ciberseguridadTIC
seguridad en informática y comunicaciones
Tai editorial
Año I Nº 4
Mayo 2023

IA, protagonista de RSAC 2023

Jesús Alonso Murillo, CISO de Sigma:
"La seguridad es negocio"

Eva Cristina Cañete, CISO de Unicaja Banco:
"Ahora lo que tenemos que proteger es a nuestro usuario y cómo se conecta"

José de la Cruz, director técnico de Trend Micro:
"El EDR está implementado sobradamente, pero se queda corto"

Avihai Ben-Yossef, cofundador y CTO de Cymulate:
"Nuestro valor es garantizar que nuestro cliente tenga un programa de ciberseguridad bien definido"

Mi primera RSA

500 empresas son muchas. Y aún habría que sumar alguna más. Son muchas si además tenemos en cuenta que todas pertenecen al mismo sector, el de la ciberseguridad. Siendo uno de los que más crece, genera 167.000 millones de dólares anuales, lo que apenas representa el 5,7 % del gasto total en IT.

500 empresas que asisten al evento de ciberseguridad más importante del mundo esperando que alguno de los 50.000 asistentes se pare a preguntar. Agradecidos si es un posible cliente, mejor si es un distribuidor o integrador con quien crear o fortalecer la relación. Porque ya sabemos que quien manda es el canal.

Aprecian la llegada de la prensa acreditada y miran de reojo a los que preguntan demasiado si no se identifican adecuadamente, vaya a ser que la competencia esté cogiendo ideas.

500 empresas que cubren todos los grandes *topics* del sector, desde el manido EDR al evolucionado XDR pasando por un *"AI Powered"* que se mira con media sonrisa. ¿Y qué más? Pues lo de siempre: seguridad de la cadena de suministro; del código, las API y las cargas de trabajo; el SSE también es tendencia, en competencia con el SASE; Zero Trust tiene un lugar destacado, así como la seguridad de los datos y las identidades, que nadie las olvide ni las eche de menos; la inteligencia de amenazas, gestión de vulnerabilidades y la formación y concienciación son también temas más que cubiertos en la conferencia.

500 empresas que ponen su ilusión y energía en apenas unos metros cuadrados de los kilómetros de pasillos que recorren asimilando nuevas marcas y nuevos logos. Sonríen y se acercan a contarte, pero no son tantos los que tienen la llave que les abra la puerta: ¿operas en el sur de Europa? ¿tienes previsto abrir oficina en España? Niegan mientras sonríen. Quizá algún día.

500 empresas que observan cuidadosamente el devenir de un mercado que ha iniciado su especial 'operación bikini'. Son muchas las empresas que hacen reajustes, no porque tengan malos resultados, ni siquiera porque esperen tenerlos. La burbuja creada por los fondos de inversión, que hace unos años iniciaron una carrera por fichar empresas de ciberseguridad que engordan para volver a poner en venta o animar a inversionistas, se está desinflando. El colapso de Silicon Bank paralizó las inversiones y las empresas empiezan a soltar lastre sin que, por el momento, se espere una caída de las ventas.

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

IA, protagonista de RSAC 2023

La última semana de abril San Francisco se convirtió en la capital de la ciberseguridad gracias a la RSA Conference. La que se iniciara en 1991 como una pequeña conferencia de criptografía volvía a reunir a decenas de miles de asistentes y más de 650 ponentes en torno a las últimas tendencias de ciberseguridad. La Inteligencia Artificial, que a finales del año pasado acaparó el interés de todo el mercado con el lanzamiento de ChatGPT, ha sido una de las grandes protagonistas de RSAC 2023.

EN PORTADA

El mundo del XDR, SASE, CSPM, BYOD, DDoS y tantas y tantas otras siglas que han ido conduciendo el mercado de ciberseguridad en los últimos años se ha rendido a dos letras: AI. ChatGPT nos ha robado el corazón. A algunos, hasta el aliento. Lo que hace más de una década nos dejaba entrever IBM Watson parece haberlo conseguido OpenAI, artífice del popular chatbot, en apenas unos meses.

Sobre lo que ocurrió con Watson ya se lo planteó Steve Lohr, del New Yort Times, en un artículo titulado *"What Ever Happened to IBM's Watson?"* y publicado en 2021, en el que el periodista asegura que IBM invirtió muchos millones para la promoción de Watson como un asistente digital benévolo que ayudaría a hospitales y granjas, así como a oficinas y fábricas. Según IBM los usos potenciales de Watson eran ilimitados, desde detectar nuevas oportunidades de mercado hasta abordar el cáncer y el cambio climático. Años después "Watson no ha rehecho ninguna industria. Y no ha mejorado la fortuna de IBM", escribía Steve Lohr.

Hoy, ChatGPT ha generado una auténtica revolución. Fue el 30 de noviembre cuando se lanzaba en Estados Unidos ChatGPT, un chatbot basado en IA y desarrollado por OpenAI, un laboratorio de investigación fundado por Elon Musk, Sam Altman y varios otros inversores en 2015. GPT es el acrónimo de Generate Pre-trained Transformer, un lenguaje desarrollado por OpenAI que puede comprender el lenguaje natural y generar textos fluidos, coherentes y similares a los humanos. Aunque no es perfecto, ChatGPT puede responder a una amplia gama de peticiones, incluida la explicación de temas complejos en términos sencillos, el resumen de párrafos largos y la generación de código python completamente funcional.

El lanzamiento de ChatGPT colapsó los servidores de OpenAI. En unos días el servicio tenía más

EN PORTADA

> “A medida que ingresamos en la era de la IA, nos enfrentamos a un nuevo desafío asombroso: los enfoques tradicionales de la identidad están muertos” Rohit Ghai, CEO de RSA Security

de un millón de usuarios, una cifra que Instagram tardó en conseguir tres meses y otras redes sociales varios años. Un par de meses después Microsoft anunciaba una inversión de 10.000 millones de dólares en OpenAI, quien a mediados de abril estrenaba un Bug Bounty Program que le ayude a detectar fallos en el código.

El interés que ha despertado ChatGPT, y más concretamente el uso de la Inteligencia Artificial en ciberseguridad, entró de lleno en el Moscone Center, donde muchas empresas mostraron cómo están utilizando la IA generativa en herramientas de seguridad.

Si bien durante el evento quedó clara la capacidad de la Inteligencia Artificial para fortalecer las arquitecturas de confianza cero o la gestión de identidades, está claro que los ciberdelincuentes también adoptarán la IA para aumentar

EN PORTADA

la sofisticación de los ataques de ciberseguridad. Es una espada de doble filo que requiere la atención de todo el mercado y que refuerza el lema del evento "*Stronger Together*". Por cierto, que el uso de la IA generativa en ciberseguridad será un mercado de 51.800 millones de dólares para 2028, según datos de MarketsandMarkets.

