it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Marzo 2021 - nº 39

La importancia de DevSecOps

‘La seguridad es una carrera de fondo prácticamente sin meta’ (Carlos Asún)

‘El control de la identidad es un gran problemas de seguridad’ (Óscar Sánchez Montaner)

Quantum, CloudGuard y Harmony, o el nuevo mundo para Check Point

#DesayunosITDS Afrontando el modelo Zero Trust

Guarda esta revista en tu equipo y ábrela con Adobe Acrobat Reader para aprovechar al máximo sus opciones de interactividad

it Digital Security

Directora Rosalía Arroyo
rosalia.arroyo@itdmgroup.es

Colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez

Diseño revistas digitales Contracorriente

Producción audiovisual Favorit Comunicación, Alberto Varet

Fotografía Ania Lewandowska

it Digital MEDIA GROUP

Director General
Juan Ramón Melara juanramon.melara@itdmgroup.es

Director de Contenidos
Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es

Directora IT Televisión y Lead Gen
Arancha Asenjo arancha.asenjo@itdmgroup.es

Directora División Web
Bárbara Madariaga barbara.madariaga@itdmgroup.es

Director de Operaciones
Ángel Porras angel.porras@itdmgroup.es

Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

La importancia de DevSecOps

Antes de la llegada de Devops, la seguridad era una ocurrencia tardía. Encontrar y minimizar las vulnerabilidades no era tarea de los desarrolladores. DevSecOps (Development Security Operations) es la práctica de incorporar seguridad de forma continua a lo largo del ciclo de vida del desarrollo de la aplicación, lo que garantiza que la seguridad sea una parte fundamental de la aplicación y no una función incorporada. En un momento en que las empresas necesitan adaptar rápidamente sus aplicaciones para seguir siendo viables en este nuevo clima de aceleración de la digitalización, DevSecOps ofrece la visibilidad, automatización y colaboración mejoradas que necesitan para garantizar la seguridad y confiabilidad de sus aplicaciones ahora y en el futuro.

Carlos Asún, CISO de Food Delivery Brands, y Óscar Sánchez Montaner, Cybersecurity Director de Puig, son los grandes protagonistas de este número de IT Digital Security. También hablamos con Alberto López, responsable de V-Valley Seguridad, y Javier Sánchez, nombrado Territory Sales Manager de Entrust una vez cerrada la compra de nCipher Security.

Zero Trust ha sido el tema de debate de uno de nuestros #DesayunosITDS. Convertido en el modelo a seguir, Zero Trust también genera nuevas complicaciones y nuevos desafíos. ¿Cómo deberían los CISO trasladar sus organizaciones de la seguridad tradicional a una arquitectura de confianza cero? El debate ha contado con expertos de One Identity, Thales, SonicWall, Sophos, Kaspersky y Netskope.

La actualidad llega marcada por la celebración del CPX 360 de Check Point, en el que la compañía anuncia una gran reorganización de producto, y la llegada a España de VMray, una empresa alemana que triunfa en el mercado de sandbox y que será liderada en nuestro país por Ovanes Mikhaylov.

¿Te interesa la seguridad? Entonces seguro que te gusta este número de IT Digital Security.

En Portada

La importancia de DevSecOps

itds

Sumario

Actualidad

Sandox Matter

Quantum, CloudGuard y Harmony, o el nuevo mundo para Check Point

Entrevistas

‘La seguridad es una carrera de fondo prácticamente sin meta’

Carlos Asún, CISO Food Delivery Brands

‘El control de la identidad es uno de los principales problemas de seguridad’

Óscar Sánchez Montaner, Puig

‘La gente es ahora mucho más receptiva al discurso del HSM’

Javier Sánchez, Entrust

‘Más que fichar empresas soy de fichar buenos profesionales’

Alberto López, V-Valley Seguridad

No solo IT

Women4Cyber Spain en el Día Internacional de la mujer

El inicio del Antropoceno Digital

Índice de anunciantes

ESET — IT Webinars

Stormshield — IT User

Trend Micro — IT Reseller

Secure&IT — CdR Almacenamiento

Doc. Eje. IT Trends — CdR Impresión

Desayuno ITDS

Sandbox Matter

La tecnología de sandboxing de la alemana VMray aterriza en España de la mano de Ovanes Mikhaylov. La plataforma de la compañía apuesta por una monitorización a nivel de hipervisor, un proceso de detección y análisis de malware automatizado, y conectores que facilitan la integración con la pila de seguridad existente para proteger anteriores inversiones.

Las técnica de evasión de malware buscan evitar la detección y uno de sus principales objetivos es la evasión de las Sandbox, o cajas de arena, un sistema que la mayoría de las compañías utilizan para detonar archivos y URL maliciosas con el fin de obtener más indicadores de compromiso y extender sus defensas con el objetivo final de bloquear la actividad maliciosa. Es un mercado con un crecimiento medio anual del 26,5% desde 2017 a 2022, según datos de Markets&Markets, consultora que asegura que son las brechas de seguridad detectadas en aplicaciones web y móviles lo que está impulsando el crecimiento de este mercado.

VMray es una compañía alemana fundada en 2013, que acumula cuatro rondas de financiación que suman 28,9 millones de dólares, según datos de Crunchbase, y que llega a España de la mano

"Tenemos toda la intención de ser algo más que un proveedor más de tecnología de ciberseguridad en el mercado español"

Ovanes Mikhaylov

de Ovanes Mikhaylov, nombrado Business Development Manager Southern Europe, quien asegura que VMray ofrece una de las tecnologías de sandboxing más fiables del mercado para la detección y análisis de malware avanzado.

"Nuestras soluciones ayudan a las empresas y las organizaciones gubernamentales a protegerse contra amenazas sofisticadas, como el malware de día cero, el malware evasivo y los ataques dirigidos complejos", asegura el directivo, añadiendo que con su solución son capaces de mejorar la capacidad de los clientes para detectar cuándo están bajo ataque, ayudando a los equipos de respuesta a incidentes y SOC a gestionar el creciente volumen y diversidad de amenazas "con mucha mayor velocidad y precisión".

"El problema de los ataques dirigidos no está resuelto", dice Ovanes Mikhaylov cuando le preguntamos qué es lo que está impulsando el mercado de sandbox. Asegura que las cajas de arena pueden detectar malware sofisticado que ha sido diseñado para evadir otras defensas y que juegan un papel importante en la protección de una organización porque "fortalecen las capas de seguridad que una organización ya puede tener. En otras palabras: varias tecnologías en la pila de seguridad de una organización pueden detectar malware, pero será una detección basada en firmas, heurísticas o búsquedas de reputación, que son muy eficaces contra amenazas conocidas, pero no contra amenazas avanzadas previamente desconocidas. Las cajas de arena cierran esta brecha en la pila de seguridad".

Las soluciones de sanbox son utilizadas “por organizaciones que son muy conscientes de la seguridad”. Explica el directivo de VMray que por lo general estos clients tipo cuentan con equipos internos de respuesta ante incidentes y SOC, y utilizan entornos aislados como parte integral de sus flujos de trabajo de protección avanzada contra amenazas; “nuestras soluciones están siendo utilizadas por una amplia variedad de organizaciones. Lo que todos tienen en común es la madurez de su estrategia de seguridad”.

La tecnología de sandbox no es nueva. ¿Qué es lo que distingue la propuesta tecnológica de VMray? Asegura Mikhaylov que el de VMray es enfoque “radicalmente diferente” y explica que las amenazas avanzadas están diseñadas para reconocer cuándo se ejecutan dentro de un entorno de análisis y están programadas para tomar medidas evasivas para evitar la detección; “hemos colocado el sistema de monitorización en la capa del hipervisor, lo que nos permite monitorizar la actividad del malware completamente fuera del entorno de análisis. Esto hace que nuestra tecnología sea prácticamente indetectable y extremadamente resistente contra la evasión de la zona de pruebas”.

Añade el directivo de VMray que otro de los puntos fuertes de la compañía es la calidad de

La tecnología de monitorización de VMRay solo captura señales que son relevantes para resolver una amenaza, lo cual es vital para la velocidad y efectividad de la respuesta a incidentes

VMray ha colocado el sistema de monitorización en la capa del hipervisor

los informes: “la tecnología de monitorización de VMRay solo captura señales que son relevantes para resolver una amenaza, lo cual es vital para la velocidad y efectividad de la respuesta a incidentes”. Por otra parte, el proceso de detección y análisis de malware está automatizado, lo que reduce la necesidad de intervención humana.

Por último, destaca Ovanes Mikhaylov que los conectores de la plataforma facilitan la integración con la pila de seguridad existente de la organización y que los resultados del análisis y la inteligencia sobre amenazas se pueden compartir en todo el entorno de seguridad, “lo que aumenta la eficacia de los sistemas que ya están instalados y protege las inversiones existentes”.

