de las inversiones se centran en el mantenimiento y crecen con el negocio", dice el directivo añadiendo que para hacer algo realmente estratégico e innovador ", tienes que dejar de hacer lo que has hecho en el pasado y hacerlo de una manera diferente"

> "*Passwordless* no es la desaparición de la contraseña, sino una nueva experiencia en la que la contraseña pasa a un segundo plano"

Dice también que las organizaciones están luchando para cambiar de la seguridad tradicional a una seguridad más innovadora; que a medida que crece la automatización los responsables de ciberseguridad "deben ser líderes de negocios, no líderes de lo técnico"; que la seguridad debe ser vista como una inversión, y no como un gasto, y por tanto "necesitamos comenzar a comprender cómo estamos impactando en el negocio".

¿Y cree que la ciberseguridad como servicio, la identidad como servicio, será la clave para cambiar el mundo? "Absolutamente. Significa que ya no te estás enfocando en la tecnología, solo la estás consumiendo. Y cuando comienzas a consumirla, entonces los negocios comienzan a enfocarse más en el lado comercial de las cosas y se convierten en los facilitadores del negocio". CST

ENLACES DESTACADOS

Delinea Platform debuta con la última versión de Secret Server

El 70% de las empresas pagan por herramientas de gestión de identidades que no utilizan

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de Delinea
John Shier, Director tecnológico Operaciones Comerciales de Sophos
José Manuel Canelada, Director Sales Engineering EMEA de Infoblox
Javier Abad, Regional Sales Director de Nozomi
TRIBUNAS

“No necesitas hacerlo solo. Hay un MDR detrás de ti”

Nos reunimos con John Shier, Director tecnológico de campo en operaciones comerciales de Sophos, para hablar de la situación del mercado de ciberseguridad, de la manera de luchar contra el ransomware, del papel de los servicios gestionados, o de cómo ver lo anormal para detectar la amenaza. Le pedimos también un mensaje de esperanza para las pymes, y que nos adelante en qué trabaja la compañía.

John Shier, Director tecnológico de campo en operaciones comerciales de **Sophos**

A la hora de hablar de la situación del mercado de ciberseguridad, dice que hay que tener en cuenta los dos lados, qué está ocurriendo en el lado de la protección y qué en el lado de los atacantes. Sobre estos últimos asegura que siguen siendo “muy oportunistas, lo que significa que no se enfocan en ninguna industria en particular”, salvo cuando se trata de estados nación, donde los objetivos están más claros.

En el lado de la protección, “estamos llegando a un punto en el que hemos infundido IA en todo, lo cual es realmente bueno porque nos permite hacer cosas a escala”. La IA, asegura, ayuda a liberar a los humanos para que hagan lo que mejor saben hacer, que es explorar las pequeñas excepciones con las que la máquina simplemente no puede lidiar.

Comentamos con el directivo de Sophos que es complicado saber lo inteligente que puede ser una inteligencia artificial. “Es una cuestión de confianza”, reconoce, porque está integrada en los productos. Añade que “los modelos se degradan con el tiempo, por lo que se vuelven menos buenos en lo que hacen. Pero seguimos capacitando a nuestros modelos”.

Ransomware

Siendo una amenaza para la que se han desarrollado multitud de defensas, sigue siendo uno de los principales dolores de cabeza de los responsables de ciberseguridad. ¿Hay alguna manera de acabar con el ransomware? “Mientras ganen dinero no hay razón para parar”, responde John Shier, añadiendo que parte del proble-

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

ma es que seguimos siendo vulnerables a los ataques.

Menciona el concepto “higiene de ciberseguridad” y recuerda que las vulnerabilidades sin parchear y las credenciales robadas son dos de los principales vectores de ataque. Además, “a pesar de que vemos más copias de seguridad hoy que nunca, se necesitan hacer más”, comenta.

Las mayores inversiones en ciberseguridad “no necesariamente están solucionando todos los problemas que deben solucionarse” porque de poco vale tener un producto para evitar cosas como el compromiso del correo electrónico si el usuario decide hacer el pago contra una cuenta bancaria. “No hay ningún producto que pueda evitar eso. Tiene que ser una cosa del proceso”, recuerda. Un proceso que contemple que, si se recibe este tipo de solicitud, hay un conjunto completo de pasos que se deben realizar para cumplir con esa solicitud, como puede ser llamar a otra persona, verificarlo, llamar a un número conocido, etc.