Google, por ejemplo, anunció Google Cloud Security AI Workbench, una plataforma de seguridad impulsada por Sec-PaLM, un modelo de lenguaje extenso (Large Lenaguaje Model - LLM) diseñado específicamente para casos de uso de ciberseguridad.

Explicaba la compañía que Sec-PaLM modifica el modelo PaLM existente de la organización y procesa los datos de inteligencia de amenazas patentados de Google junto con la inteligencia de primera línea de Mandiant para ayudar a identificar y contener la actividad maliciosa y coordinar las acciones de respuesta.

BigID, experta en gestión de datos, fue otra de las empresas que presentó soluciones de inteligencia artificial avanzada. La compañía anunciaba BigAI, una función impulsada por un modelo de lenguaje extenso (LLM) para mejorar la calidad de los entornos de datos, y el asistente virtual BigChat para responder preguntas sobre gestión de datos.

La compañía promete que BigAI puede generar automáticamente tablas de datos y nombres de columnas para mejorar la precisión, la interpretación, la agrupación de datos y la indexación. BigAI también puede dar automáticamente a los grupos de documentos mejores nombres y breves descripciones que resumen los documentos. Los títulos se generan en función de los documentos de cada grupo para mejorar la indexación y la búsqueda.

EN PORTADA

Recorded Future ha entrenado el modelo OpenAI GPT con una década de conocimiento experto de Insikt Group, la división de investigación de amenazas de la empresa

Tenable aprovechó la celebración de la RSAC para publicar un documento que describe el uso de la IA generativa para crear nuevas herramientas de investigación de seguridad. El informe, titulado "Cómo la IA generativa está cambiando la investigación de seguridad", destaca cuatro nuevas herramientas desarrolladas por el equipo de Tenable Research que crean eficiencias en procesos como ingeniería inversa, depuración de código, seguridad de aplicaciones web y visibilidad en herramientas basadas en la nube. Según el informe, las herramientas LLM, como ChatGPT, "están evolucionando a velocidad vertiginosa".

Las herramientas demuestran cómo Tenable Research está experimentando con aplicaciones de IA generativa como ChatGPT, y se han puesto a disposición del público para la comunidad de investigación de seguridad a través de un repositorio de GitHub. Una de estas herramientas, G-3PO, se explica en detalle *en este video* por parte de su creadora, Olivia Fraser.

Tras publicar, a primeros de año, un informe que ayudó a confirmar que ChatGPT estaba siendo utilizado por los ciberdelincuentes. **Recorded Future** anunciaba, poco antes de dar comienzo la RSAC, que había entrenado el modelo OpenAI GPT con una década de co-

Large Language Model (LLM) marca la diferencia

Los Modelos de Lenguaje Extenso, o LLM, representan un gran avance en IA. Son programas informáticos para el procesamiento del lenguaje natural que utilizan aprendizaje profundo y redes neuronales para reconocer, resumir, traducir, predecir y generar texto y otro contenido. Y aquí es donde radica la diferencia, porque el aprendizaje automático, que antes se esperaba que manejara solo tareas mundanas, ha demostrado ser capaz de realizar trabajos creativos complejos.

Los tamaños de los LLM han aumentado 10 veces cada año durante los últimos años y, a medida que estos modelos crecen en complejidad y tamaño, también lo hacen sus capacidades. ChatGPT es un large language model (LLM), que quizá sea el más conocido, pero no es el único. Otra gran iniciativa de código abierto es BLOOM del proyecto BigScience, un consorcio de aproximadamente mil investigadores voluntarios de IA. Otros LLM incluyen Bard y LaMDA de Google, y NeMo de Nvidia.

nocimiento experto de Insikt Group, la división de investigación de amenazas de la empresa, y en los conocimientos de su Recorded Future Intelligence Graph.

Recorded Future recopila y estructura automáticamente datos relacionados con adversarios y víctimas a partir de texto, imágenes y fuentes técnicas, y utiliza procesamiento de lenguaje natural y aprendizaje automático para analizar y mapear información en miles de millones de entidades en tiempo real.

Aseguraba la compañía durante el congreso de ciberseguridad más importante del mundo que con Recorded Future AI las empresas “pueden obtener evaluaciones automáticas de su panorama de amenazas en tiempo real y tomar

> Está claro que los ciberdelincuentes también adoptarán la IA para aumentar la sofisticación de los ataques de ciberseguridad

medidas inmediatas”. De manera específica la compañía aseguraba que los analistas podrían dedicar menos tiempo a buscar, resumir y redactar informes, mientras que los ejecutivos deberían obtener informes y análisis en tiempo real de nivel de analista, según Recorded Future.

SentinelOne presentaba Purple AI, una IA generativa dedicada a la búsqueda, análisis y respuesta de amenazas. Purple AI 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

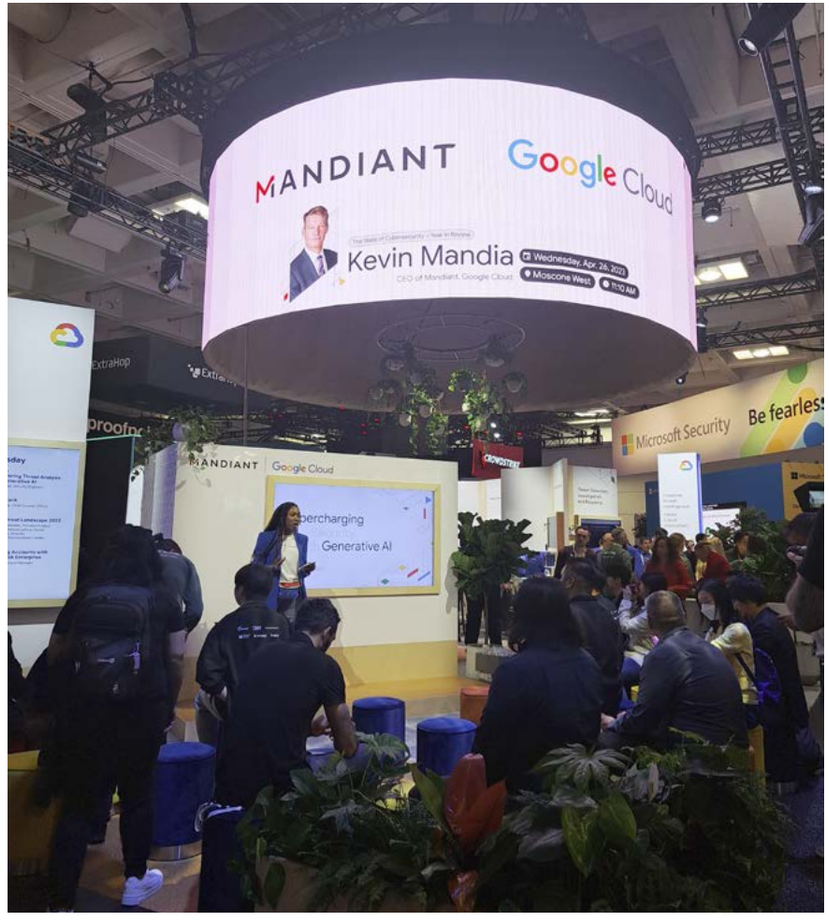
EN PORTADA

Google Cloud Security AI Workbench es una plataforma de seguridad impulsada por Sec-PaLM, un LLM diseñado específicamente para casos de uso de ciberseguridad

inteligencia artificial que puede ayudar a identificar, analizar y mitigar las amenazas mediante mensajes conversacionales y diálogos interactivos.