VMray en España

“Tenemos toda la intención de ser algo más que un proveedor más de tecnología de ciberseguridad en el mercado español”, responde el directivo cuando le preguntamos por la estrategia en nuestro país. Asegura que quieren convertirse “en un actor reconocido” y que “el éxito en la región dependerá en gran medida de nuestra capacidad para construir una sólida red de socios”.

De esta forma, las iniciativas de participación de socios se convierten en una de las principales prioridades de la agenda 2021 de la compañía. Asegura Mikhaylov que ya se cuenta con un programa de socios de canal “muy atractivo” y que “como proveedor de tecnologías innovadoras de sandboxing, buscamos socios con experiencia en SOC y respuesta a incidentes. Es fundamental que ganemos socios que comprendan nuestra propuesta de valor única y posean la experiencia técnica para llevar nuestras soluciones al mercado”.

El modelo de canal es Tier2 con cuatro niveles: Consultancy Partner, Fulfillment Partner, Silver Partner and Gold Partner. Explica el directivo que para ofrecer una estructura que se adapte a diferentes modelos de negocio, creamos el estado de Socio Consultor para atraer socios no revendedores que se especializan en consultoría de seguridad. El programa de canales está orientado a la rentabilidad, con elementos como registro de acuerdos, capacitación y certificación de socios sin cargo, soporte de marketing conjunto, así como soporte pre y posventa. “Estamos plenamente comprometidos con el éxito del canal”, asegura Ovanes Mikhaylov.

Enlaces de interés...

- VMray
- Crece el uso de malware con capacidades de antianálisis y evasión de sandboxes
- Cómo vencer al malware evasivo, o avanzado

Compartir en RRSS

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA
CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

PREDICCIÓN	PREVENCIÓN
ESET Threat Intelligence ESET Virus Radar WeLive Security	Endpoint Protection Platform ESET Mail Security ESET Gateway Security ESET SharePoint Security ESET Secure Authentication ESET Endpoint Encryption ESET Security Management Center ESET Cloud Administrator
ESET Enterprise Inspector ESET Dynamic Threat Defense ESET Security Management Center ESET Cloud Administrator	Endpoint Protection Platform ESET Dynamic Threat Defense ESET Enterprise Inspector ESET Mail Security ESET Gateway Security ESET SharePoint Security ESET Secure Authentication ESET Endpoint Encryption ESET Security Management Center ESET Cloud Administrator
RESPUESTA	DETECCIÓN

CYBERSECURITY
EXPERTS ON
YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

Quantum, CloudGuard y Harmony,

o el nuevo mundo para Check Point

Check Point Software Technologies celebraba a finales de febrero su evento anual para clientes y socios, CPX 360, el primero completamente virtual y que ha estado dedicado a abordar los desafíos de ciberseguridad más urgentes y cómo ayudar a las empresas de todos los tamaños a desarrollar estrategias de protección. La compañía propone una reordenación de su oferta en tres familias de productos para "proporcionar el verdadero nivel de seguridad que necesitamos".

Gil Shwed, fundador y director ejecutivo de Check Point, era el encargado de inaugurar el evento con una ponencia titulada "Nuevo mundo, nuevas oportunidades" en la que aseguraba que "tenemos que empezar a hacer planes para el nuevo mundo".

El coronavirus nos ha proporcionado, decía, muchas oportunidades de cambiar el mundo. Mencionó el trabajo remoto, asegurando que en plena pandemia el 87% de los empleados de la compañía trabajaban desde casa, un porcentaje que actualmente es del 85%; también habló sobre cómo ha habido un gran aumento en todos los tipos de ciberataques durante el año pasado con un incremento del 50% por ciento en ataques sofisticados.

Mirando hacia el futuro, hacia ese nuevo mundo con sus múltiples oportunidades, Shwed aseguró que el 74% por ciento de las empresas darán a sus empleados la opción de teletrabajar de forma permanente en 2021 y más allá, y esos lugares de trabajo distribuidos son "parte del mundo que tenemos que proteger".

Haciendo referencia a Sunburst o Emotet, insistió en que ahora los ciberataques son más sofisticados, y repasó la evolución de las ciberamenazas

"Nuestra misión es hacer que este mundo sea más seguro, para lo cual tenemos la oportunidad de redefinir el papel de la ciberseguridad"

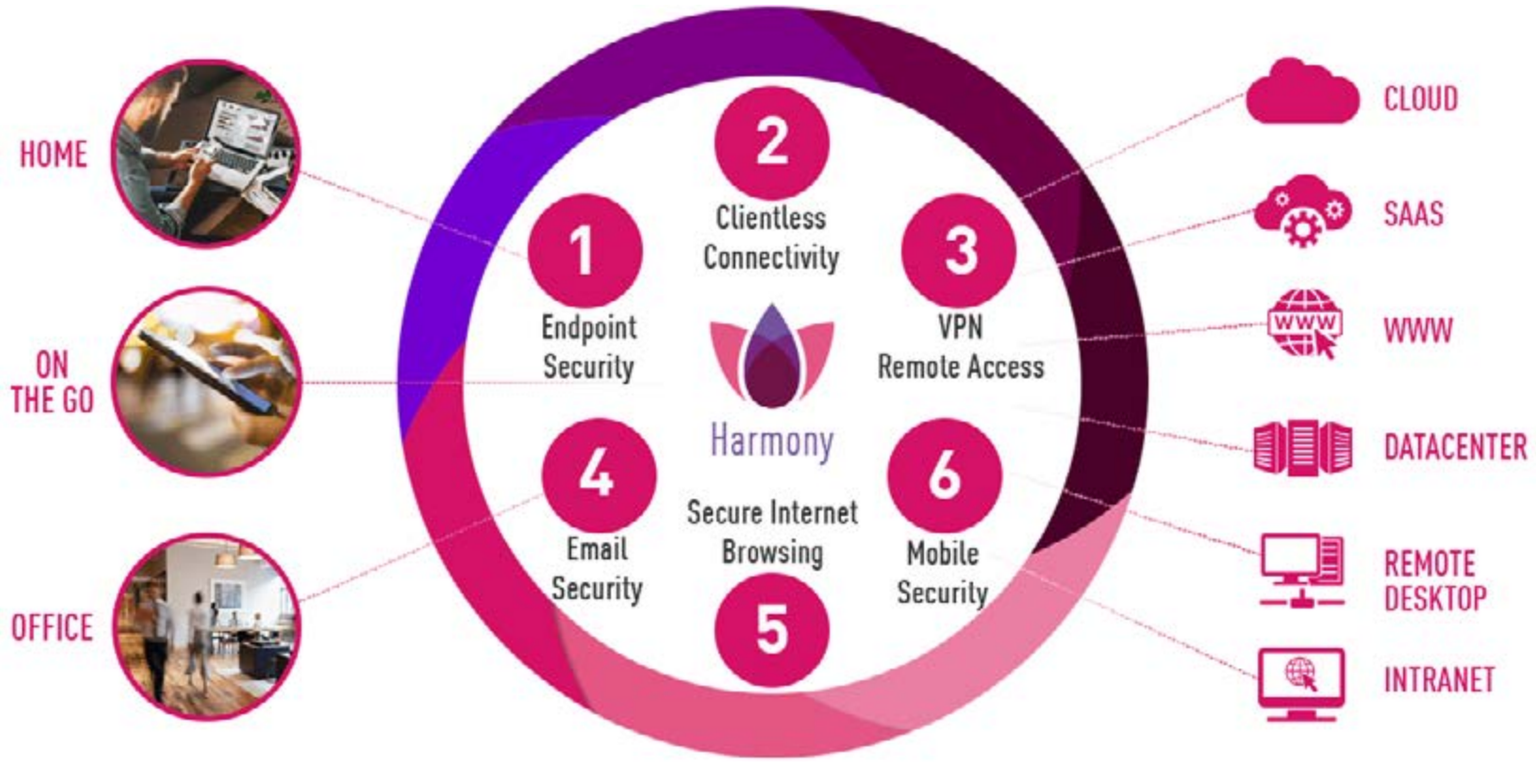
Gil Shwed, CEO, Check Point

y sus soluciones desde los años 80, tiempo de la Generación 1, a la actualidad, cuando nos encontramos con la Generación V, unos ataques que están caracterizados por ser multivectoriales, polimórficos y evasivos "lo que hace que sean muy difíciles de identificar". Los ataques de quinta generación son un reto, "pero el mayor reto es que la mayoría de las empresas utilizan tecnologías de seguridad capaces de hacer frente a los ataques de tercera generación. Nuestra prioridad es cerrar esta brecha y hacer que las organizaciones adopten la tecnología de seguridad Gen V para proteger su futuro".

En este nuevo mundo, continuaba diciendo Gil Shwed, la superficie de ataque se ha ampliado y lo que esperamos es que haya un incremento de esta quinta generación de ataques, "y nuestra misión es hacer que este mundo sea más seguro", para lo cual "tenemos la oportunidad de redefinir el papel de la ciberseguridad".

