ciberseguridadTIC
seguridad en informática y comunicaciones
Tai editorial
Año I Nº 2
Marzo 2023

Ellas también son ciberdelincuentes

Engie:
"Los CISO somos habilitadores, y estamos cada vez más cerca del negocio"

Isemaren:
"La seguridad tiene que ir asociada, por diseño y por defecto, a todos los procesos de la organización"

Netskope:
"La prioridad es proteger los datos"

Fortra:
"El esfuerzo de gestionar, administrar e integrar todos los productos de seguridad no es viable"

IR A PÁGINA SIGUIENTE

Ellas también son ciberdelincuentes

Marzo es el Mes de la Mujer, un mes que busca destacar los logros conseguidos a lo largo de los años en materia de igualdad de género y que reclama nuevas medidas que permitan seguir avanzando. En muchos sentidos, la ciberdelincuencia es una de las comunidades más meritocráticas, donde los desarrolladores son valorados por sus habilidades y experiencia, y no necesariamente por su género cuando se trata de realizar negocios clandestinos. A ello dedicamos el tema de portada.

Javier Sánchez Salas, CISO de Engie, y Jesús Valverde, CIO y CISO de Isemaren, son los grandes protagonistas de la revista de marzo. Con ellos hablamos de los retos del CISO, de cómo escoger entre tanta oferta o de las amenazas que les quitan el sueño.

En su paso por Madrid aprovechamos para hablar con Chris Andrews, vicepresidente de ventas a nivel mundial de Netskope, para quien la prioridad es proteger los datos. También hablamos por vídeo con Paolo Capello, responsable del negocio internacional de Fortra, conocida antes como HelpSystems, que ha afrontado un *rebranding* que muestre su apuesta por la ciberseguridad.

Eutimio Fernández es el nuevo responsable de Vectra AI en España y Portugal. Con él hablamos de la oferta de la compañía y sus ventajas competitivas.

En el apartado de actualidad os contamos qué ocurrió en Commvault Connections, un evento que se ha celebrado en varias ciudades europeas, incluida Madrid, y donde pudimos hablar con César Cid, VP International Sales Engineer de la compañía.

SUMARIO

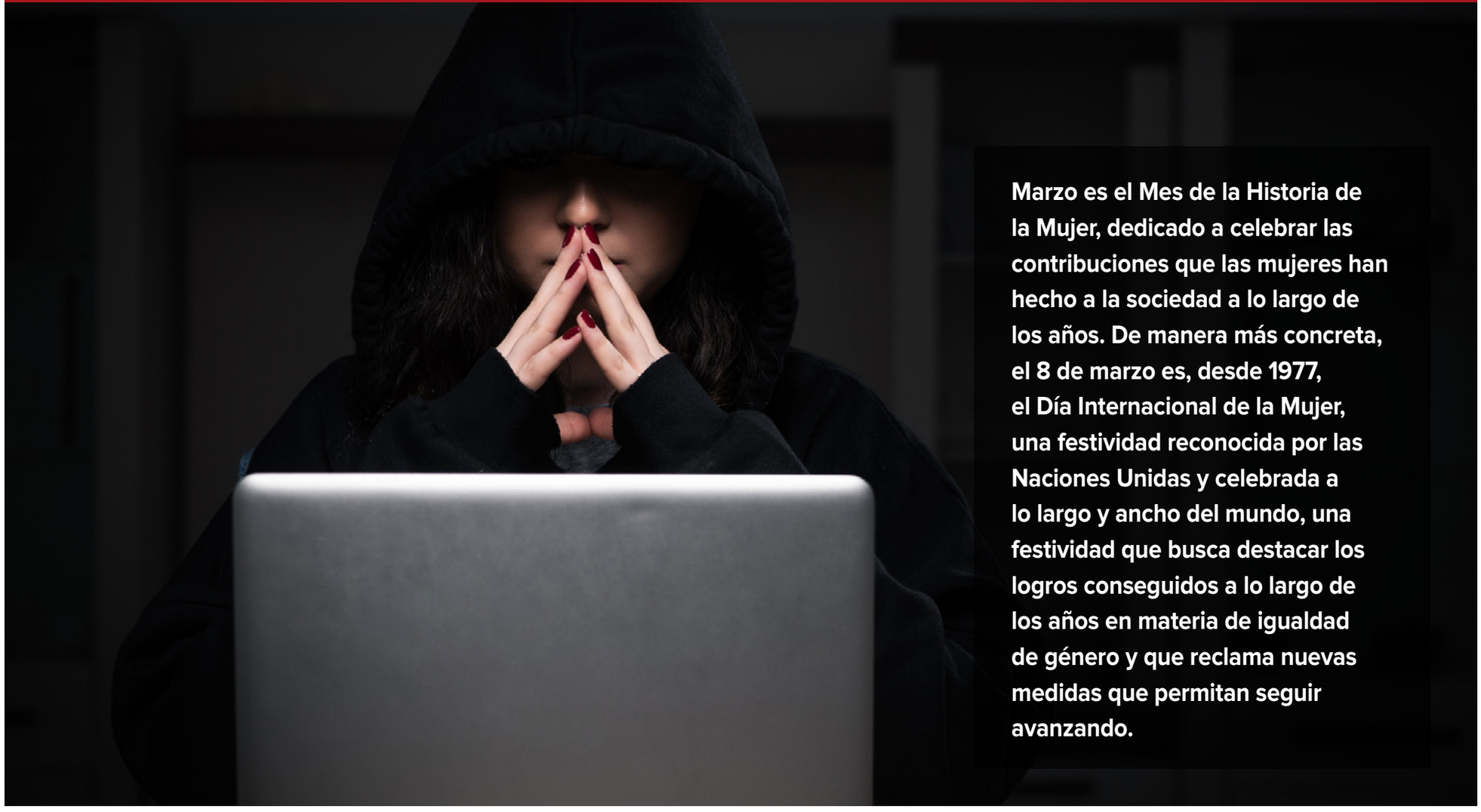
Directora:
Rosalía Arroyo
rosalia@taieditorial.es

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

Ellas también son ciberdelincuentes



Marzo es el Mes de la Historia de la Mujer, dedicado a celebrar las contribuciones que las mujeres han hecho a la sociedad a lo largo de los años. De manera más concreta, el 8 de marzo es, desde 1977, el Día Internacional de la Mujer, una festividad reconocida por las Naciones Unidas y celebrada a lo largo y ancho del mundo, una festividad que busca destacar los logros conseguidos a lo largo de los años en materia de igualdad de género y que reclama nuevas medidas que permitan seguir avanzando.

ciberseguridadTIC

Tai editorial

EN PORTADA

Hoy, el cibercrimen y los ciberdelitos están a la orden del día. El número de víctimas crece al ritmo que lo hacen las ciberamenazas, cada vez más sofisticadas, y a pesar de que son muchos, demasiados, los ciberdelincuentes permanecen sin ser rastreados y la mayoría son hombres. También hay aquí una brecha de género y también se va ganando terreno milla a milla.

Trend Micro ha elaborado un interesante informe que cifra la presencia de la mujer en el cibercrimen asegurando, en primer lugar, que la participación femenina en el ciberdelito es mucho mayor que en todos los tipos de delitos. En muchos sentidos, el de la ciberdelincuencia es una de las comunidades en línea más meritocráticas, donde los desarrolladores son valorados por sus habilidades y experiencia, y no necesariamente por su género cuando se trata de realizar negocios clandestinos.

Aunque debido al anonimato el género juega un papel menor en los foros clandestinos de ciberdelincuentes, donde se valora más a las personas por sus habilidades y experiencia,

> El género no es un problema cuando se realizan negocios en la clandestinidad

que ahora haya más mujeres involucradas en trabajos de ciencia, tecnología, ingeniería y matemáticas (STEM), se extenderá a la clandestinidad, ya que también sigue los cambios sociales y comerciales del mundo real.

Existen diferentes teorías con respecto a la falta general de participación de las mujeres en el ciberdelito, incluido el menor número de mujeres que participan en comunidades de foros online y la brecha en el acceso a Internet. Según un estudio realizado por la World Wide Web Foundation en 2020, es menos probable que las mujeres creen contenido en línea, comenten o publiquen sobre eventos políticos cuando se conectan, y el 29 % tiene más probabilidades de vender o publicitar un producto. Por otra parte, aunque su presencia en el mercado de ciberseguridad está creciendo, aún hay una brecha importante. Cybersecurity Ventures predice que las mujeres representarán el 30 % de la fuerza

Valérie Gignac

En 2015 se acusaba a Valérie Gignac, por entonces de 27 años, de cuatro cargos relacionados con el uso no autorizado de una computadora y daños en relación con datos informáticos.

Se cree que Gignac usó una botnet para espiar a las personas a través de sus cámaras web.

También dicen que Gignac es el propietario de un foro de piratería en línea que tiene 35.000 usuarios en todo el mundo.

EN PORTADA

Lauren Lide

Lauren Lide, una joven de 26 años que solía trabajar para la escuela Melbourne Flight Training, renunció a su puesto de gerente de operaciones de vuelo a finales de noviembre de 2019, después de que la compañía despidiera a su padre. Meses después, supuestamente pirateó los sistemas de su antigua empresa, eliminando y cambiando registros, en un aparente intento de vengarse de su antiguo empleador, según los registros judiciales obtenidos por Motherboard.

laboral mundial en ciberseguridad para 2025, y el 35 % para 2031. El informe mencionó que, a partir de 2021, las mujeres ocupaban el 25 % de los trabajos de ciberseguridad en todo el mundo, lo que refleja un aumento anual de mujeres practicantes incluso en promedio. En opinión de los investigadores de Trend Micro, es importante que entendamos las relaciones entre el género y el delito cibernético para comprender los problemas que los investigadores pueden enfrentar y enfrentarán más adelante: El delito cibernético no es neutral en cuanto al género.

Se da por hecho que la mayoría de los ciberdelincuentes son hombres. Con el tiempo, sin embargo, las ciberdelincuentes femeninas han ido dando a conocer su presencia. En los foros clandestinos de ciberdelincuentes, los trabajos para mujeres incluyen roles como mulas de dinero y con fines de lavado de dinero.