Resumiendo, la manera de luchar contra el ransomware es poner freno a sus modos de pago; instar a la gente a usar la tecnología, e higiene cibernética.

Vulnerabilidades

En los últimos años las vulnerabilidades no parcheadas han generado muchas e importantes brechas de seguridad a pesar de que las herramientas que permite gestionar esos parches de manera casi automática existen. Recuerda John Shier que los navegadores son un gran ejemplo de parcheos automáticos “tu navegador se ha parcheado solo durante años”.

Donde todo se vuelve un poco más complicado, dice también, es cuando se habla de aplicar parches a sistemas operativos completos o aplicaciones grandes. “Creo que las empresas, con razón, temen el tiempo de inactividad si algo sale mal. Y muchos de ellos pasan por

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

> "En SASE hay mucho que podemos hacer en el lado de la identidad"

estos largos ciclos de aplicación de parches en los que necesitan probar y garantizar la calidad de estos parches. Creo que tenemos que repensar la forma en que aplicamos los parches". En el pasado se ha optado por parchear de inmediato los ordenadores de sobremesa, las estaciones de trabajo, y se dejan para más adelante los servidores. "Yo diría que es al revés", dice Shier, proponiendo dedicar el tiempo que sea necesario para asegurarse de actualizar sus servidores web, sus puertas de enlace, todo ese tipo de cosas a las que se puede acceder desde Internet; "no van a ser tantos como sus estaciones de trabajo y están más expuestos", dice explicando que "si hay una mentalidad de prioridad, debe perseguir lo que los delincuentes van a perseguir. Lo primero que ven es tu presencia en Internet".

Servicios gestionados

¿Qué pueden hacer los servicios gestionados para ayudar a los responsables de ciberseguridad? "Muchas cosas. Pueden hacer todo para lo que no tienes tiempo. Y si además necesitas investigar, tenemos personas que pueden cazar amenazas", dice John Shier.

No sólo podemos implementar todas las capas

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

> "Mientras ganen dinero con el ransomware no hay razón para parar"

de protección primero, sino realizar análisis de manera proactiva, "y la parte proactiva es realmente importante porque podemos hacer cosas en toda la industria, en todas las geografías, en todos los tamaños de empresas". En el caso de Sophos se tiene tanta visibilidad de más de 15.000 clientes, cientos de miles de terminales, que permite a la compañía ver lo que está pasando "y nos permite ser proactivos en la protección de aquellas organizaciones que aún no han sido atacadas".

Esa visibilidad también permite a la compañía tener "inteligencia profunda sobre amenazas" y ofrecer un servicio de MDR que destaca por la visibilidad, "saber qué hacen los actores de amenazas y cómo lo hacen, para adelantarnos; y conocer los fallos, las vulnerabilidades".

Del *Best of Breed* a la apuesta por las plataformas

Hace años, tantos como para sumar más de una década, el mercado apostó por el "*best of breed*", lo que suponía comprar lo mejor de cada fabricante en lugar de aplicar una política "all-in-one". Años después, aquella decisión convirtió la complejidad en el principal reto de los responsables de TI en general, y de los de seguridad en particular. Si obtienes lo mejor de cada clase al final tienes diez herramientas diferentes con diez contratos de soporte diferen-

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

ciberseguridadTIC

tes, con diez licencias diferentes. El mundo de los orquestadores, que tuvieron su momento de gloria hace dos o tres años, se desvanece a favor de las plataformas. Son muchos, cada vez más, los fabricantes que están creando plataformas que no sólo orquesten su oferta, sino que admitan la de otros, incluidos competidores, para facilitar el día a día de los CISOs.

Preguntado en qué momento estamos del cambio de ese *best of breed* hacia las plataformas, responde John Shier que los conceptos no son excluyentes y plantea un "*best of breed Platform*". Asegurando que solo puede hablar por Sophos, dice el directivo que la misión de la compañía es que cada producto que se lance debe ser la mejor y estar basado en plataforma. Al final, asegura, si estás construyendo la plataforma con los mejores productos, entonces tienes una plataforma *Best of Breed*, "y al final del día tienes lo mejor de ambos mundos".