Si el mundo del año pasado era un poco virtual, lo que ahora estamos viendo es que somos un 90% virtual, "y esto es posible porque internet funciona", aseguraba el directivo haciendo referencia a las plataformas de vídeo online, a las clases online y, por supuesto, al trabajo remoto. La misión de Check Point, decía Gil Shwed, es la misma que cuando arrancó la compañía: ayudar a las empresas a gestionar sus empresas en internet con el mayor nivel de seguridad.

Actualmente las prioridades para las empresas son: Asegurar a los trabajadores remotos; asegurar la movilidad y el endpoint y asegurar el cloud, público y privado. La estrategia de Check Point frente a estas necesidades es "ofrecer la mejor prevención y una gestión única con una solución consolidada" para lo cual la compañía cuenta con una familia de más 80 productos "que están aquí para proteger el mundo". Pero ¿cómo hacerlas más accesibles?, se preguntaba el directivo apuntando lo que será la estrategia de la compañía para 2021, una reorganización de productos repartidos en tres áreas clave: seguridad de red, seguridad cloud y seguridad de accesos y usuarios, con tres grandes familias de productos:



Quantum para securizar la red, CloudGuard para securizar la nube y Harmony para Securtizar a usuarios y accesos.

"Estas tres familias, Quantum, CloudGuard y Harmony se podrán gestionar de manera unificada a través de Infinity Vision y estarán conectadas a través de la infraestructura Infinity ThreatCloud", explicaba Shwed durante su discurso añadiendo: "Este es el nuevo mundo. Esto es Infinity 2021".

Harmony

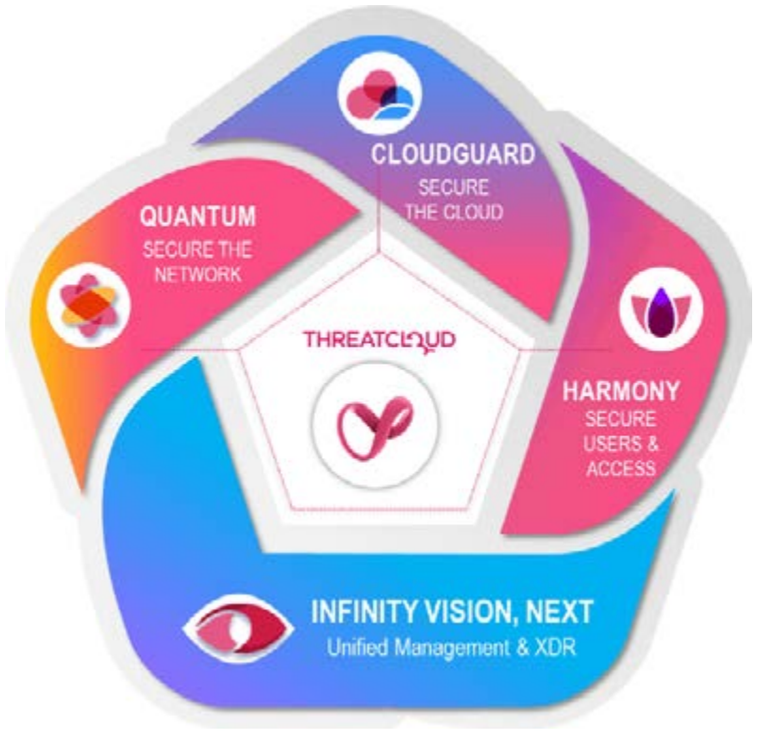
Check Point Harmony ha sido una de las grandes novedades del CPX 360 2021. Se trata de la primera solución unificada que permite una conectividad segura a todos los recursos empresariales, proporcionando una protección total de los endpoints desde cualquier dispositivo. Harmony se encarga de garantizar la seguridad tanto los dispositivos corporativos como los BYOD y sus conexiones a Internet frente a los ataques conocidos y de día cero, al tiempo que ofrece acceso Zero-Trust a las aplicaciones empresariales en una solución única y fácil de gestionar.

De forma que Harmony unifica los componentes de seguridad del endpoint, el navegador, el correo electrónico y el acceso remoto para proteger todos los dispositivos de los usuarios, así como la red corporativa a la que se conectan.

Harmony integra las principales funciones de seguridad en una única solución para ofrecer seguridad web complete a través del nuevo Harmony Browse, que proporciona una navegación web segura, rápida y privada, inspeccionando todo el tráfico SSL directamente en el endpoint -sin añadir latencia ni redirigir el tráfico- a través de un servicio web seguro. Parte de la familia es Harmony Connect, que establece una conexión segura entre todos los usuarios o departamentos y todos los recursos, con un acceso seguro a través de la red Zero Trust Network desde cualquier navegador.

Con Harmony Email & Office se asegura el correo electrónico de los usuarios, ofreciendo una protección completa para Microsoft Office 365, Exchange, Google G Suite y más. Por último, Harmony Endpoint protege a los ordenadores del robo de datos, phishing, malware y minimiza el impacto de una ruptura en el sistema con una detección y respuesta autónoma. Harmony Mobile asegura también los

La Generación V de ciberataques se caracterizan por ser multivectoriales, polimórficos y evasivos, lo que hace que sean muy difíciles de identificar



El 74% por ciento de las empresas darán a sus empleados la opción de trabajar de forma permanente desde casa en 2021, y esos lugares de trabajo distribuidos son parte del mundo que tenemos que proteger

dispositivos móviles de los empleados ante aplicaciones maliciosas y ataques en la red o al sistema operativo.

Durante su intervención, Rafi Kretchmer, Vicepresidente de Marketing de Producto en Check Point, explicaba que el movimiento masivo hacia el trabajo a distancia ha creado agujeros en la infraestructura de seguridad de las empresas que no pueden ser abordados con diferentes productos de diferentes empresas; “Harmony cierra estos huecos con seguridad unificada de varias capas y tecnologías de prevención, bloqueando los ataques desde todos los frentes. Garantiza seguridad para el nuevo entorno empresarial de “trabajar desde cualquier lugar”, con una implantación fácil y una gestión desde una única consola.” it

Enlaces de interés...

- Check Point Harmony
- Check point CPX 360 2021
- La ciberseguridad post pandemia centra el encuentro Check Point CPX360 2021

Compartir en RRSS

STORMSHIELD

Primer cortafuegos en obtener ambas certificaciones del CCN.

Producto Cualificado y Producto Aprobado

Stormshield, filial participada al 100 % de Airbus CyberSecurity, propone soluciones de seguridad completas e innovadoras para proteger las redes (Stormshield Network Security), los puestos de trabajo (Stormshield Endpoint Security) y los datos (Stormshield Data Security). www.stormshield.com/es/

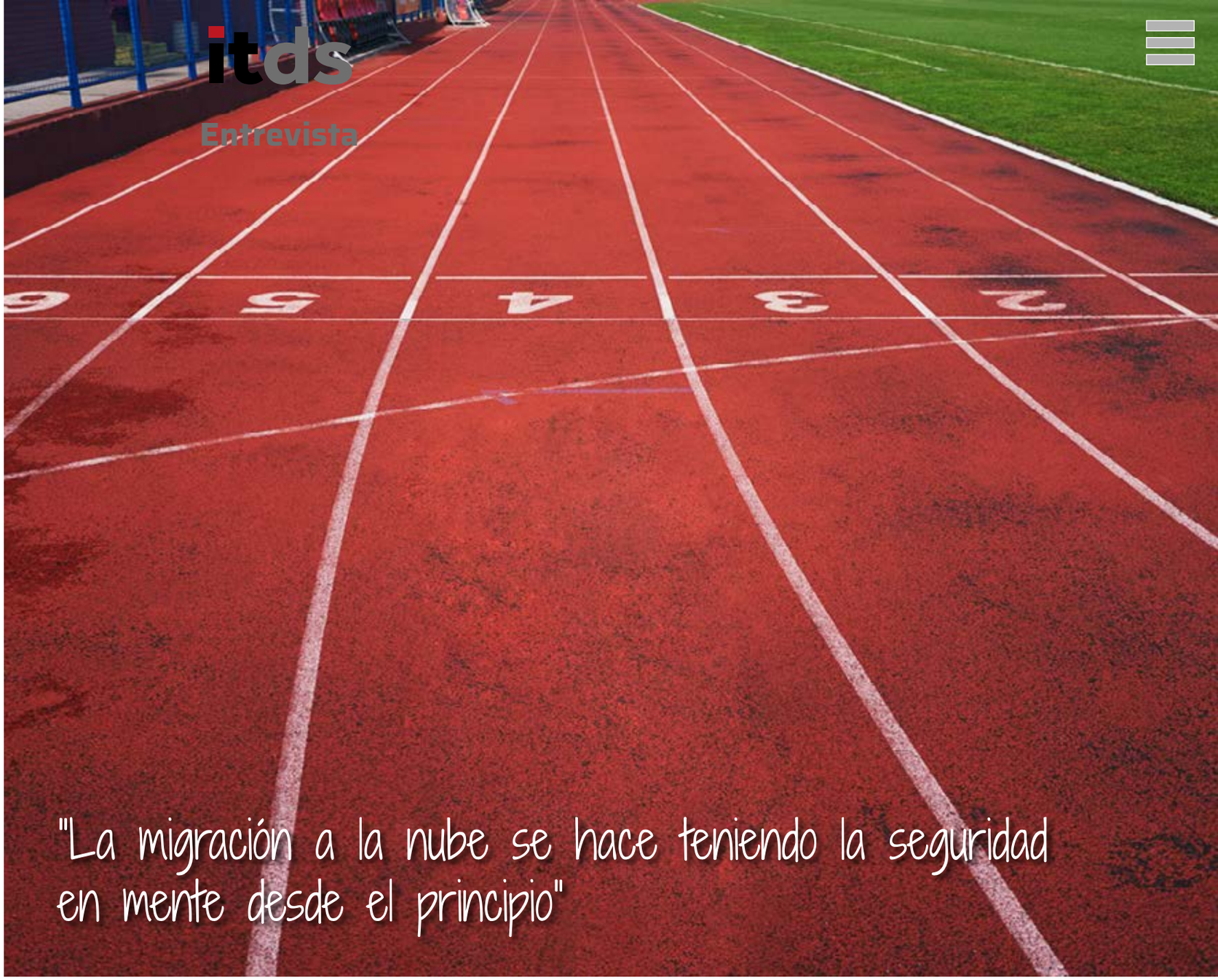
‘La seguridad es una carrera de fondo prácticamente sin meta’