Con Purple AI, los analistas pueden obtener respuestas rápidas, precisas y detalladas a cualquier pregunta, en cualquier idioma, algo que requeriría horas de investigación y múltiples consultas, sin mencionar años de experiencia, para obtener una respuesta, aseguraba la compañía.

La nueva herramienta de búsqueda de amenazas, que utiliza LLM (large language model) se ofrecerá inicialmente como un complemento de la plataforma Singularity Skylight y ahora se encuentra en versión preliminar limitada.



Bajo la sombra de GPT, **Veracode** anunciaba Veracode Fix, una solución impulsada por IA que sugiere correcciones a fallas encontrados en el software y ayudar a los desarrolladores a implementar un código seguro.

Veracode Fix utiliza un motor pre entrenado generativo, el mismo tipo de modelo de inteligencia artificial que utiliza el chatbot ChatGPT de OpenAI, para proporcionar sugerencias de código automáticas sobre cómo remediar los fallos de seguridad descubiertas después de escanear el software. Ha sido entrenado utilizando la base de conocimientos ya existente de Veracode de más de 140 billones de líneas de código y sus 17 años de investigación en seguridad.

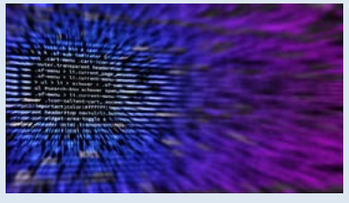
EN PORTADA

El interés que ha despertado ChatGPT entró de lleno en el Moscone Center

Rohit Ghai, CEO de **RSA Security**, dedicó parte de su discurso de apertura, titulado *The Looming Identity Crisis*, a hablar de inteligencia artificial. "A medida que ingresamos en la era de la IA, nos enfrentamos a un nuevo desafío asombroso: los enfoques tradicionales de la identidad están muertos. Esta nueva era exige que nuestro sector responda preguntas fundamentales sobre nuestro papel y capacidad para asegurar la identidad a medida que evoluciona", decía, para reconocer, además, que la IA tendrá un gran impacto en la industria de la seguridad: "Debemos aceptar que muchos trabajos desaparecerán, muchos cambiarán y algunos se crearán". Entre los que desaparecerán están aquellos que una inteligencia artificial pueda hacer más rápido y mejor que los humanos, y las capacidades que se van añadiendo a estas AI nos dice que esas tareas cada vez serán más.

Pero también generará nuevos trabajos en ciberseguridad, como la protección de los datos que la IA extrae de los ataques y garantizar que las herramientas de la IA funcionen de manera ética. CST

ENLACES DESTACADOS



OpenAI lanza un Bug Bounty Program para ChatGPT

Microsoft invierte 10.000 millones en OpenAI, el creador de ChatGPT

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

“Ahora lo que tenemos que proteger es a nuestro usuario y cómo se conecta”

Dice Eva Cristina Cañete, CISO de Unicaja Banco, que la tecnología ayuda, pero debe estar acompañada de una buena organización de la seguridad, de unos procedimientos y unos procesos bien definidos; que la perseverancia es una de las cualidades que debe tener un buen CISO y que hay que recordar que no hay presupuestos ni recursos ilimitados.

Eva Cristina Cañete, CISO de **Unicaja Banco**

Estando en el mundo de la administración de sistemas le tocó implementar la Ley de Protección de Datos. Así fue como Eva Cristina Cañete empezó a adentrarse en el mundo de la ciberseguridad. Después, “a base de ir participando en diferentes proyectos que requerían ampliar los conocimientos en ciberseguridad, me fue gustando cada vez más y aquí estoy”, explica la directiva, que ejerce como CISO de Unicaja Banco desde hace más de cuatro años y acumula más de diez en el mundo de la ciberseguridad.

Sobre las cualidades que debe tener un buen CISO, habla Eva Cristina Cañete de “perseverancia”, además de “sensibilidad hacia las necesidades del negocio”, lo que además exige tener capacidad de llevar el mensaje de ciberseguridad a los órganos de gobierno de la empresa.

Planteamos a Eva Cristina Cañete si la seguridad ha dejado de percibirse como un gasto a favor de una inversión. Responde comentando que, “en realidad, es difícil ver la monetización del gasto en que te tienes que incurrir para securizar tu entorno y tu empresa”, pero si se tuviera en cuenta el ahorro de costes que te puede suponer respecto a tener que recuperarte de una brecha, “sí que podríamos considerarlo casi una inversión”. En todo caso, añade, “todavía existe mucha más tendencia a pensar que es un gasto”.

ENTREVISTAS

> "Todos los días fracasamos un poco y todos los días tenemos un poco de éxito"

En un mercado tan saturado de fabricantes, soluciones y propuestas, ¿cómo se escoge una solución u otra? "A la hora de seleccionar una herramienta, tienes que pensar en el momento en el que te encuentras, tus circunstancias y cuál es la necesidad que quieres cubrir", responde la CISO de Unicaja Banco. Añade que a veces no se tiene que ir a una solución cara o que sea la que tenga más prestaciones, "sino la que en ese momento y a medio plazo cubra tus necesidades". Dice también la directiva que el mundo está cambiando constantemente, igual que las necesidades, y que debe tenerse la visión de que "las herramientas o soluciones que busques no se ajusten a modas o a lo que el mercado en ese momento esté intentando comercializar".

No hay una amenaza concreta que quite el sueño a Eva Cristina Cañete, sino la materialización de una amenaza que implique un grave problema; "que no tengamos la capacidad de recuperación y de resiliencia suficiente como para que el incidente se quede en las mínimas consecuencias posibles. Quizás para mí esa es la máxima preocupación", asegura.

Seguimos hablando con la CISO de Unicaja Banco y le preguntamos si en ciberseguridad todo es tecnología y qué peso cree que tiene la concienciación del usuario, los procesos... "Soy de la opinión de que la tecnología ayuda, pero debe estar acompañada de una buena organización de la seguridad, de unos procedimientos y unos procesos bien definidos que permitan

> "Hemos aprendido a movernos en el mundo físico, pero nadie nos enseña a movernos en el mundo digital"

engranar cada uno de los elementos y que te permitan gestionarla de una forma adecuada, porque también hay que recordar que no hay presupuestos ni recursos ilimitados".