Seguridad completa

La trayectoria de Sophos le convierte en una empresa experta en integrar adquisiciones. Donde otros fallan, Sophos brilla, tanto como para iniciarse en el mundo de los antivirus y adentrarse como quien no quiere la cosa en el de la seguridad de red con la compra de Astaro hace más de diez años; con la compra de Barricade en 2016 consiguió sincronizar la seguridad de red y la del endpoint; un año después, la compra de Invicea le adentró en mundo de la inteligencia artificial... La compañía suma 17 adquisiciones, la última la de SOC.OS hace más de un año para llevar la respuesta gestionada a las amenazas y capacidades ampliadas de detección y respuesta al siguiente nivel. El resultado es una oferta de seguridad para la red, el endpoint, la nube, el correo electrónico, con funcionalidades de cifrado... y todo ello en modo servicio.

> "Las mayores inversiones en ciberseguridad no necesariamente están solucionando todos los problemas"

¿En qué son realmente buenos? "Sabemos cómo usar nuestros propios productos, pero ahora también nos estamos integrando con productos de terceros", responde John Shier, añadiendo que esta integración permite ofrecer excelentes productos de vanguardia, pero reducir la carga de administración; "hemos estado haciendo esto durante 38 años y para mí eso es una gran ventaja porque siempre estamos pensando en el cliente en términos de cómo será la experiencia cuando se siente frente a nuestra consola", y ahora ni eso porque se ofrece todo como servicio para que el cliente "siga con su día, haciendo cosas estratégicas para su negocio".

La detección de amenazas consiste en identificar lo diferente. ¿Cómo se hace? ¿qué convierte lo normal en una amenaza? Habla el

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

directivo de Sophos de Living off the Land, o LotL, un método de ataque en el que los ciberdelincuentes deciden optar por entrar en los sistemas de las organizaciones a través de programas confiables que no despiertan ninguna sospecha. La clave para detectarlos es saber cuándo se está utilizando de una manera que no es habitual. La clave es el contexto. "El tiempo, la geografía, la máquina del usuario... hay todo tipo de formas diferentes en las que puedes mirar algo y decir: eso no está bien porque está sucediendo en el momento equivocado del día, o en el país equivocado". El contexto, asegura el directivo, es imprescindible en la detección de amenazas, "y ahí es donde la IA es realmente buena".

Esperanza para las pymes

Los ataques son más y más sofisticados; la complejidad es inasumible en la mayoría de las ocasiones; la cultura de ciberseguridad deja mucho que desear; y la falta de talento, precisa. En este entorno se encuentran las pymes, que entienden poco de ciberseguridad más allá de considerarlo un gasto que pesa en sus presupuestos. Y que frente a los grandes titulares que aparecen cada día de ataques y más ataques a todo tipo de empresas no saben si tirar hacia delante o dar marcha atrás y encomendarse a Dios, o al destino. Porque en realidad, si han podido con un grande que invierte en ciberseguridad lo que yo gano en un año y tiene más personal en un departamento del que tengo yo en toda una empresa, ¿para qué intentarlo?

Frente a esta situación, le pedimos a John Shier un mensaje de esperanza a ese colectivo: "No necesitan hacer esto solos. No hay vergüenza

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

en pedir ayuda", dice, haciendo referencia a lo que cada vez está más de moda: la seguridad como servicio. "El mundo ha avanzado, tenemos tecnologías mejores y más nuevas, y diferentes maneras de hacer las cosas. Hay un MDR detrás de ti. Una ayuda respaldada por casi 40 años de experiencia. Solo tienes que preguntar".

Hoja de ruta

Para finalizar le pedimos a John Shier que nos cuenta en qué está trabajando Sophos. Hacia dónde va la innovación. Lo primero es seguir añadiendo Inteligencia Artificial "en los productos que son más directamente consumibles", nos dice. Habla de un LLM que permita a los

> "Creo que tenemos que repensar la forma en que aplicamos los parches"

clientes preguntar de manera sencilla por todas las direcciones IP que haya en su rede con determinadas características.

Se continuará invirtiendo en la plataforma de Sophos "para comprender qué es lo que necesitan los clientes", como el poder hacer evaluaciones de vulnerabilidad que les ayuden a tomar decisiones de seguridad informadas.