Sin atreverse a concluir que la comunidad ci-

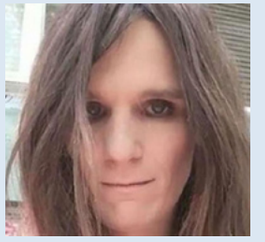
EN PORTADA

bercriminal se haya vuelto más tolerante con las mujeres, "sería más exacto decir que el género no es un problema cuando se realizan negocios en la clandestinidad", dicen los investigadores. Un ejemplo es Alla "Max" Witte, mujer y madre de 55 años acusada por su participación en Trickbot Group. Muchos en la banda de ciberdelincuentes no solo conocían su género sino también su nombre. Era tan querida que, en un momento, los miembros del grupo de *ransomware* Conti estaban considerando pagar sus honorarios legales.

Trabajos de género

Los datos del estudio de Trend Micro indican que los tipos de trabajos anunciados específicamente para mujeres en los foros de ciberdelincuentes incluyen *muling* (facilitadores para el tráfico

Paige Thompson



Ex ingeniera de Amazon, Paige Thompson desarrolló una herramienta que escaneaba Amazon Web Services (AWS) en busca de cuentas mal configuradas para obtener acceso a los sistemas de Capital One y docenas de otros clientes de AWS. Fue acusada formalmente por cargos de delitos informáticos, incluido el robo de datos de al menos 30 organizaciones y el uso de servidores pirateados para extraer criptomonedas. Thompson fue declarada culpable de fraude electrónico, cinco cargos de acceso no autorizado a una computadora protegida y daños a una computadora protegida. El jurado la encontró no culpable de fraude de dispositivo de acceso y robo de identidad agravado.

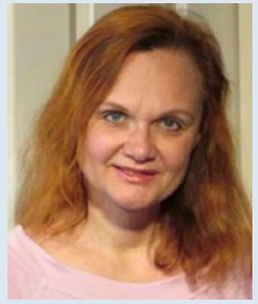
EN PORTADA

Alla “Max” Witte es una mujer acusada por su participación en Trickbot Group

de drogas y lavado de dinero, entre otros), trabajos de *call center* y estafas de ingeniería social donde generalmente se necesita voz e imágenes. Sin embargo, la mayoría de los anuncios de trabajo que se encuentran en la clandestinidad son de género neutral y están abiertos a todos, siempre que tengan las habilidades adecuadas similares al mundo real, donde el género no se menciona. En la clandestinidad, los puestos de reclutamiento de bandas de ciberdelincuentes tampoco mencionan el género.

Las mulas son utilizadas por otros para lavar el producto del ciberdelito al tomar dinero y bienes robados y convertirlos en fondos limpios. Lo hacen a través de pagos por Internet, transferencias de dinero o subastas online. Los investigadores detectaron un sitio web anunciado en un foro ruso sobre falsificación de documentos, servicios de apuestas e intercambios de criptomonedas donde se mencionaba específicamente el género y la edad.

Alla Witte, alias Max



Con 55 años, Alla Witte, alias Max, fue acusada de participar en una organización criminal conocida como el “Grupo Trickbot”, responsable de desplegar el malware Trickbot

Witte fue desarrolladora de malware y quien supervisaba la creación de código relacionado con la supervisión y el seguimiento del malware Trickbot, el control y la implementación de *ransomware*, la obtención de pagos de las víctimas y el desarrollo de herramientas y protocolos para la almacenamiento de credenciales robadas y exfiltradas de víctimas infectadas por Trickbot.

Investigación

A la hora de realizar su estudio, los investigadores utilizaron una herramienta de inteligencia artificial para determinar el género de los usuarios del foro de ciberdelincuencia. Semrush se anuncia como una solución de marketing de motores de búsqueda que utiliza algoritmos de aprendizaje automático para analizar datos de redes sociales y otras fuentes de terceros, con el fin de determinar la información demográfica de los usuarios de la web, como el género.

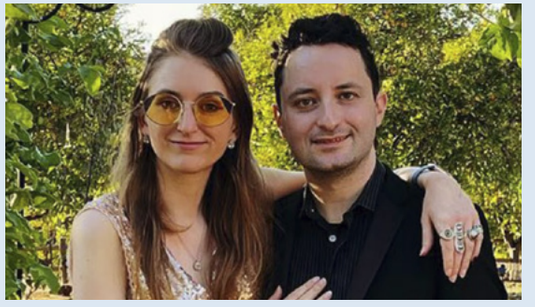
Se analizaron algunos foros en inglés (Sinister, Cracked, Breached, Hackforums, Raidforum) y otros tantos en ruo (XSS, Exploit, Vavilon, BHF, WWH-Club) escogidos “por su popularidad en la comunidad de delitos cibernéticos, la cantidad de usuarios que participan y siguen los foros, la cantidad de hilos y la cantidad de trabajos y publicaciones ofrecidos”, explican los

investigadores, añadiendo que, especialmente en el caso de los foros rusos, XSS y Exploit se clasifican como los dos foros más populares para los analistas de ciberdelincuencia e investigación de seguridad.

De una muestra de 200 visitantes a los foros en inglés, el 40 % eran mujeres, una cifra que aumentaba hasta el 42,6 % en los foros rusos. De manera más concreta, Sinister tuvo la mayor cantidad de visitantes femeninos con un 61 %; en el otro extremo se sitúa Stack Overflow, un foro de desarrolladores y programación en el que sólo el 12 % de los visitantes eran mujeres.

Para profundizar aún más en la investigación, se trabajó con un analizador de texto de género, Gender Analyzer V5 creada en 2008 por uClassify, que permitía averiguar si el texto de un foro está escrito por un hombre o una mujer.

Ilya y Heather



El matrimonio Ilya "Dutch" Lichtenstein y Heather "Razzlekhan", fue arrestados en febrero de 2022 por presuntamente conspirar para lavar criptomonedas robadas durante el pirateo de 2016 del intercambio de moneda virtual Bitfinex.

Se acusó a Lichtenstein y Morgan de tener acceso a numerosas identidades y documentos fraudulentos comprados en la dark web. Fueron acusados de conspiración para cometer lavado de dinero y conspiración para defraudar a los EE. UU.

Para esta parte de la investigación, se analizaron dos foros: XSS de habla rusa y Hackforums

de habla inglesa. En concreto, se ejecutaron 50 cuentas de usuarios aleatorios del foro XSS, lo que puso de manifiesto que el 70 % eran usuarios masculinos y el 30 % femeninos. Al comparar estos resultados con los análisis de Semrush, predijeron que XSS recibió un 59 % de visitantes masculinos en comparación con un 41 % de mujeres.

> Con un 61 %, Sinister fue el foro en inglés que tuvo la mayor cantidad de visitantes femeninos

El mismo ejercicio se realizó con 50 alias aleatorios de Hackforums. Los resultados mostraron que los alias eran 64 % masculinos y 36 % femeninos. Estos resultados están más cerca de los foros generales en inglés donde encontramos que el 40 % de las mujeres visitaron estos sitios en comparación con el 60 % cuando se utiliza Semrush.

ENLACES DESTACADOS

El coste medio de una brecha alcanzará los cinco millones en 2023

The Gender-Equal Cybercriminal Underground

Commvault Connections. Innovando con confianza

En los próximos 5 años el 55 % de las soluciones de protección de datos estarán basadas en la nube, pero el 45 % restante no. El escenario será híbrido, por lo que se necesita una estrategia de gestión de datos escalable en diferentes entornos, capaz de soportar cualquier tipo de carga de trabajo y capaz de preservar la usabilidad de los datos. Commvault tiene la solución.

“Lo que marca la diferencia es la confianza”, decía Mauro Palmigliani, vicepresidente de Commvault para el suroeste de Europa. Lo decía en Commvault Connections, un evento que se ha celebrado en varias ciudades europeas, incluida Madrid, donde la compañía ha presentado la nueva versión de su plataforma para ampliar la protección segura de los datos en entornos híbridos multi-nube y ha querido dejar claro que puede ayudar a innovar con confianza hoy y mañana.

Los datos son cada vez más importantes, las empresas se mueven en entornos híbridos y ya no solo hay que hablar de *backup*, sino de la protección y seguridad del dato, de gobernanza,

ACTUALIDAD

de cumplimiento o de analítica. Las plataformas que alojan los datos y se utilizan para estos fines deben funcionar de manera transparente tanto en la nube como en las instalaciones; “Se trata de simplificar las arquitecturas de gestión de datos para gestionar un contexto de complejidad creciente y ciberataques sofisticados”, decía Palmigliani, añadiendo que Commvault Platform Release 2023, la nueva versión de la plataforma de la compañía “muestra claramente cómo la empresa se está moviendo hoy en dos direcciones principales: seguridad e innovación”.

La nueva versión de la plataforma de gestión y protección de datos introduce nuevas características y funciones como Threat Scan Analysis (motor de detección de malware) y File Scan Analysis para el análisis de la copia de seguridad y la identificación de que ponen de manifiesto que “la línea entre la protección de datos y la ciberseguridad es cada vez más delgada”.

Decía Palmigliani durante su intervención que, aunque sea lo más mencionado, “el *ransomware* no es el único problema para la protección de datos”. Mencionaba los ataques de DDoS, que impiden acceder a los datos, y recordaba que el poder de Commvault se refleja en “The Power of And”, o la capacidad de administrar en entornos locales y en la nube para optimizar la entrega de servicios de datos en el mundo de la nube híbrida de hoy.

> “La línea entre la protección de datos y la ciberseguridad es cada vez más delgada” Mauro Palmigliani, AVP SW Europe & Israel de Commvault

César Cid, VP International Sales Engineer de Commvault, salía a escena para hablar de innovación y asegurar que “la aproximación única al Data Management es el secreto de Commvault”. Los datos crecen, pero el problema, dijo, no es la gestión de los datos, sino que ese crecimiento está ampliando la superficie de ataque;

ACTUALIDAD

"los datos no estructurados son un regalo para un ciberdelincuente", aseguraba. Mencionó el peligro del *ransomware* y Zero Loss, la estrategia de Commvault para hacerle frente, y cerró su discurso recordando la gran innovación de la compañía "en soluciones elegantes y fáciles de utilizar".