"No existen las balas de plata", dice Eva Cristina Cañete cuando le preguntamos por el peso que una correcta concienciación del usuario tiene en la ciberseguridad. Opina que "no va a tener una repercusión absoluta en tu estrategia de seguridad, pero es imprescindible. A tus usuarios los tienes que formar y les tienes que concienciar, porque el mundo digital no es un mundo natural. Hemos aprendido a movernos en el mundo físico, pero nadie nos enseña a movernos en el mundo digital".

Respecto a la Inteligencia Artificial, "estamos bastante confundidos", dice la CISO de Unicaja Banco. Explica que se trata de una disciplina que todavía está muy incipiente y que ofrecerá "muchas posibilidades de llegar a alcanzar objetivos en el plano de la seguridad que ahora no tenemos, pero no podemos olvidar que al final, detrás de una inteligencia artificial, hay una inteligencia humana que ha programado, que ha desarrollado y que necesita de ese aprendizaje para poder dar sus frutos". Añade que no hay que olvidar la doble vertiente que tiene la inteligencia artificial: la puedes utilizar para mejorar la seguridad, pero también para delinquir; "y ahí es donde quizás tenemos que poner el foco. En ver cómo va a ser utilizada por los delincuentes para atacar".

Tecnología, fracasos y normativa

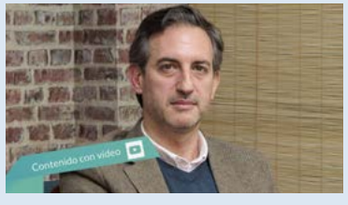
Preguntada por lo que considera imprescindible en ciberseguridad, comenta Eva Cristina Cañete que el paradigma de la protección ha

cambiado. “Ahora lo que tenemos que proteger es a nuestro usuario y cómo se conecta”, asegura, añadiendo que esto significa que “las tecnologías que son necesarias, tanto ahora como a futuro, son todas aquellas que nos permiten proteger al usuario, esté donde esté y accediendo a lo que tenga que acceder”.

Dice la CISO de Unicaja Banco cuando planteamos qué le puede hacer fracasar como CISO que “todos los días fracasamos un poco y todos los días tenemos un poco de éxito”. Añade que también puede afectar de forma negativa no contar con el apoyo interno necesario. Se trata de una cuestión que depende bastante “del grado de concienciación que tenga tu alta dirección y lo accesible que sea”, por lo que, en realidad, solo podría considerarse un fracaso del CISO si, teniendo acceso a la alta dirección, “no consigues transmitir la necesidad que tiene la empresa de protegerse”.

> “Todavía existe mucha más tendencia a pensar que la ciberseguridad es un gasto”

ENLACES DESTACADOS



IBM Cybersecurity Services: “Ni la inteligencia artificial ni la automatización son magia”

BeDisruptive: “Ser disruptivos no es hacer las cosas totalmente opuestas, es hacerlas un poco diferentes. Y en esa pequeña diferencia es donde está el valor que aportamos”

“La seguridad es negocio”

Dice Jesús Alonso Murillo, CISO de Sigma, que la tecnología que se adopte tiene que acompañar a las necesidades del negocio; que el MFA, o múltiple factor de autenticación, es imprescindible porque no podemos confiar solo en la contraseña; y que lo que le haría fracasar como CISO es no haber sido capaz de cambiar la cultura de ciberseguridad de los empleados.

De joven era la persona a la que se llamaba para instalar el sistema operativo, arreglar el ordenador, recuperar móvil o acceder a algún tipo de información. De ahí a adentrarse en el mundo de la ciberseguridad hay un gran paso que ha llevado a Jesús Alonso Murillo a convertirse ser el CISO de Sigma, la empresa matriz de Campofrío.

Asegura que, en el mundo hiperconectado en el que vivimos, los CISO se enfrentan a multitud de retos; “la digitalización es muy buena, y la necesitamos, pero la seguridad tiene que ser parte de ese proceso”, asegura el directivo. Cuando le preguntamos por las cualidades que debe tener un buen CISO, recuerda que el responsable de seguridad ya no es esa persona que trabaja en el sótano configurando proxys, firewalls y antivirus “sino que es una figura ejecutiva, una figura de negocio”, y como tal, “entre sus cualidades debe saber hablar de negocio y ser parte del negocio”, porque a día de hoy, “la seguridad es negocio”.

> “El MFA es imprescindible porque no podemos confiar solo en la contraseña”

Jesús Alonso Murillo, CISO de **Sigma**

> "La tecnología tiene que acompañar a las necesidades que tenemos como responsables de ciberseguridad"

Sobre la Guerra de Ucrania dice que ha habido un impacto desde el punto de vista que de ciertos grupos de ciberdelincuentes actúan con más impunidad, si cabe. También se ha observado un aumento de movimientos hacktivistas, así como de ataques de denegación de servicio y ransomware, sobre todo en sectores esenciales.

Saber escoger

El de seguridad es un mercado fragmentado en el que hay centenares de empresas. A la hora de escoger, ¿en qué se fija Jesús Alonso Murillo? Asegura que la tecnología "tiene que acompañar a las necesidades que tenemos como responsables de ciberseguridad", y asegura que la mayoría de las empresas tienen muchas tecnologías que difícilmente interactúan entre ellas. A la hora de optar por una solución, u otra, el directivo se fija "en que se puedan integrar, que haya unificación entre ellas y que nos alerte solo de lo que sea necesario".

Preguntado por la amenaza que le quita el sueño, menciona "aquellas que tienen que ver con lo que tú no controlas, que son las cadenas de suministro", un problema que se ha incrementado en los últimos tiempos. Recuerda el responsable de seguridad que "tú pones los mecanismos de protección para evitar que terceros accedan de una manera insegura, pero no puedes llegar a ese tercero más allá de las revisiones o contratos que puedas hacerles".

La tecnología EDR, NDR, XDR... "llamémosla

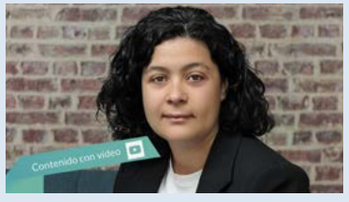
> "La digitalización es muy buena, y la necesitamos, pero la seguridad tiene que ser parte de ese proceso"

como queramos" es una de las que Jesús Alonso Murillo considera indispensable gracias a la capacidad de telemetría que ofrecen y que además permiten "que tengamos información de lo que está pasando en los dispositivos y en nuestra red". También imprescindible es el MFA, o múltiple factor de autenticación porque "no podemos confiar solo en la contraseña".