Dice Shier que Sophos está en la nube porque es hacia la nube hacia donde se dirige todo. "Construimos una plataforma en la nube y tenemos nuestros CSPM, Cloud Security Posture Management, pero estamos continuamente buscando cómo podemos mejorar", y la compañía desarrolló Cloud Optix que les permite monitorizar las cargas de trabajo, todo el tráfico de la red y todo el acceso de la identidad ya sea en Google, Amazon, Microsoft.

Habla también el directivo de SASE (Secure Access Service Edge), para asegurar que "hay mucho que podemos hacer en el lado de la identidad".

Por último, menciona el concepto Cloud Detection and Response para decir que están trabajando en ello y que esas inversiones servirán para mejorar la plataforma.

ENLACES DESTACADOS

Sophos: "Nuestra plataforma XDR permite detectar ataques de ransomware"

Virtual Cable: "La virtualización es un mecanismo para subsanar la falta de concienciación del usuario"

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

“Cada vez es más necesario utilizar elementos catalizadores como el DNS para proporcionar seguridad”

Fundada en 1999, el camino hacia lo que es la actual Infoblox se inició poco después, en 2007, cuando adquirió la *startup* francesa Ipanto, con la que empezó a desarrollar IPAM Win Connect. En 2010, Infoblox adquirió Net Cordia, que proporcionaba tecnologías para la automatización de tareas de red para, poco después, integrar la tecnología de gestión de direcciones IP de Infoblox con las tecnologías de gestión de cambios y configuración de red de Net Cordia.

José Manuel Canelada, Director Sales Engineering Europe, Middle East & Africa (EMEA) de **Infoblox**

Con el tiempo la compañía se centró en la gestión e identificación de los dispositivos conectados a las redes a través de tres funciones básicas que se engloban en el acrónimo DDI: DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol) e IP (internet Prtocol). El DNS, el sistema que convierte una dirección web en una dirección IP, es la base de Internet. DHCP es el sistema responsable de asignar direcciones IP automáticamente. La última parte del acrónimo, IP, significa protocolo de Internet y abarca otros aspectos básicos de la red. Infoblox puede ayudar a reducir el personal de TI al simplificar la configuración y el mantenimiento de las redes.

El tiempo siguió corriendo y el mercado DDI se quedó pequeño. Hoy, la misión de la compañía

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

ciberseguridadTIC

ENTREVISTAS

es “unificar las comunicaciones y la seguridad para proporcionar, por un lado, rendimiento y, por otro, protección”. Nos lo cuenta José Manuel Canelada, Director Sales Engineering Europe, Middle East & Africa (EMEA) de Infoblox. La apuesta por esta unificación se ha puesto de manifiesto con un cambio de imagen a finales de abril.

Explica el directivo que el mundo ha cambiado y que sería inocente pensar que los sistemas de protección como los entendíamos anteriormente van a seguir valiendo. “Aunque nuestra misión sea unificar las comunicaciones y la seguridad, el cómo lo vamos a hacer en Infoblox siempre va a ser a través de lo que conocemos, que es el DNS y toda la información de visibilidad que tenemos”, explica Canelada añadiendo que la nueva imagen “representa lo que hacemos y aporta la visión sobre la velocidad a la que creemos que se mueve un mundo que siempre está online”.

La nueva propuesta posiciona a Infoblox como una empresa capaz de proporcionar visibilidad

> “Unificar la seguridad y las comunicaciones aporta una enorme visibilidad”

y control en tiempo real sobre quién y qué se conecta a través de redes y entornos de múltiples nubes para ayudar a los clientes a crear entornos más seguros y resistentes. Explican desde la compañía que, al unir a los equipos de NetOps y SecOps con visibilidad, contexto de datos, automatización y control compartidos, pueden prevenir las comunicaciones de malware e identificar el origen de las amenazas.