Recordando que "es mejor prevenir que curar", Sandra Espinoza, Senior Sales Engineer de Commvault centraba su ponencia en cómo implementar una estrategia Zero Loss sin costes adicionales mencionando tres datos interesantes sobre el *ransomware* en España: el 71 % de las empresas han sufrido un ataque de malware; el 4 % de los que pagaron el rescate no recuperaron los datos; el coste medio de una brecha son 3,7 millones de dólares.

Es fundamental, aseguraba, tener un plan de respuesta y saber "quién se hace cargo de qué" para, a continuación, desgranar los tres grandes principios en los que se basa la estrategia Zero Loss: visibilidad de todos los datos de la compañía; protección extremo a extremo, "no hay ninguna carga que se quede atrás"; y una respuesta rápida, "porque si somos buenos haciendo *backup*, somos mejores haciendo restauración".

Metallic Threatwise

Mención especial merece Metallic Threatwise, mencionado en numerosas ocasiones durante el evento. Es el nombre la solución de deception de la compañía y que mejor demuestra la apuesta de la compañía en el campo de la ciberseguridad. A través de trampas y engaños, la solución permite anticiparse a las amenazas, interceptando los movimientos laterales del atacante y, a través de un tablero, rastrear los movimientos, reportarlos, contextualizarlos y pasar información ya consumible y procesada al SIEM.

El de ciberdeception es no es un mercado nuevo, pero está creciendo. Valorado hoy en 1.800

ACTUALIDAD

> Valorado hoy en 1.800 millones de dólares, el mercado de *ciberdeception* alcanzará los 5.800 millones en los próximos cinco años

millones de dólares, llegará a 5.800 millones en los próximos cinco años.

Commvault Platform Release 2023

Lanzada a mediados de diciembre de 2023, la última versión de la plataforma de gestión y protección de datos de la compañía, incluye nuevas integraciones para facilitar a los clientes la protección de sus datos en Microsoft Azure, AWS Cloud, Google Cloud Platform y Oracle Cloud Infrastructure.

Con el objetivo de mejorar la seguridad de los datos, se apoya a las herramientas SIEM (Security Information and Event Management) con un conector que facilita la alimentación de alertas, eventos y datos de auditoría a otras plataformas a través de APIs *webhooks* o *syslog*. El aprovechamiento de protocolos estándar garantiza que la empresa pueda trabajar con casi cualquier SIEM o sistema de gestión de eventos, ofreciendo a los equipos de seguridad una mejor visibilidad de las anomalías y amenazas en sus datos.

La última gran mejora de la plataforma tiene que ver son el ahorro inteligente. Las nuevas capacidades para utilizar *snapshots* de una sola región frente a *snapshots* multirregión para GCP pueden ahorrar un 30 % de ese coste a los recursos de *backup*. Las optimizaciones de Commvault para Hadoop, que aprovechan *snapdiff*, pueden reducir a minutos lo que antes eran escaneos de *backup* que duraban horas, gracias a las mejoras en la forma de escanear los bloques modificados.

César Cid: “Para nosotros la innovación es absolutamente clave”

César Cid,
VP Intl Sales Engineering de **Commvault**

“Jamás permitiremos que nuestros clientes se queden estancados a la hora de innovar porque no somos capaces de proteger un *workflow* que ellos necesitan proteger”, aseguraba César Cid durante un breve encuentro mantenido durante el evento después de comentar que la innovación es absolutamente clave para Commvault, y que la empresa escucha a los clientes, tanto como para que más de 400 novedades incorporadas a la plataforma hayan sido peticiones de los propios clientes de la compañía.

Como ejemplo de innovación hacía referencia el directivo a Metallic Threatwise, un servicio de deception que nace fruto de la compra de TrapX a principios de 2022, y que queda fuera de la actividad tradicional de protección y gestión de información de la compañía.

También asociado a la innovación está Metallic, un *backup* en modo SaaS “que tiene un crecimiento ya ni siquiera doble dígito, incluso de 50 % anual”. Con ocho trimestre de vida, Metallic ya ha superado los 100 millones en ingresos recurrente ARR y su futuro es brillante.

> “Los clientes adoptan herramientas tipo silo que generan dos problemas: aumentan el TCO y provocan riesgos de seguridad”

Preguntado sobre los principales desafíos que tienen sus clientes, menciona César Cid que cuando quieren innovar con soluciones que no son Commvault “lo que hacen los clientes es parchear. Adoptan herramientas tipo silo que generan dos problemas: aumentan el TCO y provocan riesgos de seguridad, por no hablar de conocimiento”. La alternativa, propone el directivo, es una solución única con un único punto de gestión.

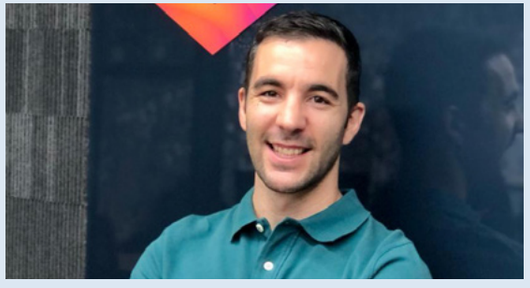
Un segundo desafío es el crecimiento exponencial de información,

"que es hasta cierto punto inmanejable" y además representa "una superficie muy amplia para que te puedan atacar". La manera que tiene Commvault de gestionar la información y poder abordar y paralizar los ataques "es única", asegura César Cid. Explica el directivo que ante un ataque de Día Cero "puedo hacer escaneos recurrentes e integrados con soluciones líderes de mercado para garantizar que estas copias son limpias, y en caso de que haya una infección limpiarla directamente del *backup*. Esto lo podemos hacer y a nivel de innovación es único".

Preguntamos también a César Cid qué funcionalidades son las más demandadas o más se valoran. Cogiendo como referencia los tres pilares de la estrategia de Zero Loss tiene claro el directivo que en End-to-end Visibility es ThreatWise, "esa herramienta de decepción mediante la cual engañamos a los actores maliciosos que quieren atacarnos" orientada a la protección del dato. En la parte de *workloads*, tiene mucho tirón "toda la parte de Salesforce y toda la integración con Microsoft". Finalmente, en la parte de "recuperaciones rápidas y eficaces destaca el *airgaping*, fundamental para garantizar que el almacenamiento es inmutable, además de la automatización, orquestación e integración con terceros".

ENLACES DESTACADOS

Metallic: "El *backup* se está incluyendo en las estrategias de ciberseguridad"



La seguridad en la nube es una responsabilidad compartida

***Backup* para un ciberataque**

Tenemos **toda la información** que necesitas

ciberseguridadTIC
Tai editorial

ENGIE: “Los CISO somos habilitadores y estamos cada vez más cerca del negocio”

Con más de 14 años de experiencia en el mundo de la ciberseguridad, Javier Sánchez Salas es el CISO de ENGIE, el sexto agente generador de España con una capacidad instalada de cerca de 3.600 MW, incluyendo 1.600 MW de activos renovables. Con una fuerte presencia en todo el territorio nacional, el valor diferencial de ENGIE es la capacidad de gestión de toda la cadena de valor de la energía, encargándose de la financiación, construcción, explotación y mantenimiento de los activos. Estas características hacen de ENGIE el socio de referencia en España para acelerar la transición energética.

Javier Sánchez Salas,
CISO de **ENGIE España**

Ser CISO es, en opinión del directivo, “una carrera de largo recorrido” que, en el caso de Javier, se inició con una carrera técnica, la de Informática. Después, “poco a poco te vas enredando y vas conociendo gente” hasta que le llegó su primera oportunidad, hace 15 o 16 años, durante los que ha estado dedicándose exclusivamente a la ciberseguridad. Esto le ha permitido vivir en primera persona la evolución del CISO.

Para Javier Sánchez Salas, los CISO “hemos pasado de ser una un mal que está en la oficina, en el sótano y de vez en cuando protestamos, a una persona que tiene un peso importante en la empresa”. Añade que los miembros del comité directivo de las empresas “nos ven como

ciberseguridadTIC

Tai editorial

alguien a quien escuchar. No estamos ahí para decir que no, sino para ayudarles a mitigar los riesgos, minimizarlos y que el negocio siga hacia adelante, pero de una forma segura, de una forma correcta". Continúa diciendo el directivo que los CISO se han convertido en habilitadores del negocio y miembros importantes de las empresas.

Preguntado por las principales cualidades que debe tener un CISO, tiene claro Javier Sánchez Salas que tiene que ser cercano a negocio, "porque si no, no te van a llamar". Añade ser resiliente, destacando que el de CISO es un perfil "que tiene que ir evolucionando con el mercado y tenemos que estar día a día, transformándonos y aprendiendo nuevas tecnologías.

¿Qué amenazas le quitan el sueño a Javier Sánchez Salas? "Todas", responde, comentando que ahora "el mayor problema que tenemos es ayudar a nuestros empleados, a nuestros usuarios, a comprender que lo primero es no caer en las trampas que poner los cibercriminales" porque "la ciberseguridad no sólo depende del equipo de seguridad o de tecnología implantada, somos todos los empleados de la empresa".

> "Las empresas ya no valen lo que valen sus equipos, sino lo que vale su información"

En un mercado tan fragmentado como es el de la ciberseguridad, con centenares de empresas y una innovación constante, ¿cómo se escoge la solución más adecuada? Responde Javier Sánchez Salas que se busca una solución que sea escalable y con la que "podamos ir haciendo un despliegue poco a poco".