(Carlos Asún, CISO Food Delivery Brands)

Carlos Asún es el CISO de Food Delivery Brands. Tiene claras cuáles deben ser las cualidades de un buen CISO; que los servicios gestionados son imprescindibles, pero que no debes atarte a ningún proveedor; que es necesario contar con un buen SIEM y un excelente SOC y que este 2021 podría ser el año de volver a las oficinas.

Rosalía Arroyo

“Ser asertivo, proactivo, empático, resolutivo, flexible, buen comunicador, dar confianza y estar muy puesto en la tecnología” son algunas de las principales cualidades que debe tener un buen CISO, una figura que tiene que interactuar con muchas áreas de negocio, que durante los últimos tiempos ha ganado peso dentro de las empresas, con cada vez más presencia en los consejos de administración. Nos lo cuenta Carlos Asún, CISO de Food Delivery Brands, un grupo que opera en 36



países a través de las marcas Telepizza, Pizza Hut, Jenos's Pizza y Apache Pizza.

Sobre la evolución del papel de CISO en los últimos años, dice Carlos Asún que ha cambiado muchísimo pero que también depende del tipo de empresa y el tipo de sector en el que se opere, algo que también influye en cuánto se prioriza la seguridad. En todo caso, la seguridad es cada vez más prioritaria dentro de las empresas, "la seguridad es un no acabar, una carrera de fondo prácticamente sin meta".

Un año después de que la pandemia nos recluyera en nuestras casas e impactara en todo el mundo, ¿qué han aprendido los CISO? Dice Carlos Asún que hay que tener en cuenta un aspecto diferenciador: las empresas y CISOs que hubieran tenido la suerte de tener el teletrabajo implantado probablemente no les haya afectado mucho, como es el caso de Food Delivery Brands, "pero hay empresas que han tenido muchos problemas, que además les ha impactado en el negocio, y para los que la pandemia ha supuesto un antes y un después".

Y los CEO, ¿han aprendido algo de ciberseguridad durante la pandemia? "Me gustaría hablar con un CEO que estuviese en contra del teletrabajo hace un año, a ver qué piensa ahora. Seguro que más de uno se va a pensar dos veces el mantener el teletrabajo".

Cloud

La migración a la nube se hace… "teniendo la seguridad en mente desde el principio", dice Carlos Asún. Asegura que la "adaptación al cloud es muy importante" y que si bien es cierto que tenemos sistemas que aún no están en la nube por diferentes circunstancias "si lo que queremos es minimizar el riesgo y ahorrar en costes la idea es ir al cloud sin ningún tipo de duda". Añade que previamente hay que hacer un buen análisis de riesgos y establecer controles de lo que puede pasar en esa migración.

"Para mí es primordial", dice el CISO de Food Delivery Brands cuando le preguntamos por el papel

"La seguridad es cada vez más prioritaria dentro de las empresas"

que juegan los servicios de seguridad gestionados. A Carlos Asún le gusta la variedad y contar con los mejores, y asegura que es necesaria "mucha coordinación y mucha comunicación entre los proveedores que le prestan diferentes servicios".

¿Cómo se encuentra al mejor proveedor? "Con mucho análisis, preguntando mucho, con RFIs y RFPs muy potentes, muchas entrevistas, reuniones e intentar no atarse mucho al proveedor porque somos humanos, nos podemos confundir, pueden pasar cosas a lo largo del tiempo y si no estás muy atado a ese proveedor la transición a otro en mucho más fácil".

Tecnologías de Seguridad

Preguntamos también a Carlos Asún cuáles cree que son las tecnologías básicas de seguridad que se deben tener, sin las cuales no se puede estar. "Depende mucho del tipo de empresa y el sector en el que estés", responde en un primer momento para después mencionar WAF como un elemento importantísimo, "tener un buen SIEM y un excelente SOC, porque si tienes un muy buen SIEM y un SOC mediocre estás totalmente vendido". ¿On premise o como servicio? "Cada empresa es un mundo y tiene que escoger lo mejor. Para mí es en modo servicio gestionado en todos los aspectos porque es muy sencillo a la hora de salir y cambiar. Si compras una herramienta de SIEM ya estás atado. La tecnología cambia mucho y

los que hoy son muy buenos mañana pueden no serlo", explica Carlos Asún añadiendo que, teniendo estas herramientas, el SIEM y el SOC en modo servicio, pierdes algunas cualidades, "pero sabes que, si mañana tienes que cambiar, la transición es rápida, el trastorno es mínimo. Pero es mi opinión".

Seguimos hablando de tecnologías y de herramientas, que en seguridad son muchas, muchísimas. Como imprescindibles hemos hablado del WAF, del SIEM, del SOC; también menciona el NAC, sobre el que dice que es "una herramienta muy potente a nivel interno de la empresa", así como el PAM, CASB, ISD/IPS… y llegamos a los simuladores de ataque y vigilancia de la darkweb como elementos a tener muy en cuenta.

2021

Sobre si este año prevé un cambio significativo en torno a la seguridad, menciona que existe la posibilidad, para muchas empresas, de que sea el año de

"La inteligencia artificial irá a más, y a lo mejor podremos encontrar algo nuevo que nos pueda ayudar en la parte de seguridad"

volver a las oficinas, y eso significa que habrá que devolver los equipos a las oficinas, equipos que habrá que revisar después de meses sin demasiado control si dichas empresas no lo han hecho.

"Si hablamos de otros aspectos, me imagino que todo lo relacionado con la inteligencia artificial irá a más, y a lo mejor podremos encontrar algo nuevo que nos pueda ayudar en la parte de seguridad", añade Carlos Asún, sin olvidarse que "los ataques siempre van a estar ahí, cada vez van a ser más sofisticados y tenemos que estar proactivamente preparados para que cuando nos pase podamos reaccionar de la mejor manera posible con esos niveles de resiliencia que demuestre tener cada empresa".

Enlaces de interés...

- 'SASE no será algo que pase de refilón. Todas las empresas iremos en esa dirección' (Carlos Manchado, Naturgy)
- 'El cloud no viene ni a ni a resolver ni a empeorar la situación a nivel de seguridad' (Elena García, Indra)
- 'En seguridad la heterogeneidad es compleja de gestionar, y sobre todo de financiar' (Jesús Alonso Murillo, Ferrovial Servicios)
- 'Los CISO somos ciberresilientes desde hace mucho tiempo' (Javier Sánchez Salas - HAYA Real Estate)
- 'No tiene sentido ver la seguridad como un gasto' (Rubén Fernández, Grupo DIA)

Compartir en RRSS

Todo lo que necesita para asegurar su nube.

Simplifique su seguridad en la nube con Trend Micro Cloud One™, la plataforma de servicios de seguridad para desarrolladores líder en el mundo.