El cambio no se ha producido de la noche a la mañana. Hace unos años se lanzaba BloxOne, plataforma de servicios de red y seguridad basada en SaaS y nativa en la nube donde la compañía da respuesta a las principales necesidades de los responsables de ciberseguridad. El primero de ellos, comenta José Manuel Canelada, es que se tienen demasiadas herramientas de ciberseguridad “sin que el retorno de inver-

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

ciberseguridadTIC

editorial

sión de esas herramientas sea visible". El segundo reto, o necesidad, es poder entender cuál es el tiempo de remediación de un ataque, y el tercero la evaluación del riesgo asociado a ese ataque

La pregunta obvia es cómo puede un proveedor de DDI, que históricamente ha sido un nicho de mercado, tener ese tipo de impacto. La respuesta: a través de DNS. Los expertos de la industria han pedido que la seguridad y las redes se unan durante décadas, pero ha sido lento, principalmente porque cada uno tenía sus herramientas. Sin embargo, hoy en día el mundo es bastante diferente, ha pasado a estar centrado en la red. Un malware ya no se queda en el endpoint, sino que puede llegar rápidamente a un servidor o a cualquier cosa que toque la red de la empresa, incluidas otras empresas. Por eso, la única forma de combatir las amenazas modernas es vincular las redes a la seguridad.

"El DNS es un elemento catalizador. Está en cualquier tipo de comunicación que hagamos, da igual que se esté en un premise, que cloud, que conectados desde nuestra mesa o desde un aeropuerto. Siempre vamos a utilizar el DNS. Esto reduce muchísimo el coste de aportar ciberseguridad a nuestros clientes", explica José Canelada.

Además del coste, menciona el directivo la capacidad de la compañía de reducir el tiempo de remediación al poder aportar información de valor sobre cada uno de los ataques, y compartirla con cualquier elemento de ecosistema. Unificar la seguridad y las comunicaciones aporta, además, "una enorme visibilidad".

Alrededor de BloxOne

A partir de BloxOne lo que ha hecho la compañía es añadir servicios adicionales. Uno de ellos es BloxOne Threat Defense, considerada la primera solución del mercado que aprovecha el sistema de nombre de dominios como la primera línea

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

> "El DNS es un elemento catalizador. Está en cualquier tipo de comunicación que hagamos"

de defensa para detectar y bloquear amenazas de ciberseguridad. La solución utiliza tecnología de inteligencia artificial y de aprendizaje automático para detectar las más recientes técnicas de malware, ransomware, *phishing*, kits de explotación, filtrado de datos basada en DNS, algoritmos de generación de dominio, DNS Messenger, ataques de flujo rápido y otras.

Además, gracias a su enfoque híbrido, permite utilizar la nube para detectar un mayor número de amenazas, al tiempo que proporciona visibilidad y conocimiento profundo de la postura de seguridad de la empresa, así como integración total con el ecosistema de seguridad corporativo.

Explica José Manuel Canelada que esto llevó a Inflobox a dar un paso más, a "intentar controlar lo que no se puede controlar. ¿Qué es lo que no se puede controlar? Que otras entidades registren dominios que se parecen mucho a mi dominio y eso sea utilizado en ataques de *phishing*, *smshing*..., explica el directivo. Así nació Lookalike Domain, que busca reducir el riesgo de suplantación de marcas para cometer fraude, acompañado de TakeDown, un servicio que contacta con los proveedores para echar abajo estos dominios que se crean con fines maliciosos.

Mercado español

Preguntamos a Canelada qué es lo que están demando los clientes. Responde diciendo que además del DDI tradicional se avanza en lo que define como el DNS Detection and Reponse.

Explica el directivo que desde la pandemia las empresas tienen más servicios digitales en la nube y a más gente trabajando fuera de las oficinas, lo que significa "que cada vez tienen más

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

El valor de la "nueva" Infoblox

Preguntado por el valor diferencial de Infoblox, responde José Manuel Canelada que el valor diferencial de la nueva Infoblox empieza por la misión de la compañía: unificar las comunicaciones y la seguridad. Algo que se va a hacer utilizando la visibilidad y el DNS como elemento de catalización; "a la vez que proporcionamos la resilencia en las comunicaciones y esta capacidad de automatización extrema, lo que vamos a hacer es proporcionar esta misma capacidad de automatización y resiliencia en la seguridad, por medio de reducción del riesgo, del tiempo de remediación, de la agregación de múltiples fuentes de inteligencia y del conocimiento de nuestra inteligencia artificial". No se olvida el directivo de mencionar el incremento del retorno de inversión del stack de ciberseguridad a través del uso del DNS.

necesidad de utilizar elementos catalizadores como el DNS para proporcionar seguridad". En opinión de José Manuel Canelada, es evidente que el paradigma de la seguridad ha cambiado y "no es que haya diferentes *Edge* en las comunicaciones, o diferentes *branches* en las empresas, es que cada uno de nosotros somos un *edge* de la comunicación de nuestra corporación".