En segundo lugar, "que no sea una aplicación que sepas que va a ser un *one-off*, que una vez que la despliegas te olvidas. Tiene que evolucionar igual que el negocio" y pone como ejemplo el mercado de soluciones de seguridad *endpoint*, que han evolucionado de las soluciones tradicionales basadas en firmas a propuestas con inteligencia y *machine learning* "que hacen estadísticas, establecen un cuadro de mandos que pueda ser medible y te permita tener tus propios PKIs dentro de herramientas, que es algo ya básico", asegura el directivo.

Centrándonos en el segmento de mercado al que pertenece Engie, el industrial, dice Javier

ciberseguridadTIC

Tai editorial

ENTREVISTAS

Sánchez Salas que es “un poco menos tradicional en cuanto a ciberseguridad”. Comenta que además de la seguridad IT que tienen todas las compañías, “tenemos un componente de seguridad OT”, un entorno más complicado de gestionar que implica no solo que muchas de las instalaciones están en sitios no acondicionados para tener un CPD de ciberseguridad, sino que “incluso caemos en problemas que antes no me había planteado, como es el polvo, que puede afectar a elementos de seguridad como el firewall”.

Comenta también Javier Sánchez Salas que el mundo industrial va a una velocidad distinta del mundo IT y que el impacto de un ataque es diferente; “si nosotros no somos capaces de parar una subestación energética a tiempo puede haber un problema mayor a la población que si se paraliza una transacción financiera. No es igual el impacto económico que el impacto social que puede tener”.

> “La pérdida de perímetro ha cambiado la forma de entender la seguridad”

Tecnologías

Planteamos al CISO de ENGIE qué tecnologías de seguridad básicas debe tener cualquier empresa. Lo primero, asegura, es “tener un proveedor de soluciones que sea adecuado en cuanto al alojamiento de tu infraestructura”. Habla también de herramientas antimalware proactivas, “que detecten y te solucionen el día a día y te hagan un seguimiento de las incidencias que tienes”, es decir un EDR o XDR. No se olvida de la monitorización “para ver eventos y patrones de ataque”.

Y fuera de lo que es seguridad de la infraestruc-

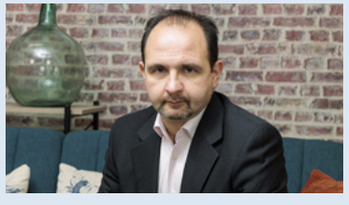
> "Buscamos soluciones que sean escalables y con las que podamos ir haciendo un despliegue poco a poco"

tura, donde entran los *firewalls*, IDS, IPS... se decanta el Javier Sánchez Salas por el paradigma del SD-WAN, "que es maravilloso" y ofrece la posibilidad de que cualquier usuario se pueda conectar desde cualquier sitio con las mismas protecciones que si estuviera en la oficina, "y eso para mí es un *must* ahora mismo".

La pérdida de perímetro, ¿ha cambiado el paradigma de la seguridad? "Ha cambiado la forma de entender la seguridad", asegura el directivo, añadiendo que "las empresas ya no valen lo que valen sus equipos, sino lo que vale su información. Y tenemos que proteger esa información".

Los modelos Zero Trust y SD-WAN son elementos del mercado de seguridad imprescindibles en el corto plazo, "porque es una tecnología que te va a permitir tener tu información controlada y enrutada por donde tiene que ir".

ENLACES DESTACADOS



Veeam: "Cada vez está más claro que el *backup* es la última línea de defensa"

Hillstone Networks: "La complejidad es el activo más caro"

Isemaren: “La seguridad tiene que ir asociada, por diseño y por defecto, a todos los procesos de la organización”

Jesús Valverde, CIO y CISO de Isemaren, imagina un mundo ideal en el que el CISO estaría en una posición de reconocimiento por la Dirección de la compañía en la que pudiese, si es necesario, decir que no a una iniciativa estratégica para el CIO /CFO / CHRO si esa iniciativa no está adecuadamente planteada. Dice que no existen soluciones mágicas que te protejan de todo sin necesidad de intervención humana; que lo que le quita el sueño es que la información de su empresa pueda verse comprometida; que el usuario es el eslabón más débil sólo si el departamento de seguridad de la empresa no ha sido capaz de formarlo o concienciarlo; y que hay fabricantes de DLP que lo han evolucionado de formas increíbles.

Jesús Valverde,
CIO y CISO de **Isemaren**

Nos cuenta Jesús Valverde, CIO y CISO de Isemaren, que llegó al mundo de la ciberseguridad desde una ingeniería de telecomunicaciones complementada con un máster en Gestión Integral de las TIC, donde se familiarizó con conceptos y estándares internacionales como la ISO 27001. Fue en uno de sus primeros puestos de trabajo, donde se incorporó como responsable de operaciones, “donde fui sumando cargos más concretos, como responsable de soporte, de protección de datos, de seguridad…” y donde acumuló experiencia en la gestión de las TI y de ciberseguridad, que posteriormente reforzó durante más de tres años formando par-

ciberseguridadTIC

Tai editorial

ENTREVISTAS

> "Todo el mundo tiene claro el riesgo económico, pero el riesgo de ciberseguridad es más complejo de explicar"

te del equipo de seguridad global de Telefónica y otros tres, siendo el CISO de Aenor hasta que, a finales de septiembre de 2022, se incorporó a Isemaren como CIO y CISO.

Isemaren es una ingeniería especializada en el sector de la energía y la sostenibilidad que aporta soluciones globales abarcando todas las fases de los proyectos: Viabilidad, desarrollo, financiación, construcción y operación. ¿Ser CIO y CISO al mismo tiempo facilita tu trabajo? Dice Jesús Valverde que los riesgos son infinitos pero los recursos finitos, y explica que, en organizaciones donde la función de ciberseguridad es una de las que caen dentro del paraguas de TI, el presupuesto de ciberseguridad es sólo una de las partidas dentro del presupuesto de tecnología; a su modo de ver "el presupuesto de seguridad debe ser un presupuesto global de toda la organización. La ciberseguridad no está solo en las iniciativas que se lideran desde el área TIC, sino que tiene que ir asociada, por diseño y por defecto, a todos los procesos de la organización, y que los responsables de dichos procesos deben conocer el riesgo y que el presupuesto para mitigarlo".

En opinión de Jesus Valverde, "en un mundo ideal el CISO estaría en una posición de reconocimiento por la Dirección de la compañía en la que pudiese, si es necesario, decir que no a una iniciativa estratégica para el CIO / CFO / CHRO si esa iniciativa no está adecuadamente planteada o, en lugar de resolver riesgos de seguridad para la organización, y que los responsables de dichos procesos deben conocer el riesgo y que el presupuesto para mitigarlo".

ciberseguridadTIC

Tai editorial

ENTREVISTAS

En su día a día, Jesús Valverde trabaja “con una dirección está muy concienciada con la digitalización y con esa transformación digital, que obligatoriamente tiene que tener una componente de seguridad”, de forma que en todo lo que se está diseñando dentro de Isemaren “ese componente de seguridad tiene un peso específico y primordial”.

Cualidades

Respecto a las cualidades que debe tener un buen CISO, dice Jesús Valverde que tiene que ser muy buenos identificando y traduciendo los requisitos de seguridad exigidos en un pliego, un proyecto, o los objetivos estratégicos de la organización; tiene que ser capaz, añade, de visibilizar esos riesgos, “porque todo el mundo tiene claro el riesgo económico, pero el riesgo de ciberseguridad es más complejo de explicar y hay que ser capaces de hacer entender que una inversión para proteger la información de la empresa y de los clientes garantiza la continuidad de la empresa”.

> “No hay ninguna solución de seguridad que tal cual la pones a funcionar te proteja de todo sin necesidad de intervención humana”

Menciona también como otra buena cualidad del CISO el saber gestionar un equipo “y más en el campo de la ciberseguridad donde hay muy pocos profesionales y una escalada salarial que no todas las empresas pueden afrontar”.

Saber escoger

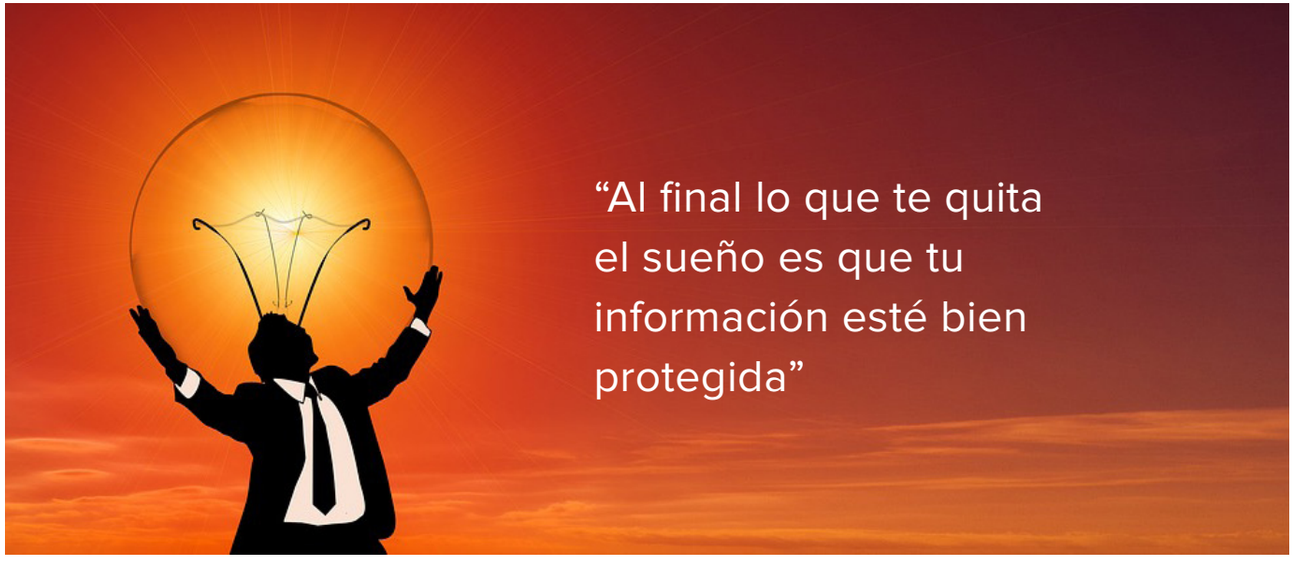
En un mercado tan saturado de fabricantes, soluciones y propuestas como es el de ciberseguridad, ¿cómo se escoge? “En un mundo ideal en el que tuvieses un presupuesto infinito, y ade-

ciberseguridadTIC

Tai editorial

más tuvieses unos equipos con una capacidad de proceso ilimitada, sería muy fácil", dice Jesús Valverde sonriendo. La realidad es otra. La realidad es que, de acuerdo con el presupuesto de la compañía, que debería estar alineado con el apetito de riesgo de la organización, "hay que ver qué soluciones van a integrarse mejor con las que ya tienes", porque, como bien dice el directivo de Isemaren "normalmente no se parte de cero. Siempre hay soluciones que ya están implantadas". Añade que son imprescindibles unos objetivos realistas y la realización de pruebas de concepto para ver cuál de las soluciones es la que mejor se integra y con cuál de ellas hay un mejor desempeño por parte del equipo de seguridad, porque "no hay ninguna solución de seguridad que tal cual la pones a funcionar te proteja de todo sin necesidad de intervención humana, una solución que sea total y absolutamente autónoma".