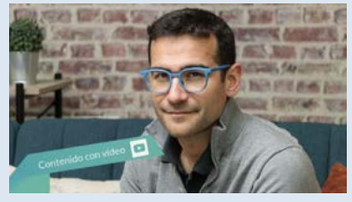
De cara al futuro habla de poder proteger los mecanismos de inteligencia artificial, así como las tecnologías que permitan predecir, a través de análisis de datos, "de dónde puede venir el próximo ataque".

"No haber sido capaz de cambiar la cultura" es una de las razones que le haría fracasar como CISO, dice Jesús Alonso. Explica que todos debemos ser capaces de ver que la seguridad es importante en nuestras vidas, no solo en nuestro trabajo diario, y que "si no has sido capaz de hacer cambiar esa cultura personal y profesionalmente, por muchos mecanismos tecnológicos que pongas, vamos a estar perdidos". CST

ENLACES DESTACADOS



Enthec: "Las compañías están mucho más abiertas de lo que ellas mismas pueden suponer"



Redtrust: "Hay que fortificar el acceso a la identidad digital"

“El EDR está implementado sobradamente, pero se queda corto”

Habla José de la Cruz, director técnico de Trend Micro, de la profesionalización de los ciberdelincuentes como uno de los grandes retos a los que se enfrentan las empresas; dice que lo que demandan los clientes son soluciones, y que el nuevo perímetro lo conforma una triada compuesta por las identidades, los *endpoints*, y los servicios cloud.

José de la Cruz, director técnico de **Trend Micro**

Profesionales y eficientes. Así son los ciberdelincuentes y por eso son uno de los mayores retos a los que se enfrentan las empresas cuando se habla de ciberseguridad. Esa profesionalidad se demuestra en su capacidad para atacarnos por todos lados, a través del correo electrónico, el *endpoint*, la cadena de suministro, los servicios

ciberseguridadTIC

Tai editorial

ENTREVISTAS

cloud, el mundo OT...; su capacidad para diversificar el tipo de ataque, desde un día cero a utilizar vulnerabilidades expuestas o elementos de la cadena de suministro; y lanzar ataques dirigidos y persistentes, no ya solo contra las empresas grandes, sino también contra empresas más pequeñas. Todo esto nos lo cuenta José de la Cruz, director técnico de Trend Micro, una compañía fundada en 1988 en Los Angeles por Steve Chang, su mujer, Jenny Chang, y su hermana, Eva Chen, y que, como algunas otras, nació en el mercado de antivirus y ha ido ampliando su oferta hasta convertirse en un referente de la seguridad *cloud* y el punto final.

"Lo que demandan los clientes son soluciones, bien en forma de servicios o en forma de productos", dice José de la Cruz, añadiendo que las soluciones deben ayudarles a hacer frente a los ciberataques "de una manera eficiente, escalable y sostenible". Sobre si tendencias como Zero Trust, SASE o XDR están cambiando las reglas del juego, si están ayudando a las empresas a hacer frente a los ciberataques, dice

"Trend Micro One es una plataforma diseñada para hacer frente a los ataques modernos"

el directivo que "al menos lo está moldeando". Explica que el nuevo perímetro lo conforma una triada compuesta por "las identidades que tú utilizas para acceder a servicios, los *endpoints* con los que trabajas, y los servicios *cloud* donde se alojan esos servicios o esos datos que tú manejas". Para proteger el nuevo perímetro tenemos modelos como Zero Trust que establece tres cosas: El principio de mínimos privilegios, el "*never trust, always verify*", y asumir la brecha, explica José de la Cruz, añadiendo que, en base a estos principios, lo que hace Trend

La solución de Virtual Patching de Trend Micro convirtió la debacle de Log4Shell en un caso de éxito para la compañía

Micro es analizar la postura de seguridad para saber si estás cumpliendo con lo básico, como puede ser tener usuarios administradores que no tienen que serlo, tener vulnerabilidades sin parchear, o credenciales que están siendo expuestas a Internet; "antes de proteger, controla lo básico, y contrólalo de manera recurrente. Eso es importante".

Analizar la postura de seguridad permite detectar las debilidades para anticipar lo que puede llegar a ocurrir, "y eso eleva mucho el nivel de seguridad. Y fíjate que todavía no estamos protegiendo", asegura el directivo.

SOCs y XDR

Sobre la evolución del EDR al XDR, dice José de la Cruz que "el EDR está implementado sobradamente", pero en un contexto en el que nos atacan por todos lados con técnicas diferentes, "el EDR se queda corto porque solo cubre el *endpoint*, y también tenemos que cubrir las redes, los servicios cloud... El XDR es el que te va a ayudar a cubrir esos vectores de ataque", y va a generar la correlación que necesitas para que te des cuenta de qué está ocurriendo y si te están atacando. Asegura también José de la Cruz que el XDR tiene una particularidad que lo hace único: "genera una única alerta", lo que permite a las empresas "detectar el ataque de manera temprana antes de que pase nada. Por ese motivo, XDR aplica a todo el mundo".

Preguntamos también al director técnico de Trend Micro por la evolución el mercado de SOC. "Todo el mundo tiene uno, o necesita uno", asegura, pero vuelve al comienzo de la

Resumen anual de ciberseguridad de 2022

A primeros de marzo Trend Micro lanzaba al mercado su 'Resumen anual de ciberseguridad de 2022'. Sobre los resultados de informe destaca José de la Cruz algunos datos, como la desaparición del grupo de ciberdelincuentes Conti como consecuencia de la guerra de Ucrania, que también ha generado muchos ataques a nivel mundial.

Desde el punto de vista estadístico, "hemos bloqueado 147 billones de amenazas, de las que un 54% llegan a través del correo electrónico". También se han incrementado las detecciones relacionadas con el mundo OT y contra los entornos sanitarios.

"Otra cosa que me ha llamado la atención es que las tácticas y técnicas de ataque más detectadas están relacionadas directa o indirectamente con identidades", lo que demuestra más allá de toda duda que las identidades son un foco de atracción de los ciberdelincuentes.

Finalmente destaca el director técnico de Trend Micro que la vulnerabilidad más explotada este año 2022 ha sido Log4Shell.

conversación: antes de implementar tecnologías vamos a tener un análisis de la postura de seguridad, vamos a tener herramientas o visibilidad de lo que está ocurriendo. Sobre los iSOC, comenta que se están poniendo de moda por los entornos industriales, "pero yo soy partidario de que hacer la guerra por tu cuenta no tiene sentido. Y más hoy en día".

Recuerda que hace años el mundo OT no quería saber nada del mundo IT ni de lo que lo rodeaba; ellos tenían sus propias tecnologías, pero eso hoy en día ha cambiado. "Lo que hacen las empresas es optimizar, interconectar y si hacemos un análisis individual con un ISOC, que está específicamente asociado al mundo OT, nos perdemos parte de la foto. Yo soy partidario de

> "Antes de proteger, controla lo básico, y contrólalo de manera recurrente"

tener la foto completa", asegura. Y lo hace con el peso que le da que su compañía sea pionera en proteger el mundo industrial y lleve muchos años invirtiendo en OT con el objetivo de que "una empresa pueda monitorizar con una única consola, que es la división ONE".