Cloud One™ Cloud Security simplificada

La infraestructura global evoluciona con el tiempo pero Trend Micro va por delante optimizando la protección. Creado con datos reales por el artista **Andy Gilmore**

Descubra Cloud One en este video:

Conozca más en www.trendmicro.es

TREND MICRO™

‘El control de la identidad es uno de los principales problemas de seguridad’

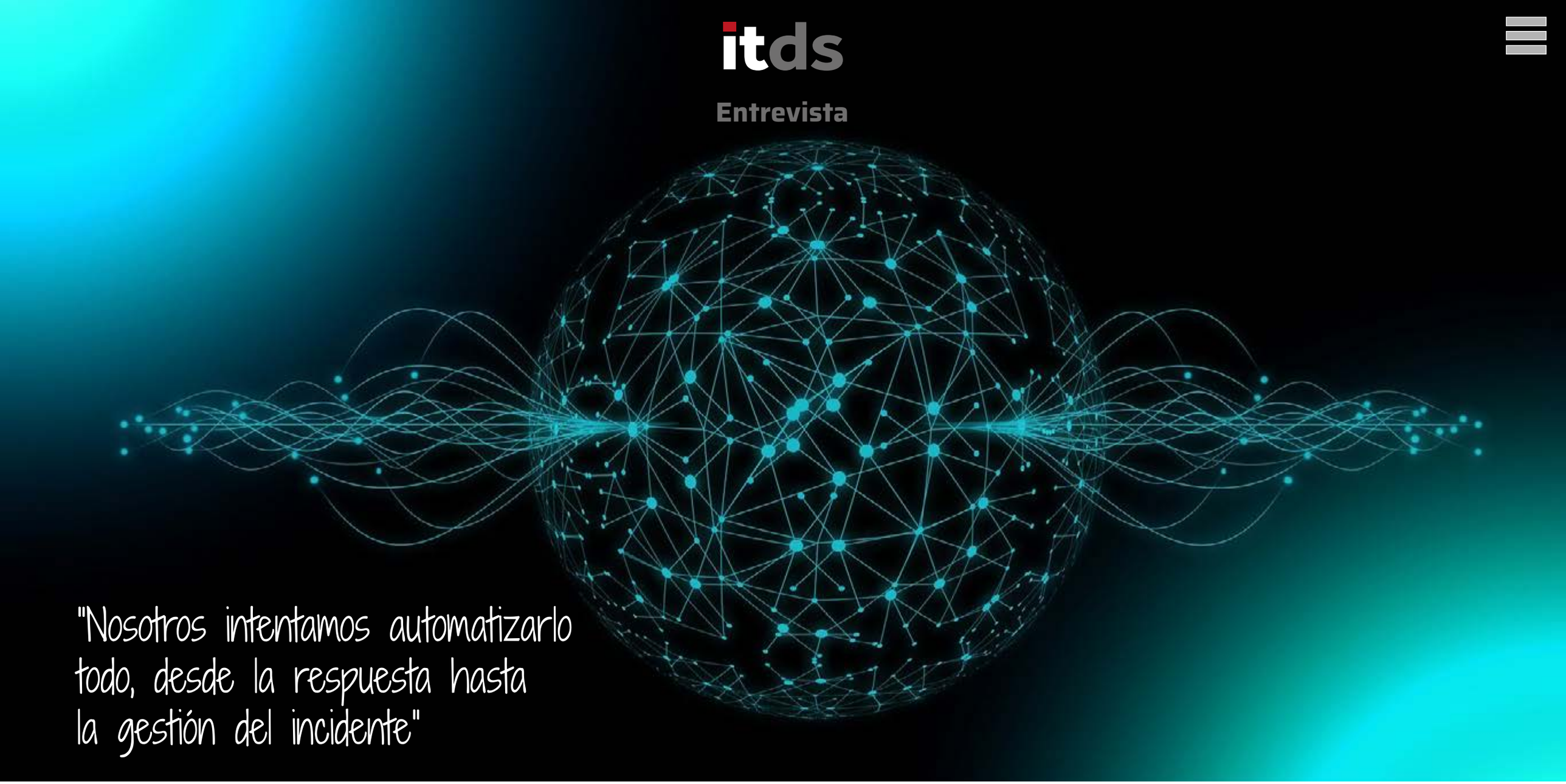
(Óscar Sánchez Montaner, Puig)

A la seguridad le falta ir al ritmo del negocio, dice Óscar Sánchez Montaner, Cybersecurity Director de Puig, para quien la evolución del papel del CISO ha sido bastante accidentada; el control de la navegación imprescindible; la ciberseguridad una prioridad; la experiencia un grado a la hora de escoger proveedor de servicios; y la automatización el futuro.

Rosalía Arroyo

Puig es una empresa familiar de moda y fragancias con sede en Barcelona. Con 26 filiales y una distribución que llega a más de 150 países de todo el mundo, la compañía afrontaba recientemente una reorganización de su estructura empresarial que le ha llevado a crear tres divisiones: Beauty and Fashion, Charlotte Tilbury y Derma, todas ellas operativas a partir del 1 de enero de 2021. Detrás de estas tres divisiones están marcas tan conocidas como Paco Rabanne, Carolina Herrera, Jean Paul Gaultier, Nina Ricci, así como Uriage, Apivita, o Isdin, de la que Puig posee el 50%. El objetivo de la compañía es ambicioso: alcanzar los 3.000 millones de euros en ventas para 2023.

Entre bambalinas, manteniendo la seguridad de los sistemas de Puig desde hace más de tres años se encuentra Óscar Sánchez Montaner, Cybersecurity Director, para quien la evolución del papel del CISO ha sido “bastante accidentada, y especialmente en nuestro país”. Dice que todavía hay que empoderar las C del CISO, que las empresas



"Nosotros intentamos automatizarlo todo, desde la respuesta hasta la gestión del incidente"

deberían, tanto a nivel de estrategia como de organigrama, dotar a esta figura, que en muchas ocasiones depende aún del CIO.

La pandemia ha dado mucha visibilidad a las ciberamenazas, y eso ha hecho que se haya reforzado el papel del responsable de ciberseguridad. Los órganos de dirección de las empresas, asegura Óscar Sánchez, "están cada vez más preocupados. No concienciados, sino preocupados" lo que lleva a que exista un movimiento para que el responsable de ciberseguridad participe más de la estrategia de la empresa y tenga un poco más de voz y voto en estos órganos.

Añade Óscar Sánchez que algunos responsables de seguridad también tienen tareas pendientes, como es el saber comunicar, utilizar otro vocabulario, hablar el idioma de negocio "y saber simplificar nuestros pensamientos; cuesta mucho explicar al CEO, o al CIO, un incidente que has tenido; cuesta mucho sintonizar el mismo lenguaje. Pensamos que es fácil intentar explicar algo a alguien que no es del mundo tecnológico, pero para ellos es complicado".

Empresas y ciberseguridad

"Las empresas que no vean que la ciberseguridad es una prioridad, que debe estar dentro de los dos o cinco temas que les tienen que preocupar, creo que están abocadas a que en un futuro tengan serios problemas", dice Óscar Sánchez cuando le preguntamos si cree que la seguridad se ha

convertido en una prioridad para la empresa española. ¿Y cuándo es una empresa familiar como Puig? “Puig está muy concienciada [con la ciberseguridad]. Prácticamente opera bajo las mismas estructuras y esquemas que una multinacional que no sea familiar y cotiza en el IBEX”, dice el responsable de ciberseguridad de Puig, añadiendo que colocar la seguridad como una prioridad dentro de la empresa tiene más que ver con las personas que están al frente de la misma, de su visión del riesgo, que el hecho de que las empresas sean grandes o familiares.

Sobre el impacto que grandes brechas de seguridad como las de SolarWinds o Equifax tienen, dice Óscar Sánchez que actúan como medios de concienciación y demuestran que la seguridad no tiene fin, que no te puedes relajar por contar con un departamento de seguridad y dotarlo de presupuesto.

Cloud y Servicios

La adopción del cloud se hace… “de una forma acelerada y muchas veces el driver es negocio”, dice el responsable de seguridad de Puig; añade que “a la seguridad le hace falta ir al ritmo del negocio”, porque se tiende a pensar que proteger la empresa es esencial, pero las empresas tienen “sus objetivos de negocio marcados y los departamentos de seguridad tenemos que ser capaces de seguir ese ritmo y ayudarles”.

La adopción de servicios cloud a espaldas de los departamentos de TI, es lo que se conoce como Shadow IT. ¿Se ha dado el paso de tener herramientas que te den visibilidad de ese Shadow IT? “Sí. De hecho, son necesarias. Necesitas herramientas que te den visibilidad de todo, de lo bueno y lo malo, y ente ellas del Shadow IT”. Por suerte, añade, cada vez más los departamentos son conscientes y consultan las repercusiones que podría haber con el uso de algún servicio o tecnología.

Sobre los servicios de seguridad gestionada, “tienen un papel importante, no sólo en Puig sino a nivel general”, dice el directivo. Añade que se trata de

"Los cibercriminales que están al otro lado cada vez están más preparados y tienen más recursos"

"Necesitas herramientas que te den visibilidad de todo, de lo bueno y lo malo, y ente ellas del Shadow IT"

encontrar el equilibrio, porque un sistema totalmente externalizado tendrá riesgos y uno internalizado se hace insostenible. A la hora de seleccionar un servicio gestionado "miramos varios ejes, entre ellos la experiencia en ofrecer ese tipo de servicios".