> "El canal es uno de nuestros principales vectores de crecimiento"

Preguntado si la estrategia de unir redes y ciberseguridad ha tenido, o tiene, un impacto en el canal, dice Canelada que el canal "es uno de nuestros principales vectores de crecimiento" y que trabajar con más mercado requiere una expansión, no solo cuantitativa, sino también cualitativa. Añade que hay que proporcionar una relación de mayor calidad a los partners de la compañía, "porque el mundo es mucho más competitivo".

ENLACES DESTACADOS

Infoblox anuncia nueva estrategia de integración de networking y seguridad

Efficient IP: "El DNS es uno de los servicios más críticos y menos protegidos de las empresas"

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

“Ayudamos al cliente a entender qué riesgos tiene su entorno de OT”

Los productos de Nozomi Networks se centran en la detección de anomalías, la gestión de vulnerabilidades y el análisis de datos en entornos de OT, incluidas plantas de fabricación, atención médica e infraestructura crítica, aunque su cartera ha crecido para incluir también soluciones de seguridad de IoT. De esto y otras cosas hablamos con Javier Abad, responsable de la compañía para la región de Iberia.

Javier Abad,
responsable de **Nozomi** para la región de Iberia

Las soluciones de Nozomi Networks prestan servicio a más de 89 millones de dispositivos en miles de instalaciones en los sectores de energía, manufactura, minería, transporte, servicios públicos, automatización de edificios, ciudades inteligentes e infraestructuras críticas. Los productos de Nozomi Networks se pueden desplegar en la infraestructura propia de una compañía y en la nube, y abarcan TI, OT e IoT para automatizar el trabajo de inventariar, visualizar y supervisar las redes de control industrial mediante el uso de la inteligencia artificial. Los casos de uso van más allá de la ciberseguridad e incluyen la resolución de problemas, la gestión de activos y el mantenimiento preventivo.

Habla Javier Abad de un mayor acercamiento entre los mundos de IT y OT, así como de unos ciclos de amortización muy dispares en uno y otro entorno que son “el primer *gap* que hay que romper” porque la ciberseguridad, explica Javier Abad, no entiende de esto; “tienes que estar constantemente actualizado”, asegura el directivo, añadiendo que, a nivel presupuestario, las compañías empiezan a entender que hay que tener un foco constante en lo que es la parte ciber.

Dice también el responsable de Nozomi en España que ya no existen los llamados entornos

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Javier Sánchez Salas, CISO de ENGIE España
John Shier, Director tecnológico Operaciones Comerciales de Sophos
José Manuel Canelada, Director Sales Engineering EMEA de Infoblox
Javier Abad, Regional Sales Director de Nozomi
TRIBUNAS

ENTREVISTAS

> "Una vez que encuentro una amenaza, ¿qué quieres que haga con ella? ¿informo al SIEM? ¿al SOAR? ¿configuro una regla automática en el firewall?"

'air gap', burbujas dentro de una organización que no tienen conexión con el exterior. "Para mí el principal reto de las organizaciones es que sean conscientes de que hay una apertura y tienen que empezar a entender qué es lo que tienen y poner las medidas necesarias para poder funcionar de una forma eficiente y sin riesgos", asegura Javier Abad.

Preguntado por el valor diferencial de Nozomi, tiene claro el directivo que es "ayudar al cliente a entender qué riesgos tiene su entorno de OT". Y para ello, lo primero es saber lo qué se tiene. Nozomi ha estado muy reconocida en el mercado por su capacidad para entender todos los protocolos y dispositivos vinculados con el mundo industrial, y el primer paso para proteger el entorno industrial asegura Javier Abad, es "ayudar al cliente a tener una foto en tiempo real de qué dispositivos tiene, y sobre ellos saber cuál es la postura de seguridad".