Para Jesús Valverde, lo ideal es tener un equipo que te dé soporte 24/7, o lo más cercano a ello, y unas herramientas que te permitan una alerta temprana, ver desviaciones de un comportamiento estándar para poder saber si lo que está ocurriendo es una amenaza o no, y si tienes que empezar a tomar acciones de contención o de mitigación.



Preguntado por la amenaza que le quita el sueño, responde Jesús Valverde que, como responsable de seguridad, lo que te quita el sueño no es una amenaza con nombre concreto, "sino que la información de tu empresa, o la información que tu empresa tiene de otras empresas o de los usuarios pueda verse comprometida". Menciona también de forma directa el llamado Fraude al CEO por el que se roba dinero engañando a los empleados tras el robo de credenciales que permiten al ciberdelincuente suplantar a un directivo para solicitar una transferencia a unos datos bancarios que hace que el dinero llegue a quien no debe.

Respecto al *ransomware* menciona Valverde que hoy en día el chantaje es doble, porque no sólo te cifran la información, sino que te amenazan con publicarla si no pagas. Y el hecho de pagar no garantiza el éxito "porque el descifrado

ciberseguridadTIC

puede fallar, o te pueden exigir el pago de nuevo dentro de seis meses, o un año, ya que los ciberdelincuentes se han hecho una copia de tu información". Esto hace que ahora "no solo tienes que ser capaz de recuperar tus sistemas y recuperar tu información para seguir trabajando, sino que además tendrías que haber sido capaz de detectar un tráfico de información anormal, con un origen o un destino que no es normal, a unas horas que no son normales, por un usuario que normalmente no accede a sus repositorios o no copia esa información porque por ahí te la pueden estar robando".

Continúa diciendo Jesús Valverde que "al final lo que te quita el sueño es que tu información esté bien protegida, que tus procesos sean robustos y que las personas que siguen esos procesos sospechen cuando algo se salga de lo normal". Incluir en la ecuación a las personas lleva al directivo a señalar que la seguridad "es algo transversal y que debe tenerse en cuenta en todos los procesos de la organización, incluso en aquellos en los que la componente tecnológica es más baja". En cuanto al papel del empleado en la seguridad empresarial, dice el CISO de Isemaren que "el usuario va a ser el eslabón más débil si el departamento de seguridad de la de la empresa no ha sido capaz de formarlo y de concienciarlo".

Tecnologías

Preguntado por las tecnologías de seguridad que deberían ser el mínimo imprescindible para cualquier empresa, menciona Valverde el sentido común, "algo que es gratis pero muy complicado de conseguir en las dosis necesarias".

Partiendo de esta base comenta el CISO de Isemaren que también es básico parchear, "algo que no requiere un esfuerzo desproporcionado" y que además debería hacerse "como mínimo una vez al mes, y si hay algo absolutamente urgente se tiene que buscar la ventana de cambio sin dilación alguna, o incluso notificar al cliente un paro extraordinario para ello. Lo van a comprender, porque ellos también estarán parcheando".

ENTREVISTAS

El tercer elemento requiere una inversión, y no es otra cosa que un antivirus de nueva generación que sea capaz de detectar comportamientos anómalos y detenerlos, "y que, en vez de funcionar de forma aislada, esté conectado a una consola en la que se reporten de forma automática esas incidencias y esté dotada de una cierta inteligencia artificial y capacidad de correlación". Sin saber ponerlo antes o después de lo mencionado, suma a la lista de imprescindibles una capa de seguridad para el correo electrónico y personal dedicado a la seguridad, "porque las herramientas de seguridad no lo hacen todo por sí solas".

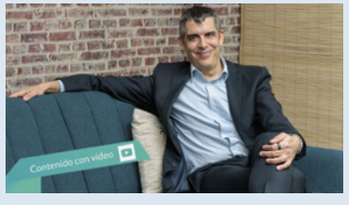
En cuanto a las tecnologías de futuro por las que apuesta el directivo, comenta Jesús Valverde que la consola centralizada a la que está reportando ese EDR que decíamos imprescindible, "no se quede ahí, sino que vayamos a un SIEM en el que además se estén recibiendo otros *inputs* del resto de herramientas de seguridad. Y que ese SIEM tenga unas ciertas automatizaciones para la respuesta".

En la parte de protección de la información, "que al final es uno de los activos principales", asegura Valverde que "hay fabricantes que han evolucionado el DLP de formas increíbles" para decir que las herramientas de Data Loss Prevention son un futuro esencial.

También considera que será relevante un área de *compliance* donde se establezcan las políticas de seguridad y donde haya unos documentos formalmente escritos y firmados por todos los trabajadores, para que las herramientas de seguridad puedan estar implantadas y habilitadas para funcionar con su máximo potencial y en caso de que haya un mal uso se puedan tomar medidas.

De carta a este año cree Jesús Valverde que, "tristemente, va a haber muchas noticias". Añade de que los ciberdelincuentes actúan como empresas que se dedican a atacar de manera profesionalizada tanto a grandes empresas como a pequeñas, y logran con ello beneficios que superan el PIB de muchos países. "Me gustaría creer que se lograráun cambio significativo en la percepción de gobiernos y empresas de que es necesario invertir en seguridad", comenta el directivo, que reconoce que ya se están dando muchos pasos hacia el camino correcto.

ENLACES DESTACADOS



One Identity: "El mercado se mueve hacia la convergencia de la identidad"

Metallic: "El *backup* se está incluyendo en las estrategias de ciberseguridad"

Netskope: “La prioridad es proteger los datos”

Dice Chris Andrews, SVP WW Sales en Netskope, que la mayoría de las amenazas provienen de la nube; que la mayor parte del tráfico está en el *cloud*, pero la mayor parte del gasto sigue centrada en el *on-premise*, y que empezar en el mundo del CASB fue una decisión inteligente para la compañía, que recientemente ha conseguido una ronda de inversión de 401 millones de dólares.

Chris Andrews,
SVP WW Sales en **Netskope**

“Nuestra misión desde el primer día fue tratar de convertirnos en una gran empresa en el espacio de seguridad en la nube”, dice Chris Andrews, vicepresidente de ventas a nivel mundial de Netskope, durante un breve encuentro mantenido con Ciberseguridad TIC en un reciente viaje a Madrid.

Hoy, poco más de diez años después, la compañía es un referente en el mercado de seguridad *cloud*. Hoy acumula 1.400 millones de dólares en varias rondas de financiación. Hoy tiene una de las redes de seguridad privadas más importantes del mundo para ofrecer sus servicios.

“Sentimos que se avecinaba un gran cambio en la forma en que los clientes implementaban o accedían a sus aplicaciones y datos”, y que eso “iba a requerir una nueva arquitectura de seguridad a la que los proveedores tradicionales iban a tener dificultades para adaptarse”, recuerda el directivo, añadiendo que ese cambio se convirtió en una gran oportunidad para la compañía.

Pensar a largo plazo ha permitido a la compañía seleccionar a los empleados, *partners* e inversores adecuados. Reconoce el directivo que se ha invertido mucho en la plataforma tecnológica, en la que ha habido mucho desarrollo propio gracias a los más de mil ingenieros que trabajan en Netskope, aunque también se han realizado adquisiciones puntuales, un total de

ciberseguridadTIC

Tai editorial

ENTREVISTAS

cinco, las dos últimas el año pasado: Sift Security (2018), New Edge Labs (2019), Trace Data (2021), Wootcloud (2022) e Infiot (2022).

CASB

Netskope llegó al mercado abanderando el mercado CASB (Cloud Access Security Broker) para la seguridad del *cloud*. Fue un segmento del mercado que no tardó en consolidarse, con grandes acuerdos de compra, como el de Adallom y Microsoft; McAfee y Skyhigh Networks; Blue Coat adquiriendo Perspecsys o Elastica, o Cisco haciéndose con CloudLock, por mencionar unas pocas.

> "El viaje inicial fue convencer a los clientes y ayudarles a comprender que en realidad ya estaban usando aplicaciones en la nube"

"Comenzamos con CASB porque no había otros proveedores de CASB", asegura Chris Andrews. Explica también que la visión de la compañía fue siempre la de convertirse en un jugador de seguridad destacado a largo plazo y que eso significa ofrecer servicios "no solo para las aplicaciones que están en la nube y los datos que están en la nube, sino también para las aplicaciones heredadas", porque, aunque cada vez hay más datos y más tráfico yendo a las aplicaciones basadas en la nube ahora que en onpremise, el modelo heredado tradicional "no va a desaparecer, y eso significa que se necesitan un grupo ampliado de capacidades de seguridad".