Parcheando

Otro de los mercados en los que brilla Trend Micro es en el mundo de la detección e investigación de vulnerabilidades. La solución de Virtual Patching de la compañía es un referente en el sector que convirtió la debacle de Log4Shell en un caso de éxito para la compañía.

El impacto de Log4Shell fue mundial y contra todo tipo de organización en todas las indus-

trias. Es un fallo difícil de encontrar, pero fácil de explotar, que pone en riesgo a cientos de millones de aplicaciones, bases de datos y dispositivos basados en Java. Además, remediar esta vulnerabilidad resultó no ser un proceso simple y de una sola vez. Los clientes de Trend Micro no se vieron afectados.

El número de vulnerabilidades no deja de crecer y los retos a los que las empresas deben hacer frente son los de siempre: falta de recursos o no poder parchear sistemas legacy que a veces son críticos para el negocio. En todo el tema de la gestión de vulnerabilidades vuelve José de la Cruz al principio: analizar la postura de seguridad, "porque si puedes identificar cuáles son tus activos críticos, vas a acometer

la labor de una manera diferente", dice José de la Cruz explicando que, si no puedes parchear el CMS, intentarás tenerlo totalmente aislado.

Sobre el parcheado virtual dice el directivo que es una tecnología diferencial de Trend Micro que ayuda a reducir la superficie de ataque y darle tiempo al cliente para que pueda parchear, "si es que puedes, porque hay veces que no se puede".

"Trend Micro One es una plataforma diseñada para hacer frente a los ataques modernos. Para eso ha nacido", responde José de la Cruz cuando le preguntamos por esta propuesta. Explica que Trend Micro tiene una posición privilegiada en el mercado gracias a una oferta que cubre todos los vectores. "Y precisamente lo que queremos hacer es ofrecer a nuestros clientes una plataforma unificada donde vas a poder detectar, analizar la postura de seguridad, identificar cuáles son los riesgos antes de que representen un ataque, y proteger todos los vectores de ataque". CST

ENLACES DESTACADOS

Trend Micro: La postura de seguridad ya forma parte de las negociaciones con clientes potenciales y proveedores

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

“Nuestro valor es garantizar que nuestro cliente tenga un programa de ciberseguridad bien definido”

Hace siete años Cymulate fue uno de los pioneros en el mercado de Breach and Attack Simulation (BAS), ofreciendo tecnología para automatizar las simulaciones de ataque lanzadas contra los controles de seguridad y optimizarlas. Extended Security Posture Management (XSPM) es la próxima generación de las herramientas (BAS) y de Validación Continua de la Seguridad. Sobre esto y otras cosas hablamos con Avihai Ben-Yossef, co-fundador y CTO de Cymulate.

Avihai Ben-Yossef, co-fundador y CTO de Cymulatee **Cymulate**

No queda mucho para que Cymulate, la empresa israelita que hace unos años se adentró en el mercado español para convertirse en un caso de éxito, se convierta en una empresa pública. Su salida a bolsa está programada para un futuro no muy lejano después de acumular 141 millones de dólares en cinco rondas de financiación, la última una Serie D en septiembre de 2022 que recogió 70 millones de dólares.

La compañía, que nació al amparo del concepto BAS (Breach and Attack Simulation), ayuda a las empresas a verificar, de manera continua, su postura de ciberseguridad a través de una propuesta a la que se refieren como Extended Security Posture Management.

Durante la #RSAC de San Francisco, Ciberseguridad TIC tuvo la oportunidad de reunirse con Avihai Ben-Yossef, quien en 2016 y con 26

ciberseguridadTIC

Tai editorial

ENTREVISTAS

años cofundó Cymulate para transformar la forma en que las empresas realizan pruebas de seguridad. Decía Avihai Ben-Yossef que "las empresas tienen mucho que proteger", algo que afrontan añadiendo capas de seguridad. Pero "cuantas más capas de seguridad tienen, cuanto más grande es su entorno, más difícil se vuelve realmente administrar la seguridad. Es entonces cuando entienden que necesitan administrar continuamente esa postura de seguridad o esa gestión de la exposición".

De forma que las tecnologías de simulación de ataques y brechas de seguridad (BAS) se han quedado cortas. Las organizaciones necesitan ir más allá de la validación y los conocimientos de los controles de seguridad. Extended Security Posture Management (XSPM) es la próxima generación de las herramientas de Simulación de Infracciones y Ataques (BAS) y Validación Continua de la Seguridad, porque "la validación integral y de extremo a extremo es imprescindible", asegura el CTO de Cymulate.

La plataforma Extended Security Posture Management de la compañía, que aprovecha su tecnología y capacidades nativas de seguridad ofensiva, incorpora cuatro pilares fundamentales unidos con análisis para proporcionar información práctica sobre la postura de seguridad: gestión de la superficie de ataque, formación de *red teams* automatizada continua, simulación de infracciones y ataques, y formación de *purple teams* avanzada.

El valor de Cymulate, aseguraba Avihai Ben-Yossef es "garantizar que nuestro cliente tenga un programa de ciberseguridad bien definido". Explica el directivo que la compañía proporciona visibilidad de la postura de seguridad o exposición a amenazas y "nos aseguremos de que el programa de seguridad de nuestros clientes sea muy sólido y sostenible"

> "No es necesario ser un experto para operar Cymulate"

Seguridad Ofensiva

La industria de la ciberseguridad se basa en el principio de que los ciberdelincuentes suelen estar un paso por delante y los defensores están un paso por detrás. Para tratar de darle la vuelta, las empresas necesitan comprender dónde su postura de seguridad es débil y vulnerable. Hay diferentes enfoques para hacer pruebas ofensivas.

- **Gestión de superficie de ataque (ASM): busca activos digitales o información de la empresa que estén expuestos y accesibles. Esencialmente, esta tecnología se usa para emular la etapa de reconocimiento de un adversario.**
- **Equipos rojos automatizados continuos (CART - Continuous Automated Red Teaming): campañas de penetración de extremo a extremo que señalan los caminos a través de los cuales podría generarse una brecha de seguridad.**
- **Simulación de infracciones y ataques (BAS): simula ataques contra todos y cada uno de los controles de seguridad para validar su eficacia.**
- **Marco Advanced Purple Teaming: escenarios de ataque avanzados y personalizados que siguen el marco MITRE ATT&CK para modelar a los actores de amenazas y optimizar las defensas.**

Extended Security Posture Management (XSPM) es un proceso de varias capas que combina las capacidades de Attack Surface Management (ASM), Breach and Attack Simulation (BAS), Continuous Automated Red Teaming (CART) y Purple Teaming para evaluar y puntuar continuamente la ciberseguridad y resiliencia de la infraestructura de una empresa.