Tecnologías

¿Qué tecnologías de seguridad cree que son imprescindibles? Menciona Óscar Sánchez la protección del correo como una de las principales, además del control de la navegación, los endpoints a través de un antimalware y un EDR, concienciación, así como sistemas que permitan un correcto control de la identidad, "que hoy en día es uno de los principales problemas de seguridad".

Mirando hacia adelante dice el responsable de ciberseguridad de Puig que la automatización será imprescindible. "Nosotros intentamos automatizarlo todo, desde la respuesta hasta la gestión del incidente, y si además le puedes aportar elementos o métodos de lo que se deriva de inteligencia artificial, Deep learning y todas esas técnicas de estudio de datos masivos que además te pueden dar patrones, mejor".

Después de un año de pandemia, ¿esperas algún cambio significativo en torno a la seguridad? "Yo creo que continuaremos más o menos en la misma senda: el teletrabajo seguirá siendo un pilar fundamental"; añade que lo que se están viendo son ataques cada vez más sofisticados, entre otras cosas porque "los cibercriminales que están al otro lado cada vez están más preparados y tienen más recursos".

Enlaces de interés...

- 'SASE no será algo que pase de refilón. Todas las empresas iremos en esa dirección' (Carlos Manchado, Naturgy)
- 'El cloud no viene ni a ni a resolver ni a empeorar la situación a nivel de seguridad' (Elena García, Indra)
- 'En seguridad la heterogeneidad es compleja de gestionar, y sobre todo de financiar' (Jesús Alonso Murillo, Ferrovial Servicios)
- 'Los CISO somos ciberresilientes desde hace mucho tiempo' (Javier Sánchez Salas - HAYA Real Estate)
- 'No tiene sentido ver la seguridad como un gasto' (Rubén Fernández, Grupo DIA)

Compartir en RRSS

Secure&IT by LKS

www.secureit.es

CIBERSEGURIDAD EN LA DESESCALADA DE LA COVID-19

& Promoción especial

Auditorías y seguridad gestionada

& Privacidad vs. COVID-19

¿Qué medidas de contención pueden implementar las empresas?

& Adecuación a la normativa e-commerce

¿Cómo adaptar una web para vender de forma online?

+ INFO

Un 8 de febrero de 2018 Alberto López se convertía en el director de la división de seguridad en V-Valley, el negocio de valor añadido de Esprinet Ibérica, tras un largo recorrido de más de 25 años por el mercado de distribución que deja pistas suyas en Afina, Magirus, Westcon e Ingecom.

Rosalía Arroyo

‘Más que fichar empresas soy de fichar buenos profesionales’

(Alberto López, V-Valley Seguridad)

Tres años le han bastado a Alberto López para recuperar un negocio que agonizaba. No sólo se ha recuperado la facturación y “se ha mejorado el portfolio, sino que nos hemos convertido en un área muy atractiva para que la gente quiera trabajar aquí”, y esto, en un mercado de adolece de profesionales, es decir mucho. “Más que fichar empresas soy de fichar buenos profesionales, lo otro llega solo”, dice, añadiendo que lo fundamental de las compañías es el equipo humano.

"La compra de GTI aporta muchísima experiencia en cómo ir a modelos de pago por uso y securizar entornos cloud"

Actualmente Alberto López dirige un equipo de 22 personas y prefiere hablar de soluciones, y no de marcas.

El proyecto que ponían en sus manos era tan atractivo como difícil, "pero una de las claves es que me han dejado trabajar con una agilidad impresionante". Alberto López iniciaba la nueva aventura con unas premisas básicas: "hay que trabajar en Excel, ser muy ágil e invertir en personas claves". En tres años la facturación ha aumentado con menos fabricantes. Sobre el portfolio, habla Alberto López de un equilibrio entre los fabricantes más tradicionales, y un par de marcas, o tres, más pequeñas, o menos conocidas, pero con potencial. Diferencia el negocio de volumen, donde prima el "cuantas más marcas mejor", al negocio de valor "donde soy partidario de tener menos fabricantes, pero mejor trabajados". Durante estos años se ha conseguir racionalizar la oferta, reteniendo a los fabricantes que interesaba tener y complementarlos con otras marcas "pero sin crear conflictos".

La palabra 'valor' dentro del canal de distribución no es nueva, pero con tecnologías como el cloud, el as-a-service y la complejidad y cantidad de tecnologías, ha ido cobrando todo su sentido. Hablando de proyectos asegura Alberto López que una parte importante de la inversión de V-Valley Seguridad es "en preventas que ayuden a la integradores en respuesta a pliegos". Explica que muchos de los pliegos incluyen pagos aplazados, por lo que, además de la parte técnica, "necesitas a alguien que dé forma financiera a ese proyecto".

2020, año de pandemia

"Hemos crecido muchísimo", dice Alberto López haciendo referencia a 2020; "quizá porque hemos conseguido hacer un equipo muy potente, de mucha experiencia". La estrategia, asegura, es tener claro hacia dónde vas; la ventaja, contar con un grupo financiero muy potente "que nos permite

hacer proyectos muy grandes y financiados"; y el resultado ser "el único mayorista de volumen que ha triunfado la seguridad".

Actualmente Esprinet es el primer mayorista en negocio de volumen y el segundo en valor; "el objetivo en dos años es ser el número uno en valor", dice el responsable del negocio de seguridad de V-Valley, que ha trabajado en la parte Enterprise con los grandes integradores de seguridad y ha puesto los medios "para que sea muy fácil trabajar con nosotros", explica Alberto López añadiendo: "la pregunta que le hago a cualquier fabricantes es: ¿qué necesitas por mi parte?".

¿Qué es lo que han aprendido las empresas durante la pandemia? "Lo que todos ya sabíamos, que el perímetro se acaba; que el teletrabajo se ha impuesto, lo que ha implicado el tener que dotar a los dispositivos de seguridad y accesos remotos". Dice también Alberto López que durante el año pasado creció mucho el negocio de accesos remotos, tecnologías de validación del puesto y en temas de NAC; asegura que se compró a un ritmo frenético, entre otras cosas ordenadores y tablets que hay que securizar y actualizar, y cree que "este año es el sector público quien va a tirar el carro de la seguridad", un sector en el que la compañía está

it whitepapers

INFORME EMPLEOS EMERGENTES 2020

Este texto recoge el estudio anual que realiza LinkedIn sobre las profesiones emergentes que irrumpen en el mercado de trabajo de España. Gracias a los datos recopilados en la red social, se han identificado los 15 perfiles profesionales que han surgido a lo largo de los 5 últimos años y las habilidades específicas que estos requieren. Al mismo tiempo se han localizado las provincias y los sectores donde se concentra la demanda de estos nuevos empleos.

"Contar con un grupo financiero muy potente nos permite hacer proyectos muy grandes y financiados"

focalizada y en el que dice: “hemos empezado muy bien el año”.

Adquisiciones

La compra de GTI no sólo ha convertido al Grupo Esprinet en un líder del mercado mayorista en España por volumen de ingresos, sino que le ha permitido dar un salto significativo en los negocios del software y cloud, donde GTI tenía una posición avanzada

Sobre la compra de GTI dice Alberto López que “aporta muchísima experiencia en cómo ir a modelos de pago por uso y securizar entornos cloud”. La compra ayuda a Esprinet a convertirse en “el distribuidor que puede dar a esos fabricantes de seguridad un posicionamiento muy fuerte en la parte cloud”, añade.

Siglas y modas

Los fabricantes van empujando con sus tecnologías y productos en un mercado en el que los clientes tienen sus propios ritmos y el canal hace de intermediario entre las prisas y la extrema prudencia. Ahora está de moda ser un convencido de Zero Trust, un apasionado de SASE y convertir el EDR y el Threat Hunting en el elemento clave para detectar y parar un ciberataque, pero ¿están llegando estas tecnologías y modelos realmente a los clientes? “Al final son un poco modas. Cada boom, cada momento, tiene sus palabras clave”, dice Alberto López. Añade que las necesidades del cliente son siempre las mismas, que los entornos van cambiando y que lo que parece nuevo es de lo que llevamos hablando toda la vida.

¿Qué es lo que está comprando la empresa española? “Todo lo que rodea al endpoint, tanto el EDR, como el DLP, está generando proyectos importantes”, explica el director de V-Vallery Seguridad, añadiendo que también hay mucho interés por los SIEM y la apertura de tráfico cifrado SSL.

Enlaces de interés...