Del mismo modo que las empresas del entorno industrial deben entender que no pueden ser burbujas y tienen que abrirse e interoperar con los diferentes departamentos, la propia Nozomi se ha abierto al mercado. De forma que no hace mucho Nozomi Networks anunció una asociación estratégica global expandida con Mandiant para ayudar a los clientes industriales y empresariales a anticipar, diagnosticar y responder a las ciberamenazas de IT y OT en sus operaciones empresariales críticas. Es de-

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

ciberseguridadTIC
Tai editorial

"Vamos a ser un poco más activos"

cir, la compañía está apostando por integrar su inteligencia de amenazas con otros fabricantes para dar un paso más porque "una vez que encuentro una amenaza, ¿qué quieres que haga con ella? ¿informo al SIEM? ¿al SOAR? ¿configuro una regla automática en el firewall?". Añade Javier Abad que Nozomi es un elemento pasivo dentro de la red. Nosotros no bloqueamos nada, no estamos en medio del tráfico. Ese es un trabajo que saben hacer muy bien otros fabricantes, y es con ellos con los que operamos".

En el mercado de seguridad OT se han visto dos tendencias. Por un lado, la aparición de empresas que han nacido para proteger estos entornos. Por otro, los fabricantes de ciberseguridad más tradicionales, sobre todo de seguridad endpoint, que han querido ampliar su mercado y proteger también estos entornos... sin mucho éxito, todo hay que decirlo. ¿Cómo debe abordarse este mercado para tener éxito? La pregunta da pie a Javier Abad a hablar de los inicios de Nozomi. Sus dos fundadores, Andrea Carcano y Moreno Carullo, trabajaban para la empresa nacional de hidrocarburos italiana; uno estaba haciendo un doctorado en ciberseguridad, el otro en inteligencia artificial, y alguien les pidió que inventariaran todos los dispositivos de OT de una organización y establecer la postura de seguridad. "Esto fue hace diez años en una empresa de 30.000 emplea-

PORTADA
EDITORIAL
SUMARIO
EN PORTADA
ACTUALIDAD
ENTREVISTAS
Joseph Carso, Chief Security Scientist y Advisory CISO de **Delinea**
John Shier, Director tecnológico Operaciones Comerciales de **Sophos**
José Manuel Canelada, Director Sales Engineering EMEA de **Infoblox**
Javier Abad, Regional Sales Director de **Nozomi**
TRIBUNAS

dos, distribuida en 60 países. Es nuestro ADN. Nos hemos ido adaptando al mercado, no porque tengamos ideas felices, sino por lo que van necesitando los clientes", explica el directivo.

La estrategia de la compañía pasa por seguir mejorando la propuesta tecnológica. "Vamos a ser un poco más activos", asegura "porque los clientes nos lo han pedido". Es decir, si la compañía ya está descubriendo que un dispositivo es Windows 95, "¿por qué no me dices qué versión de antivirus tiene? De forma que mediante técnicas que denominamos *smart pooling* somos capaces de interrogar un poco más, de ser un poco más activos e incluso ver quién está hablando con ese entorno para poder también discernir qué protocolos hay más allá del *switch*".

> "Las empresas tienen y poner las medidas necesarias para poder funcionar de una forma eficiente y sin riesgos"

El otro elemento estratégico para la compañía es "seguir apoyando y ayudando a nuestro canal". CST

ENLACES DESTACADOS

Nace ETHOS, una plataforma para el intercambio de información de alertas en el mundo OT

Opscura llega al mercado con una inyección de capital de 9,4 millones de dólares

TRIBUNAS

Cómo presentar las soluciones Zero Trust al director general y al consejo de administración

Hay una increíble oportunidad para que los responsables de TI conciencien y eduquen a la alta dirección sobre la confianza cero y la presenten como un motor empresarial de alto valor. Como dice Heng Mok, CISO AJP de Zscaler, en esta tribuna, es el eslabón perdido que ayuda a las empresas a prepararse hoy para las tecnologías del futuro.

MÁS INFORMACIÓN

Las claves para una recuperación inmediata

En este artículo Jaime Balañá, Sr. Solutions Engineering Manager Iberia & LatAm de NetApp, propone tres pilares clave que ayuden a las empresas a consolidar una estrategia que mantenga a salvo los datos de amenazas internas y externas.

MÁS INFORMACIÓN

La evolución del ransomware: navegando por la nueva era de ciberdelincuencia

En esta tribuna Mario García, director general de Check Point Software para España y Portugal, recorre la evolución del ransomware: el número de víctimas está disminuyendo y las demandas de los piratas informáticos están cambiando.

MÁS INFORMACIÓN