> "Las empresas tienen mucho que proteger"

Explicaba durante la entrevista que, "cuando se desea tener un programa de seguridad sostenible, se necesitan usar escenarios de ataque para validar, pero también se necesita buscar configuraciones incorrectas y vulnerabilidades". Esas nuevas necesidades son las que la han llevado a la compañía a ir más allá, "a cambiar nuestro producto y nuestra visión" y a lanzar, hace más de un año, Attack Surface Management (ASM), que "mapea la superficie de ataque y brinda mucha visibilidad de las vulnerabilidades, los activos, la red y los servicios. Todo lo que la organización hace", nos contaba el CTO de Cymulate. Explicaba que, haciendo ese ejercicio de mapeo, se descubren los escenarios de ataque, y que el BAS puede validar mucha de esta información, tanto si tiene o no un impacto en su organización. Pero, "al final,

necesitas gestionar todos esos datos que se recopilan sobre tu organización, y para poder generar acciones priorizadas necesitas ser capaz de gestionar esos datos de la manera correcta", comentaba Avihai Ben-Yossef, añadiendo lo que para el directivo son las tres etapas en el viaje hacia la madurez de la postura de seguridad: escanear, validar y administrar.

Que en la agenda de las grandes empresas esté el tener la mayor visibilidad posible hace que sean clientes potenciales de Cymulate. En todo caso, la visión de Avihai Ben-Yossef a la hora de fundar su empresa fue ayudar a las organizaciones a mejorar su postura de seguridad gracias a su experiencia en seguridad ofensiva, y eso incluye a empresas medianas; "no es necesario ser un experto para operar Cymulate. Esa fue parte de nuestra visión desde el primer día. Queríamos asegurarnos de que podemos ayudar también a las empresas que podrían no tener presupuesto para un *red team*".

Además, la compañía trabaja con MSSP "para brindar un servicio administrado a empresas más pequeñas que no tienen el personal, los recursos humanos, para operarlo por sí mismos. Y estamos trabajando con muchos proveedores de servicios gestionados que están brindando simulación como un servicio debido a la facilidad de uso y la simplicidad de implementación".

De cara a futuro, la hora de ruta de Cymulate seguirá los pasos mencionados por el CTO: herramientas que ayuden a las empresas a administrar su programa de seguridad, validarlo y, por supuesto, escanearlo.

ENLACES DESTACADOS

Cymulate amplía su gestión de superficie de ataques con cuatro nuevas capacidades

Afrontando los ciberataques con una aproximación Zero Trust

“Lo que nos hace distintos es que a nosotros nos dejan tocar”

Los equipos de IT y OT han crecido por separado y trabajan en diferentes mundos con diferentes prioridades. Según un informe de investigación del Instituto Ponemon sobre ‘El estado de la ciberseguridad industrial’, solo alrededor de un tercio de las organizaciones estudiadas dijeron que sus equipos de IT y OT tienen una estrategia de seguridad unificada.

Gerard Vidal, cofundador y CTO de **Opscura**

Opscura, antes Enigmedia, es una compañía española dedicada a la ciberseguridad de sistemas de control industrial (ICS). Dice Gerard Vidal, cofundador y CTO de Opscura, que la ciberseguridad clásica es un mercado muy trillado, mientras que la ciberseguidad industrial es un sector nuevo, “a pesar de que los equipos que protege son todos viejos”. Otra diferencia, añade, es que “los sistemas de IT están pensados para que el usuario final sea una persona, mientras que en el mundo industrial el dispositivo final es una máquina”.

Asegura también el CTO de Opscura que el gran problema de la ciberseguridad industrial es que, en la mayoría de las ocasiones, incrementar el nivel de ciberseguridad implica cambiar los switches, la disponibilidad, los equipos electrónicos o la red de la fábrica, porque cuando los diseñaron Internet no existía; “Lo que hacemos nosotros es incrementar el nivel de ciberseguridad sin tocar ningún componente de la fábrica” asegura Gerard Vidal, explicando que lo que es fácil en el mundo IT, como tener visibilidad del número de dispositivos conectados a la red, en el mundo industrial es muy complicado.

ciberseguridadTIC

Tai editorial

ENTREVISTAS

Añade el CTO de Opscura que la compañía es capaz "de desplegar esta ciberseguridad en cuestión de horas cuando normalmente un proyecto de segmentación de red puede tardar meses. Ahí es donde nosotros aportamos el mayor valor, a la hora de incrementar estos niveles de seguridad de una forma muy fácil".

Hablando de valor, ¿qué ventaja competitiva tiene Opscura frente a otros jugadores del mercado de ciberseguridad industrial como pueden ser Nozomi o Armis? "Nosotros nos dedicamos a la protección", asegura, añadiendo que las empresas mencionadas son más conocidas por la detección de anomalías. "Lo que hacemos nosotros, que es único, es lo siguiente: creamos una capa de cifrado de tráfico seguro en el mundo industrial, y a partir de ahí, implementamos políticas de seguridad", explica Gerard Vidal, añadiendo que uno de los grandes retos del mundo industrial es que es tremendamente fácil de hackear porque las máquinas que componen el ecosistema industrial "no estaban preparadas para la ciberseguridad".

> "Somos malísimos haciendo marketing, pero somos buenísimos desplegando"

El dicho 'si funciona no se toca' es muy popular en el mundo de la ciberseguridad, y especialmente repetido en el mundo industrial, donde una parada de producción puede ser un auténtico desastre. "Lo que nos hace distintos es que a nosotros nos dejan tocar", asegura Gerard Vidal.

De Enigmedia a Opscura

El pasado mes de febrero Enigmedia anunciaba un cambio de nombre y anunciaba el cierre de una ronda Serie A, de 9,4 millones de dólares liderada por Anzu Partners y con inversiones de Dreamit y Mundi Ventures.

Opscura en RSA 2023

La RSA Conference sirvió a ICEX e INCIBE como marco para invitar a Gerard Vidal, CTO de Opscura, a compartir el caso de éxito de la compañía durante una mesa redonda que se celebró en paralelo a conferencia de San Francisco.

"Ciberseguridad española en EE.UU." fue el titular de una sesión en la que Gerard tuvo la oportunidad de explicar su evolución y compartir las experiencias, desde cómo lanzaron una due diligence a Enigmedia y cómo, tras dos años de intenso trabajo, se ha convertido en Opscura Inc. gracias a una ronda Serie A, de 9,4 millones de dólares liderada por Anzu Partners y con inversiones de Dreamit y Mundi Ventures.