Empezar en CASB fue una decisión inteligente porque "el panorama competitivo estaba

ciberseguridadTIC

Tai editorial

> "La mayoría del tráfico ahora va a la nube, pero la mayor parte del gasto está aún más en *on-premise*"

en contra de empresas más pequeñas, como la nuestra. Los grandes gigantes estaban en el espacio de la seguridad o en el espacio de las redes, pero no estaban haciendo seguridad en la nube. Y aquellos que estaban tratando de hacerlo no lo estaban haciendo de manera efectiva. Comenzamos allí porque era efectico, pero siempre tuvimos el objetivo y la visión de expandirnos más allá".

Adoptando la nube

Hace años que las empresas están en la nube, aunque hubo quien tardó en darse cuenta o no sabían hasta qué punto la estaban utilizando. El viaje inicial, recuerda el directivo de Netskope, fue "convencer a los clientes y ayudarles a comprender que, en realidad, ya estaban usando aplicaciones en la nube de manera bastante significativa", lo que implicaba que sus datos estaban en la nube, y que no tenían visibilidad, ni control, ni seguridad contra amenazas o fuga de datos.

"Así que al principio fue: déjame mostrarte lo que estás usando y dónde están algunos de los puntos de riesgo"; eran los tiempos del CASB, pero luego se fue avanzando y ahora "la mayoría de los clientes son conscientes de que tienen muchas cosas en la nube, que tienen mu-

ciberseguridadTIC

Tai editorial

chos datos y muchas aplicaciones, algunas de las cuales son administradas y pagadas por la TI corporativa y otras que están a la sombra". El siguiente paso fue cómo ayudar a las empresas a habilitar de manera segura el uso de aplicaciones que tal vez no están administrando, asegura el directivo. Añade que ahora el discurso se entiende y que son los propios clientes los que piden ayuda para habilitar de manera segura las diferentes aplicaciones que tienen.

Explica también el directivo que la realidad es que "la mayor parte del tráfico ahora va a la nube, pero la mayor parte del gasto está aún en *on-premise*" y los clientes quieren saber cómo hacer esa migración a la nube de una manera segura y económicamente práctica. "Y tenemos muchas maneras de ayudarles a hacerlo", gracias al Business Value Services de la compañía, que ayudan a los clientes a "comprender dónde estarán los ahorros de costos con el tiempo y cómo los justificamos económicamente".

Hoy, la compañía es un jugador destacado en el mercado SSE, la evolución de SASE (Secure

Access Service Edge) que, acuñado por primera vez por Gartner en 2019, es un marco para diseñar arquitectura de redes y seguridad que incluye tanto las tecnologías requeridas como la forma en que esas tecnologías se integran y entregan no solo para igualar la flexibilidad y la economía del acceso a la nube, sino también para alinearse con la evolución de las prácticas de evaluación, adquisición e implementación. SSE es un término más reciente, descrito por Neil MacDonald y John Watts de Gartner en 2021 y que describe el conjunto de capacidades necesarias para lograr la seguridad que SASE describe, centrándose en los requisitos de la plataforma central, incluido el agente de seguridad de acceso a la nube (CASB), seguri-

ciberseguridadTIC

> "Siempre tuvimos el objetivo y la visión de expandirnos desde el CASB"

dad puerta de enlace web (SWG) y acceso a la red de confianza cero (ZTNA).

New Edge

New Edge uno de los diferenciadores más destacados de Netskope. Empieza explicando Chris Andrews que "la prioridad es proteger los datos", y que eso significa dos cosas: por un lado, protegerlos para que no se vayan donde no deben y, por otro, que nadie los robe. "Para brindar esa protección de datos podríamos haber ideado nuestra pila de tecnología y ponerla en uno de los grandes proveedores de servicios en la nube", pero lo que decidió Netskope fue "construir nuestra propia red de seguridad, que fuera la red de mayor rendimiento y menor latencia" de forma que el tiempo que se tarde en analizar un paquete de datos se mida en milisegundos. "Eso es New Edge", dice Andrews. Para el directivo de Netskope, "si vas a tener un coste asociado con la latencia, la mejor manera de ayudar a mitigarlo es colocar los centros de datos cerca de donde están los usuarios". New Edge cuenta con 65 centros de datos repartidos en todo el mundo, dos en España (Ma-

ChatGPT

Aprovechando el revuelo que ha generado ChatGPT preguntamos a Chris Andrews qué opina de este chatbot. Diciendo que quizá sea algo temprano saber qué va a ocurrir con la aplicación, plantea varias consideraciones. Por un lado, "podría ser una herramienta muy interesante y útil para muchos proveedores", ya que podría utilizarse para generar informes o análisis de clientes en entornos de vulnerabilidades, o saber cuántos usuarios tengo en China y qué servicios están usando; "algo tan simple como eso podría ser muy útil para construirlo en el producto para nuestro propio uso y para nuestros clientes".

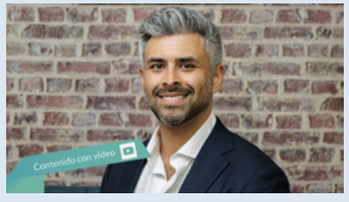
Por otro lado, Netskope se dedica a analizar aplicaciones y aplicarles un nivel de riesgo (bajo, medio o alto), y ChatGPT es una aplicación "que tendríamos que catalogar" porque los clientes nos preguntarán si es una aplicación segura para usar o cómo debe usarse de forma segura. "No digo que lo hagamos todavía, pero sería un ejemplo de hacia dónde iríamos", comenta.

Una tercera consideración es que, existiendo la posibilidad de que sea utilizada por los ciberdelincuentes, "nosotros como empresa podríamos ser un objetivo y tendremos que plantearnos cómo lo usará la gente en nuestra contra, o cómo podrían usarlo para explotar las vulnerabilidades con nuestros clientes".

drid Y Barcelona) a los que se unirán otros 15. Preguntado por la apuesta de Netskope por el mercado español, dice Chris Andrews que alrededor del 55 % de los ingresos de la compañía se generan en América del Norte; y del 30 % que se genera en EMA y Latinoamérica, "la mayor parte procede de Europa". Nos cuenta también Andrews que España es uno de los cinco o seis países principales "en los que tomamos la decisión temprana de invertir". No sólo hay dos centros de datos, sino que se ha invertido en ventas y es donde se ha implementado la sede europea de atención al cliente, además de abrirse, en Madrid, un centro de I+D, con la contratación de un equipo de ingenieros que contribuye al desarrollo de productos a nivel global.

ENLACES DESTACADOS

Stormshield: "Los fabricantes debemos hacer un esfuerzo por facilitar el uso y el acceso a tecnologías de seguridad"



Semperis: "La protección y resiliencia del Directorio Activo es la protección y resiliencia de negocio"

Vectra AI: “La visibilidad de la red es crítica”

A Eutimio Fernández le gustan los retos. Como responsable de Sourcefire le tocó evangelizar durante más de tres años sobre las bondades del IDS hasta que Cisco compró la compañía en 2013 por 2.700 millones de dólares. Integrado en Cisco, vivió la apuesta de la compañía de redes por el mercado de ciberseguridad que le llevó a iniciar una oleada de compras, desde la propia Sourcefire a ThreatGRIG, OpenDNS, Portcullis, Lancope, Jasper, Cloudlock, Duo Security o Sentryo. Siete años y medio después apostó por el mercado de ciberinteligencia, no maduro, asumiendo la dirección de ThreatQuotient. Desde hace algo más de dos meses apuesta por el mercado de NDR con la dirección de Vectra AI.

Eutimio Fernández,
Country Manager Iberia **Vectra AI**

Cada vez se necesitan más inversiones en ciberseguridad, y en todo tipo de tecnologías que permitan ver ataques cada vez más dirigidos e inteligentes. Nos lo cuenta Eutimio Fernández, un veterano del sector de la seguridad que acaba de asumir el liderazgo de Vectra AI en la región de Iberia.

Preguntado por cómo ve el mercado de ciberseguridad, dice también Eutimio Fernández que ahora están de moda los ataques basados en inteligencia artificial y en automatismos, y que “cada vez hay más concienciación y más inversión”, sobre todo si tenemos en cuenta que el tamaño medio de una brecha de seguridad son 3,6 millones de dólares.

En 2010 se fundaba Vectra AI con el objetivo de integrar inteligencia artificial especializada en ciberseguridad para hacer detección de ciberamenazas. La compañía se mueve con soltura en el segmento de NDR, o Network, Detection and Response, que no es otra cosa que “toda la detección de amenazas que se puede ver desde la red”, explica el directivo.

ciberseguridadTIC

Tai editorial

> NDR es un mercado que generará ingresos por valor de 4.829 millones de dólares hasta 2027, con un crecimiento medio anual del 23,46 %

Asegurando que la detección de amenazas en le red “es crítica”, recuerda Eutimio Fernández que hace unos meses Gartner publicó un informe en el que se hablaba de la necesidad de implantar un NDR por varias razones, la primera por la visibilidad que aporta; “la parte de visibilidad de la red es crítica, es una parte que falta y sin la que no se puede estar” asegura el nuevo responsable de Vectra AI.

Que la red sea la que comunica todo y donde todo sucede, y que el NDR sea capaz de detectar a los ciberdelincuentes que saben moverse por la red es lo que demuestra la importancia que tiene “implantar este tipo de soluciones, e implantarlas como las implantamos nosotros: con una inteligencia artificial que sabe interpretar lo que sucede en la red, y donde podemos incluso identificar ataques y problemas, aunque el tráfico vaya cifrado”.

NDR es un mercado que generará ingresos por valor de 4.829 millones de dólares hasta 2027, con un crecimiento medio anual del 23,46 %. Para muchos es “la última capa de protección, porque es desde donde se puede ver un problema cuando todo lo demás ha fallado”.