- ‘Las empresas necesitan madurar en el área de ciberinteligencia’ (Eutimio Fernández, ThreatQuotient)
- MobileIron y Pulse Secure son ahora Ivanti e Ivanti Security Solutions
- ‘Zero Trsut y SASE ponen en valor las soluciones de gestión de identidades privilegiadas’ (Carlos Ferro, Thycotic)
- ‘2021 va a convertirse en el año de la inteligencia artificial y la automatización de procesos’ (Pedro Pablo Pérez, Telefónica Tech)
- ‘Las empresas no pueden ser negligentes en la gestión de dato’ (Francisco Valencia, Secure&IT)

Compartir en RRSS

Descarga este documento ejecutivo de IT RESEARCH

NUEVO INFORME

it Digital Security

Entrevista

‘La gente es ahora mucho más receptiva al discurso del HSM’

(Javier Sánchez, Entrust)

Javier Sánchez Fuertes es el Territory Sales Manager de Entrust, y un experto en cifrado y módulos HSM. Dice que las claves de cifrado son la última frontera de la seguridad y propone el HSM como un repositorio de confianza mientras asegura que “esto no va tanto de proteger el dato, que también, como el proceso de negocio”.

Los HSM (Hardware Security Module), o módulos de seguridad hardware, son dispositivos que generan, almacenan y protegen claves criptográficas. Uno de los referentes del mercado es Entrust, quien en los últimos años ha realizado una serie de compras y fusiones estratégicas que le convierten en un verdadero experto en protección de identidades, pagos y datos con tres unidades de negocio destacadas: Soluciones de Certificación, Gestión de identidades y Accesos y HSM.

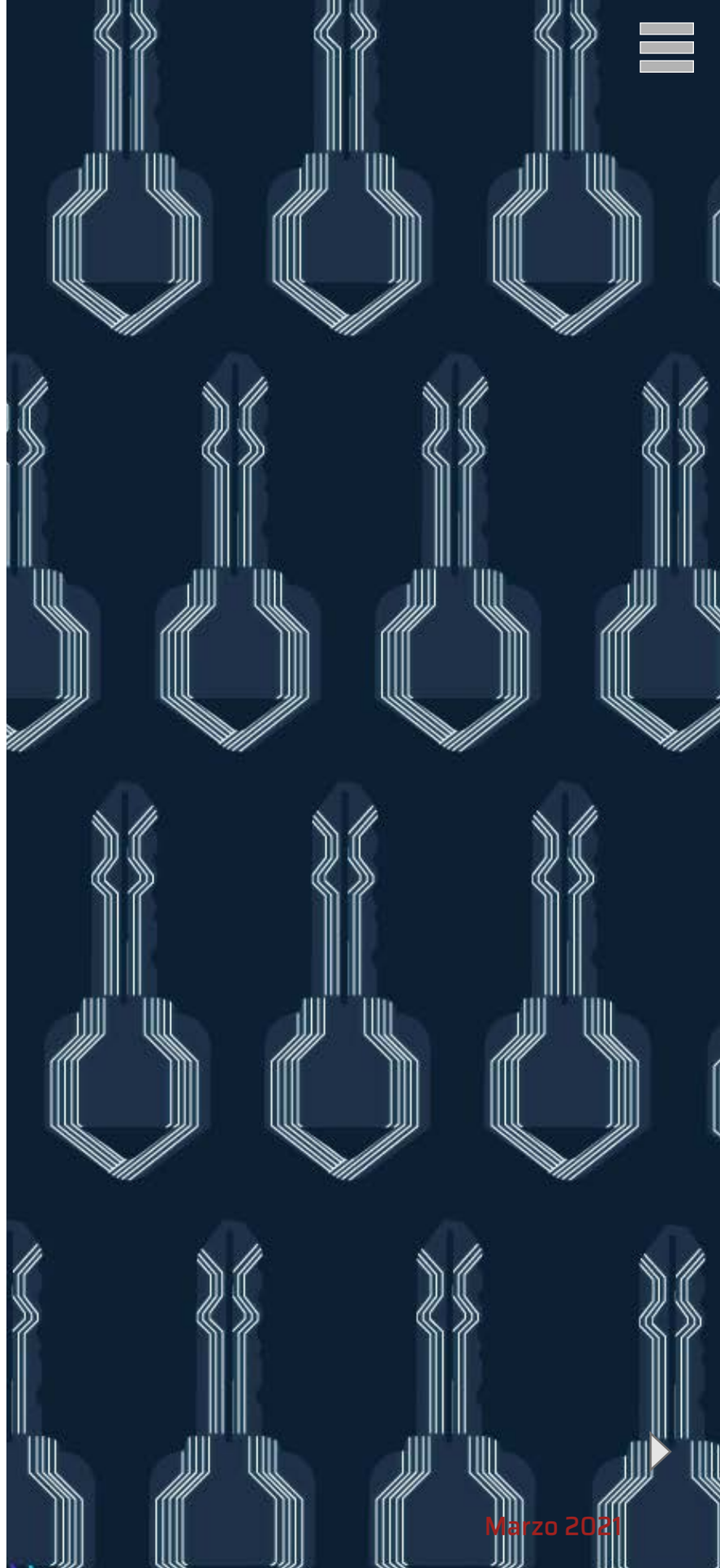
Los últimos tiempos de lo que ahora es el negocio de HSM de Entrust, antes Entrust Data Card, han sido algo convulsos. Hace unos años se produjo uno de esos acuerdos de compra que hacen historia y desbordan titulares. Thales Group anunciaba su intención de comprar Gemalto por 4.800 millones de dólares, para lo cual la Unión Europea le impuso como condición la escisión de su negocio de módulos HSM por temas de competencia. Esa unidad de negocio, Thales eSecurity, llevaría por nombre nCipher y sería vendida a Entrust Data Card en febrero de 2019. Tras unos meses de convivencia, a finales del año pasado se completaba la integración de ambas compañías y nCipher se convertía, oficialmente en Entrust.

Javier Sánchez Fuertes, quien fuera el director general de Thales eSecurity, es ahora Territory Sales Manager de Entrust, una empresa sobre la que dice que tiene productos interesantes y competitivos, cuya presencia en algunos mercados es tremendamente fuerte, una empresa con buenos resultados y que a nivel de recursos humanos funcionan muy bien… Dice que la compra de Entrust no ha tenido ningún impacto en el negocio de nCipher al tiempo que asegura que lo que quieren los clientes es que detrás de la nueva marca, “a poder ser siga la misma persona”.

Protegiendo el proceso de negocio

La compra por parte de Entrust le da a este directivo con más de diez años de experiencia en el mercado de cifrado nuevas oportunidades al pasar a forma parte de una empresa con una oferta que va más allá de los HSM. Habla Javier Sánchez de “interacción” con los compañeros, tanto los que llevan soluciones de PKI como soluciones de firma digital; “allí donde hay una PKI y una firma digital hay una

"Cualquier empresa que haga su movimiento a la nube puede hacer uso de las herramientas de cifrado que le den los proveedores de nube pública, pero en ese momento pierdes el control"



Según este estudios, el uso de certificados digitales está creciendo rápidamente para aplicaciones en la nube y autenticación de usuarios. Además, el rápido crecimiento en el uso de dispositivos de IoT está teniendo un impacto en el uso de tecnologías PKI y se está reconociendo que PKI proporciona tecnologías de autenticación centrales importantes para IoT.

clave privada, y entonces me compete porque el HSM importa".

Sobre los HSM asegura que "no va tanto de proteger el dato, que también, como el proceso de negocio". Explica Javier Sánchez que cuando se está protegiendo un proceso de firma electrónica "no estás protegiendo tanto el contenido del documento como asegurándote de que nadie lo modifica".

Saltamos al IoT y dice el directivo que cuando se le da identidad a las cosas mediante la emisión de certificados, en el fondo es lo que estás garantizando es que nadie pueda suplantar esas identidades; "cuando firmas código que luego se va a cargar en un coche o en una cámaras de vídeo, se hace de forma segura en un HSM, y lo que en el fondo se está garantizando es que no va a haber un mal uso de esas cosas conectadas".

Explica Javier Sánchez que "las cosas como tal necesitan de una identidad y para ello hay que generar un certificado que dice quién eres, lo que puedes hacer y durante cuánto tiempo". Para emitir esos certificados Entrust tiene una PKI (Public Key Infrastructure – Infraestructura de Clave Pública) "que nos permite habilitar la identidad de las cosas".

"Cuando firmas código que luego se va a cargar en un coche o en una cámaras de vídeo, se hace de forma segura en un HSM, y lo que en el fondo se está garantizando es que no va a haber un mal uso de esas cosas conectadas"

"Ha llegado el momento de proteger las claves de cifrado"

El siguiente paso es “cómo hacer que esa identidad que damos a las cosas se haga de forma segura. La respuesta es: haciendo que cada vez que se firme ese certificado, se firme un entorno seguro, que es el HSM”. Así que, en cuanto al proceso de dotar de identidad de forma segura a las cosas, “tenemos una oferta completa”.

La siguiente vuelta de tuerca, continúa explicando Sánchez, es lo que tiene que ver con la firma de código. Menciona el directivo los coches, las cámaras, los móviles… un montón de cosas que periódicamente tienen una actualización de software, revisión de parches, etc. “Todas estas cargas de software tienen que venir firmadas, y la firma tienen que haber ocurrido dentro de un entorno seguro, que es un HSM, para garantizar que nadie ha podido modificar ese código que ha sido firmado con una clave legítima”.