Opscura se convierte así en una empresa global de ciberseguridad de sistemas de control industrial (ICS) con foco y visión internacional.

ciberseguridadTIC

Tai editorial

ENTREVISTAS

Explica el CTO de Opscura que la compañía ha contado con el apoyo de dos fondos de inversión de Estados Unidos, uno de los cuales es un fondo especializado en ciberseguridad, y que el dinero recaudado se destinará a la apertura de operaciones en Estados Unidos, “uno de los mercados más grandes y más sensibles a la ciberseguridad”, donde se establece la sede de la compañía.

Respecto al nuevo nombre nos cuenta Gerard Vidal que Opscura recoge la ‘Op’ de Operaciones, y la palabra ‘opscura’, “que viene de oscuridad, de ofuscación. Porque lo que nosotros hacemos es ofuscar el tráfico”, que supone que, si un ciberdelincuente entra en la red, “no sabe lo que hay y, por lo tanto, no puede atacar”.

> Cualquier fábrica que tenga unos ingresos de más de 20 millones de euros es un cliente potencial de Opscura

Estas herramientas de ofuscación no son nuevas, ¿nadie las había aplicado al entorno industrial? “Cuando nosotros implementamos seguridad hacemos lo más básico que te puedes imaginar”, explica el CTO de la compañía, mencionando tareas como la segmentación de la red, el firewalling, mejora de la visibilidad, o ayudar con el cambio de las políticas de seguridad. “Son cosas que están trilladísimas. No hemos inventado la rueda. Todo eso existe”, asegura Gerard Vidal, añadiendo que la clave está en la rapidez con la que trabajan: “la capa de cifrado la podemos hacer a nivel de milisegundos”.

> "Nosotros no nos dedicamos a la detección de amenazas, sino a la protección del entorno OT"

Clientes

En opinión de Gerard Vidal, cualquier fábrica que tenga unos ingresos de más de 20 millones de euros, "que para una fábrica en el sector industrial no es tanto", es un cliente potencial de Opscura, una empresa que lo mismo protege una planta de agua que una refinería, dos entornos con diferente sensibilidad, pero en los que "la complejidad desde el punto de vista operacional es parecida".

Preguntamos también al CTO de Opscura qué es lo que más sorprende a sus clientes cuando se acercan y hacen una primera prueba de concepto. "Donde realmente brillamos es en el despliegue. Ahí es donde nos lo ganamos, porque somos malísimos haciendo marketing, pero somos buenísimos desplegando". CST

ENLACES DESTACADOS

El 40 % de los ordenadores OT se vieron afectados por malware en 2022

El 35 % de las vulnerabilidades en los sistemas de control industrial no tiene parches

"Afrontando la seguridad del dato en las Administraciones Públicas"

Aunque el sector público ha logrado un progreso notable en la resiliencia cibernética, todavía existen brechas significativas. Las soluciones de protección de datos son esenciales, y pensar en la copia de seguridad es un buen primer paso, pero igualmente importante es tener en cuenta la continuidad del negocio.

TAI Editorial, a través de sus cabeceras Director TIC y Ciberseguridad TIC, ha organizado un encuentro en el que se ha debatido sobre la evolución del backup en un mundo híbrido y multinube, la protección de un dato cada vez más disperso y una continuidad de negocio cada vez más compleja.

En el debate participaron diferentes directivos de sector público que dejaron interesantes reflexiones.

"Ya no basta con tener un backup. Ahora necesitamos tener diferentes escenarios de desastre y cómo vamos a actuar ante ellos"

Ignacio Pérez,
CISO, AST – **Gobierno de Aragón**

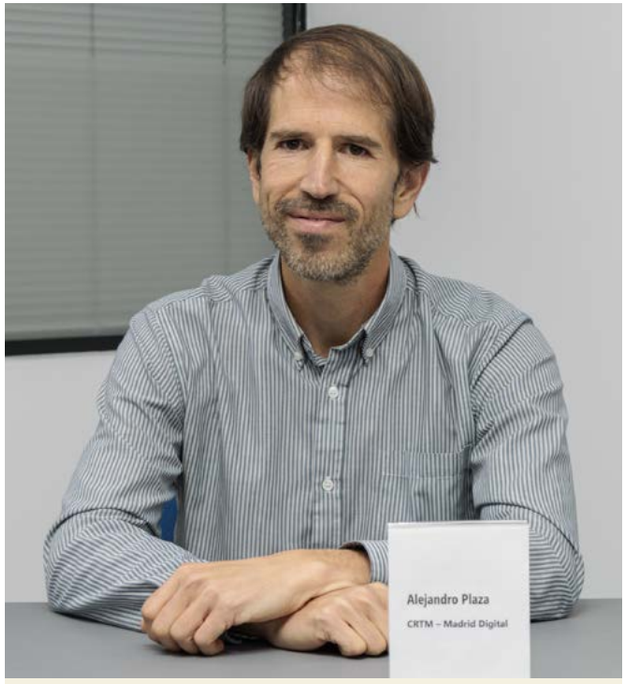
DEBATES

"La información está muy distribuida y dispersa. El reto es acotarla"

Julián Fernández de Heredia González-Chamarro,
Responsable IT y Sistemas – **Cámara de Comercio, Industria y Servicios de Madrid**

"Las cintas son la última salvaguarda"

Miguel Ángel Blanco Arribas,
Jefe de Área de Planificación y Sistemas Informáticos, Subdirección General de Sistemas y Aplicaciones para la Financiación Territorial – **Ministerio de Hacienda y Función Pública**



"El futuro está en las soluciones híbridas"

Alejandro Plaza Gómez,
Centro de Operaciones de Ciberseguridad Madrid Digital

DEBATES

"Las tecnologías de copia inmutable son un avance importante"

Francisco Manuel Cortes Jurado,
Jefe de Servicio de Explotación de Sistemas Informáticos – **Gobierno de Castilla la Mancha**

Accede al resumen del debate descargando el documento

TRIBUNAS

Gestión de activos: el papel del CIO en la protección de los entornos cloud

En opinión de Sergio Pedroche, country manager de Qualys para España y Portugal, contar con una solución potente de Asset Management debería ser una prioridad principal para los CIOs porque, sin ella, siempre habrá un terreno irregular sobre el que construir en el futuro.

MÁS INFORMACIÓN

Cómo reforzar el privilegio mínimo con la gestión de las identidades

Para Albert Barnwell, Sales Director Iberia de CyberArk, en una era en la que los privilegios están en todas partes, los pilares básicos para la gestión de las identidades exigen un nuevo enfoque.

MÁS INFORMACIÓN

Estrategia de gasto en una economía restrictiva

En medio de un estancamiento económico, Neil Thacker, CISO de Netskope para EMEA, enumera en esta tribuna algunas de las ventajas financieras derivadas de la transformación de la seguridad y la red.

MÁS INFORMACIÓN

Tenemos **toda la información** que necesitas