Preguntado sobre la propuesta de Vectra AI, nos habla Eutimio Fernández de una solución de detección de amenazas en red basada en inteligencia artificial. Asegura el directivo que se cuenta con “una IA muy entrenada para detectar las técnicas, tácticas y procedimientos de los atacantes”, que empieza a funcionar cuando

se implanta la solución y que va mejorando en el entorno del propio cliente. El gran diferencial, asegura "es que no solo hacemos esto en la red, sino que además estamos cubriendo la *cloud* (AWS, Azure...) o plaformas IaaS (Office 365, etc)" a través de conectores específicos para hablar con la plataforma mediante APIs sin instalar nada; no se olvida de la identidad, para muchos el nuevo perímetro de seguridad, ya que la tecnología de Vectra AI se puede integrar con plataformas de gestión de identidades; "la combinación de todo esto es lo que nos da una IA muy potente a la hora de detectar ataques, y una capacidad muy buena de hacer esto de una forma amplia y correlada. Podemos relacionar un problema que hemos visto en la red con un usuario que se ha dado de alta en aquel directorio activo o que está intentando hacer algo en mi Office 365, y todo esto llevarlo a conclusiones para que desde un SOC puedan generar una respuesta correcta".

Respecto a lo inteligente que es la inteligencia artificial de Vectra, comenta Eutimio Fernández que "el valor de una inteligencia artificial depende de cómo la entrenes. Y este es uno de nuestros grandes valores" porque la inteligencia de Vectra está muy entrenada en identificar problemas y detectar anomalías. "Donde nuestra tecnología brilla habitualmente es en grandes cuentas, donde somos capaces de identificar

> "El valor de una inteligencia artificial depende de cómo la entrenes"

Vectra AI se mueve con soltura en el segmento de NDR, o Network, Detection and Response

qué está pasando y cómo está pasando. Ahí es donde está el valor, en cómo tenemos entrenada a nuestra IA para hacer toda esta detección y llegar a conclusiones cuando los ataques son enrevesados y ejecutados por gente que sabe".

Cognito Platform

Vectra AI Cognito Platform es la joya de la corona de la compañía. Incorpora inteligencia artificial (IA), aprendizaje automático profundo y monitorización de tráfico. La plataforma tiene dos componentes principales, por un lado, los sensores de red, en formato hardware o virtualizados, que envían los datos a un cerebro, un dispositivo 1U donde entra todo el potencial de la IA.

¿Cómo afronta Eutimio Fernández este nuevo reto?

"Yo estoy encantado", responde Eutimio Fernández cuando le preguntamos, en un plano más personal, cómo afronta este nuevo reto.

Nos habla de las señales que ha visto a la hora de apostar por Vectra AI. En primer lugar un informe de la consultora Gartner que dice que una vez acabado de implantar el EDR, lo siguiente es el NDR. También ha visto cómo el canal, los *partners*, están apostando por tecnologías como la que ofrece Vectra, "y además he visto que es una necesidad. Las empresas están instalando el SIEM y el EDR y la visibilidad completa de toda la red es lo que les falta".

Añade con media sonrisa que compañías que no han hablado nunca de NDR, empiezan a hacerlo ahora, lo que significa "que hay mercado. Los clientes están viendo que hay una necesidad". Que esté dirigiendo una empresa que es líder en NDR, y los crecimientos que la compañía está logrando en otros países hace que Eutimio Fernández no vea "ninguna razón para no tener mucho éxito en los próximos años".

Preguntado por los casos de uso de la plataforma Cognito, explica Eutimio Fernández que son muchos, aunque el principal es atención y respuesta en un SOC. Es esta capacidad para detectar amenazas de forma dinámica y rastrearlas a medida que se expanden dentro de una red lo que da a Cognito la apariencia de un IDS, o Sistema de Detección de Intrusiones.

Para Eutimio Fernández es un IDS evolucionado hacia la detección y respuesta.

Otro caso de uso es la protección de entornos IaaS, "complementando plataformas como la que puede tener Microsoft. En este caso no competimos contra lo que ellos hacen porque ayudamos a los clientes a proteger estos entornos con inteligencia artificial, sin tener que instalar nada y dando una información que habitualmente las plataformas IaaS estándar no pueden dar".

Clientes

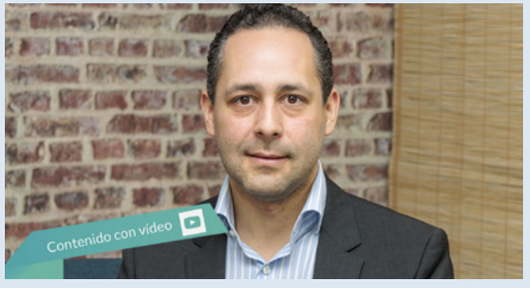
La primera impresión de Eutimio Fernández cuando se hizo cargo de Vectra AI fue que la tecnología tenía que ir a clientes que supieran de detección y respuesta, que tuvieran un SOC... "pero me estoy encontrando muchos clientes que no son grandes empresas pero que sí necesitan de herramientas que les den una visibilidad y un control de la red que hasta ahora no tenían".

Que el despliegue de la plataforma sea tan muy sencillo, junto con los servicios de MDR (Managed Detection and Response) es lo que está ayudando a llegar a un mercado de empresa mediana. La propuesta de Vectra es ofrecer una tecnología "que de por sí ya aporta una inteligencia muy superior a otras para detectar problemas, y lo complementamos con un servicio de MDR precisamente para acompañar a nuestros clientes", lo que permite a la compañía acceder "a mucho cliente mediano". CST

ENLACES DESTACADOS

Innovery: "Para este 2023 serán determinantes el Machine Learning, la Inteligencia Artificial y el Procesamiento del Lenguaje Natural"

Hillstone Networks: "La complejidad es el activo más caro"



"El paso de la criptografía tradicional hacia la protección con algoritmos post cuánticos requiere tiempo" (Utimaco)

ciberseguridadTIC

tai editorial

Fortra: “El esfuerzo de gestionar, administrar e integrar todos los productos de seguridad no es viable”

Los últimos años han sido intensos para Fortra. La que naciera en 1982 con el nombre de HelpSystems y como un proveedor de soluciones de software para la línea midrage de IBM, y con el objetivo de ayudar a las organizaciones a ser más seguras y autónomas, ha evolucionado hacia el mercado de la ciberseguridad a golpe de adquisiciones que han hecho que la oferta de soluciones y servicios, así como el tipo de clientes, haya cambiado. Hoy, la compañía es una empresa diferente, que aborda la ciberseguridad de frente y que quiere reflejarlo con un cambio de imagen y de nombre que ha convertido a la vieja HelpSystems en Fortra.

Paolo Capello,
General Manager International en EMEA de **Fortra**

La incursión de HelpSystems en la seguridad comenzó en agosto de 2008 con la adquisición de PowerTech, un proveedor de seguridad de red y herramientas de auditoría para el servidor IBM i. Siguió unos meses más tarde con la adquisición de Bytware, que ofrecía el único software antivirus para la plataforma de IBM. La compañía siguió acumulando adquisiciones, tantas que en 2016 había completado un total de quince compras, muchas en el entorno IBM i. Era solo el comienzo, desde 2018, la que fuera HelpSystems completó 17 adquisiciones más, muchas de las cuales pertenecían al mercado *cíber*.

ciberseguridadTIC

Tai editorial

ENTREVISTAS

Durante el año pasado Helpsystems se convirtió en Fortra. Esta iniciativa de *rebranding* es consecuencia del cambio en la trayectoria a la empresa, según nos cuenta Paolo Capello, responsable del negocio internacional de la compañía, que durante los últimos cinco años se ha ido centrando cada vez más en el mundo de la ciberseguridad. Ese giro, comenta el directivo en una entrevista en vídeo, se tenía que reflejar en el nombre, lo que les llevó a revisar "la forma en la que nos presentamos en el mercado" eligiendo Fortra como nombre de la empresa y buscando que el reconocimiento de la compañía se traslade al mundo de la ciberseguridad.

En los últimos dos años Fortra ha realizado una importante inversión en la adquisición de empresas, entre las que podemos nombrar a Digital Guardian, Phishlabs, Agari o Digital Defense. Preguntado sobre si el cambio de nombre y el inicio de esta nueva etapa supone paralizar de alguna manera este crecimiento inorgánico, asegura Paolo Capello que esta estrategia de compras ha demostrado ser una estrategia ganadora, por lo que se seguirá con las adquisiciones. En todo caso, explica, hay muchos factores que impactan en la rapidez con la que se pueden producir las adquisiciones y ahora mismo se trabaja en procesos de integración, "procesos importantes que requieren un esfuerzo relevante porque cuando se adquiere una compañía, el objetivo no es de mantenerla como un

> Fortra quiere simplificar la complejidad de la gestión de la seguridad, "algo más fácil de decir que de hacer"

Adquisiciones que convirtieron a HelpSystems en Fortra

- Septiembre 2022 — Ouftlank
- Abril 2022 – Terranova Security
- Marzo 2022 – Alert Logic
- Febrero 2022 — Tripwire
- Octubre 2021 — Digital Guardian
- Octubre 2021 — PhishLabs
- Mayo 2021 — Agari
- Mayo 2021 — Beyond Security
- Febrero 2021 — Digital Defense
- Enero 2021 — FileCatalyst
- Diciembre 2020 — Vera
- Junio 2020 — Boldon James
- Junio 2020 — Titus
- Marzo 2020 — Strategic Cyber
- Diciembre 2019 — ClearSwift
- Febrero 2019 — Core Security
- Febrero 2019 — SecureAuth
- Enero 2018 — Fox Technology

silo o un negocio que sigue su propio camino, sino construir un porfolio que ayude a las empresas a gestionar su propia seguridad de una forma más sencilla y de una manera integrada". Integrada es una palabra relevante en el mundo de la ciberseguridad. Se calcula en decenas el número de productos que las compañías tienen que gestionar para mantenerse a salvo de los ciberdelincuentes. "El esfuerzo de gestionar, administrar e integrar todos esos productos no es viable", asegura el directivo, añadiendo que la complejidad en la gestión de la seguridad es el principal problema al que se enfrentan las empresas, "y ahí es donde queremos estar nosotros, ayudando a reducir esa complejidad".

¿Cómo se reduce la complejidad? Por un lado con productos que ayuden "a que su implantación sea extremadamente más rápida y sencilla y, por otro, añadiendo servicios gestionados, que es de donde venimos como empresa".

> "Queremos ser aliados de seguridad. Disponer de todo lo necesario para que una empresa pueda gestionar su seguridad"

Entre los servicios prestados por Fortra destaca uno de MDR, o de detección y respuesta gestionada, procedente de la compra de Alert Logic, que "ayuda a todas esas empresas que no tienen suficientes recursos a gestionar su seguridad" porque, recuerda, no hay que olvidarse de lo que está pasando en el mercado: "no hay suficientes recursos, no hay suficientes personas con conocimientos de seguridad para poder responder a la demanda que hay".

Oferta

Como decíamos, Fortra quiere simplificar la complejidad de la gestión de la seguridad, algo

ciberseguridadTIC

que para el directivo es más fácil de decir que de hacer. ¿Cuál es la forma de hacerlo? Explica Capello que primero se tienen que mirar cuáles son las principales fuentes de vulnerabilidades y brechas de seguridad para después preguntarse por dónde hay que empezar, "y hemos identificado cuatro pilares", que son las cuatro unidades de negocio de la compañía: Infrastructure Protection & Data Security; Managed Security Services; Automation y, por último, IBM i Solutions.

En la parte de protección de infraestructuras y seguridad de los datos se incluye el control de vulnerabilidades; seguridad ofensiva; seguridad del correo electrónico, protección de datos, control del riesgo y transferencia segura de archivos. Explica Capello que no sólo se priorizan las vulnerabilidades, sino que se busca extender la seguridad más allá de la red, hacia la información, "para lo que necesitamos saber qué información gestionamos y cuál es el nivel y los protocolos de seguridad que tenemos que aplicar a esta información". Asegura Paolo Capello que se apuesta por definir políticas y límites en la forma en la que la información se puede compartir, se puede almacenar, se tiene que encriptar; "quién tiene que tener acceso, cuándo y por qué medio se puede compartir esa información".

Habla el canal. Also.

Eduardo Valenzuela es BDM en Also, el mayorisa de Fortra. En una breve conversación mantenida con Ciberseguriad TIC, nos cuenta que Data Secuity Suite es la propuesta de Fortra que más están moviendo en nuestro país. Se trata de una completa solución de protección de la información compuesta por herramientas de clasificación de la información a través de dos grandes marcas, Titus y Boldon James, compradas por Fortra en 2020; Prevención de pérdida de datos, o DLP, a través de Digital Guardian; y Gestión de derechos digitales, o DRM, que se afronta con Vera.

Este año se apuesta, además, por posicionar las propuestas de la compañía en torno al *pentesting* y las auditorías, con soluciones como Core Impact y Cobalt Strike. Tras confirmar que se están produciendo cambios y que se ha notado un incremento de la apuesta por el mercado español, comenta Eduardo Valenzuela que la presencia de la compañía es más habitual y se está potenciando en el mercado *enterprise* y administración pública.

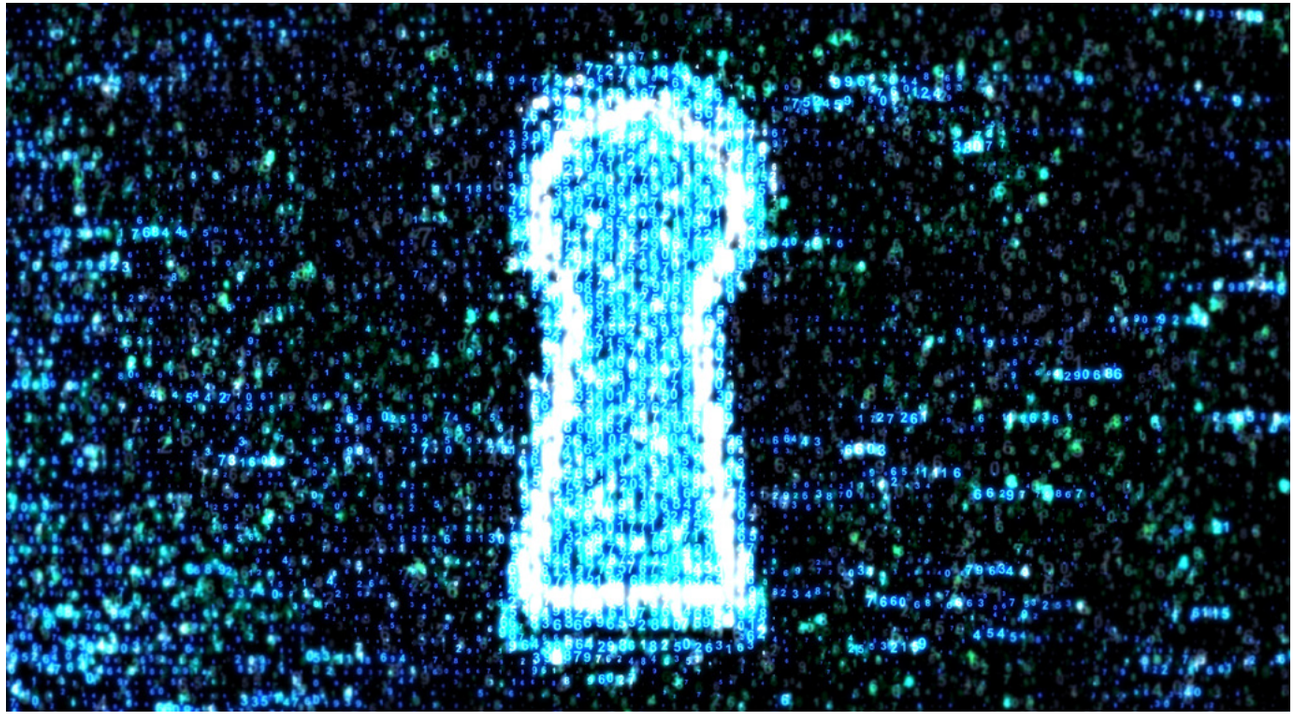
"La *security awareness* es un componente importante de nuestra oferta gracias a la compra de Terranova Security"

ciberseguridadTIC

Tai editorial

ENTREVISTAS

Dice también el directivo de Fortra que a esta parte de gestión de vulnerabilidades y seguridad ofensiva se añaden las personas porque "son el origen de cualquier tipo de campaña maliciosa". Esto hace que la *security awareness* sea "un componente importante de nuestra oferta" gracias a la compra de Terranova Security, una compañía experta en la generación de contenido, pruebas y simulaciones de campaña de *phishing* para medir realmente cómo de capacitados están los recursos de una empresa en identificar un ataque malicioso.



Los servicios de seguridad gestionados, o MSSP, es otra de las propuestas clave de la oferta de Fortra, lo que lleva al directivo a asegurar que con estos pilares "cubrimos probablemente el 85% de las amenazas de una empresa. Aquí es donde queremos jugar". Y esto, asegura Paolo Capello, "no significa que no queramos extender este *portfolio* para cubrir ese 15% de lo que hoy no disponemos y que seguramente en los próximos meses y años se irá sumando".

Fortra Application Hub

En 2022 se anunciaba el lanzamiento de HelpSystem One, que el proceso de *rebranding* de la compañía ha rebautizado como Fortra Application Hub. Explica el directivo que en la plataforma se ha realizado una fuerte inversión "porque no paramos de adquirir nuevos productos y nuevos servicios que tienen que revisarse e integrarse en la plataforma", donde ya se encuentran disponibles unos cuantos componentes y productos.

Fortra Application Hub es la gran apuesta de la compañía porque "reducir la complejidad solo se logra si todos los productos pueden trabajar juntos". ¿Se tiende entonces a que la oferta de la compañía sea la propia plataforma de productos y servicios? "Queremos ser aliados de seguridad. Disponer de todo lo necesario para

que una empresa pueda gestionar su seguridad", dice Paolo Capello.

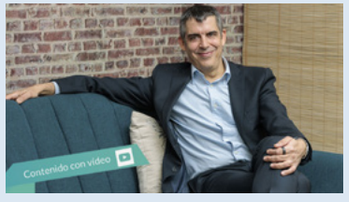
Añade el directivo que saber cuáles son los riesgos de una empresa y por dónde tiene que empezar ya no es un tema técnico, sino de negocio. La plataforma "tiene que ayudar a las empresas a decidir por dónde empezar y dónde de invertir su tiempo".

Mercado Español

A Fortra le falta reconocimiento en el mercado español. A pesar de que 2022 fue un buen año, y que el gran reconocimiento que la compañía tiene en Estados Unidos se empieza a extender en Reino Unido, Francia o Alemania, reconoce Paolo Capello que en nuestro país "estamos empezando". En todo caso, 2022 acabó con un incremento del 15% de la platilla.

Dice también el directo que es probable que las empresas conozcan los productos de la compañía y no a Fortra, "y ahí es donde creemos que hay una gran oportunidad". Viniendo de un mercado "muy *enterprise*", se apuesta por un *midmarket*, lo que, en opinión de Paolo Capello, debería ayudar a crecer en nuestros país".

ENLACES DESTACADOS



One Identity: "El mercado se mueve hacia la convergencia de la identidad"

Secure&IT: "La respuesta ante incidentes debe ser técnica, organizativa y jurídica"

Las cinco capacidades de ITDR que más necesitan las organizaciones

Explica Ray Mills, Director de Ventas en España para Semperis, que a medida que las empresas buscan protegerse más de las amenazas relacionadas con el directorio activo, las soluciones de ITDR diseñadas específicamente para defender los sistemas de identidad han subido rápidamente en la lista de prioridades de las empresas.

MÁS INFORMACIÓN

Espera lo mejor, planifica para lo peor

Francisco Arnau, vicepresidente de Akamai para España y Portugal, planea tres preguntas sobre *ransomware* que todo líder en seguridad debería poder responder.

MÁS INFORMACIÓN

¿Es la desconfianza digital la respuesta?

En esta tribuna de opinión Iona Simpson, CIO para EMEA de Netskope, asegura que las organizaciones que generan confianza digital tienen más probabilidad de experimentar un crecimiento, tanto en ingresos como en sus resultados.

MÁS INFORMACIÓN