Dice Javier Sánchez que a pesar de que una brecha de seguridad tiene un mayor impacto mediático; “si eres un banco y resulta que el 90% de tu clientes se relacionan contigo a través de la app del móvil y se produce una modificación ilegítima que hace que la experiencia sea mala, pones en riesgo todo tu negocio. Aquí el riesgo no es una multa, es que el cliente tira la app a la basura y ya está”. Añade el directivo que las empresas se han gastado

montón de dinero en proteger sus sistemas con firewalls, antivirus, con seguridad endpoint… “pero resulta que las claves, que son la última frontera de seguridad, están desamparadas”.

Las claves por sí solas no se pueden proteger, dice Javier Sánchez, reconociendo que ahora los responsable de seguridad de las compañías asumen que sí tienen que proteger las miles de claves que hay en una empresa y que será “o bien por temas de presupuesto, o cuestión de tiempo, o de disponibilidad por lo que todavía no hayan llegado a dotar a su empresa de ese nivel de seguridad en cuanto a la protección de claves que se requiere, pero saben que tienen que hacerlo y ese es un cambio importante”.

HyTrust, más allá del HSM

El discurso de Entrust, con buena acogida en el mercado, es proponer el HSM como un repositorio de confianza donde todas las claves de toda la compañía, bien sean de la PKI, la de firma electrónica, de las sesiones SSL, las claves con las que se cifran las base de datos, las que utilizo para firmar el código… se protejan con una plataforma segura, que no es otra que el HSM.

“Ahora las empresas son mucho más receptivas al discurso del HSM. Ha llegado el momento de proteger las claves”, dice el Territory Manager, Entrust.

Entrust tiene varios tipos de módulos de seguridad de hardware, que funcionan exactamente igual y hacer más o menos lo mismo, pero a velocidades diferentes. Aproximadamente el 85% de lo que se vende son HSM de red, el 10% tarjetas HSM y un 5% son las cajas USB. Y hasta ahora este ha sido el negocio de Entrust Data Protection Solution.

El cambio llegaba a primeros de este año con la compra de HyTrust una compañía que se complementa con Entrust y sobre la que Javier Sánchez destaca su solución para el cifrado de máquinas virtuales y de control de claves, “una propuesta que el mercado está demandando”.

Explica el directivo que cualquier empresa que haga su movimiento a la nube puede hacer uso de las herramientas de cifrado que le den los

"Lo que quieren los clientes es que detrás de la nueva marca, a poder ser siga la misma persona"

proveedores de nube pública, pero que en ese momento "pierdes el control", y que "el hecho de que seas tú quien pueda desplegar tus propias políticas de cifrado, gusta mucho; que seas tú quien pueda desplegar tus propias políticas de control de claves, gusta más todavía".

La propuesta que añade HyTruts genera nuevas oportunidades de negocio en un mercado que está pidiendo este tipo de soluciones, asegura el directivo

Expansión horizontal

Cuando hablamos del tipo de cliente que consume HSM y cómo ha evolucionado, comenta el directivo que aunque es cierto que el tamaño de las empresas sí que ha cambiado algo, lo que ha ocurrido es que el cifrado ha sido adoptado de una manera más horizontal dentro de las empresas; "si al principio una empresa te compraba los HSM para proteger su PKI corporativa, con el paso del tiempo utilizan también un HSM para proteger las claves con las que se cifran las bases de datos, y también para la gestión de cuentas privilegiadas…", de forma que lo que está ocurriendo es que el uso de HSM se está extendiendo dentro de las empresas, haciendo realidad el mensaje de HSM como repositorio de confianza.

Explica el directivo que esa expansión horizontal hace que las conversaciones se realicen con diferentes interlocutores: con el responsable de comunicaciones si hablas de proteger las claves del cifrado SSL o con el de desarrollo cuando se trate de proteger las claves con las que se firma el código.

Tras un año de pandemia, este año… "habrá que seguir pedaleando, y creo que un poquito más fuerte que el año pasado", asegura Javier. Lo dice, eso sí, con la confianza puesta en una oferta de productos más amplia e integrada, una oferta que "el mercado tiene interés en ella".

Enlaces de interés…

- Entrust Datacard adquiere la empresa Safelayer
- Thales vende nCipher a Entrust Datacard y cierra así la compra de Gemalto
- Primeros pasos con eIDAS
- W The nCipher Security World Architecture
- 'Security World es una arquitectura de protección de claves criptográficas' (nCipher)

Compartir en RRSS

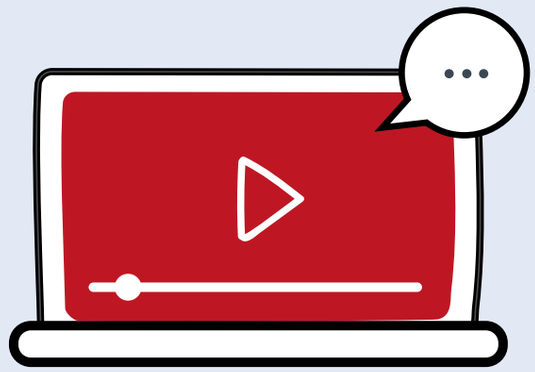
Aplicaciones,
¿cómo desarrollo y entrego mi mejor software?

Porque las aplicaciones son hoy -más que nunca- la cara del negocio y estamos en la era del DevSecOps... ¿cómo creo mi mejor software y lo pongo a disposición de mis usuarios? Únete a esta sesión online y conoce las mejores prácticas y todos aquellos aspectos a tener en cuenta cuando se desarrollan aplicaciones y software, así como a la hora de ponerlas en producción. ¡Reserva ahora tu sitio!

REGISTRO

Ya vivo en la nube, ¿y ahora qué?
Mejores prácticas para desenvolverse en entornos híbridos

Los entornos de TI multicloud e híbridos se están convirtiendo en el modelo hacia el que se dirigen las arquitecturas de TI actuales. Gestionar estas infraestructuras cloud, controlar sus costes, desarrollar nuevos servicios nativos en cloud, asegurar la disponibilidad del negocio basado en la nube, garantizar el cumplimiento normativo y proteger los activos que residen en la cloud, son cuestiones que todo responsable de TI debe tener bajo control. ¡Regístrate ahora!



#ITWEBINARS

Afrontando el modelo Zero Trust

Zero Trust se ha convertido en el modelo a seguir, pero también trae nuevas complicaciones y nuevos desafíos. ¿Cómo deberían los CISO trasladar sus organizaciones de la seguridad tradicional a una arquitectura de confianza cero?

Marzo 2021

Zero Trust se ha convertido en el modelo a seguir, en un objetivo que algunos consideran inalcanzable, un viaje que se tarda en recorrer, pero hay que iniciar cuando antes. Para saber qué viene a solucionar el modelo Zero Trust, qué se necesita para iniciar el viaje o qué hay que tener en cuenta para seleccionar a los proveedores que ayuden a implementar el modelo, celebramos uno de nuestros #DesayunosITDS, en el que han participado un grupo de expertos, empezando por Guillermo Martín Soto, Regional Sales Manager, Spain, Portugal & North Africa - IAM (Identity & Access Management) de Thales; Alberto Ruiz Rodas, Presales Engineer for Spain and Portugal de Sophos; Raúl D'Opazo, Solutions Architect de One Identity; Pedro García Villacañas, Head of Pre-Sales de Kaspersky Iberia; Sergio Martínez, Iberia Regional Manager de SonicWall y Javier Campo Azofra, Sales Engineer de Netskope.

Lo primero que planteamos es qué viene a solucionar el modelo Zero Trust. Dice Raúl D'Opazo que para One Identity el modelo Zero Trus como tal "intenta definir una estrategia de seguridad basada en conceptos" que lleven a que un usuario sólo podrá acceder a los datos o aplicaciones que tenga garantizados, de una manera concreta y cuando lo necesite. Pero esto, "que parece algo sencillo de lograr, no lo es".

Para Alberto Rodas, el modelo Zero Trust viene a solucionar "sobre todo los problemas de seguridad tradicional". Explica el directivo de Sophos que no son lo mismo los permisos que tiene un empleado trabajando dentro de la oficina, que fuera de la red de la empresa, y que "tenemos que verificarlo todo "para no dejar que esas VPN y esas redes entre oficinas o esos accesos que tiene un usuario por pertenecer a la red de usuarios, se conviertan en un coladero".

Zero Trust viene a resolver "este nuevo escenario en el que estamos", dice Guillermo Martín Soto, añadiendo que con la transformación digital, la nube o el teletrabajo "el perímetro de seguridad ha desaparecido y ahora todo gira en torno a otros conceptos como el usuario, el servicio, la sensibilidad de servicio al que se accede, el dispositivo en el que se accede, etcétera".

Javier Campo explica que cuando se definió, el objetivo de Zero Trust era de proteger los activos de la empresa, proteger a los usuarios, y sobre todo proteger los datos, y que se fundamenta en el paradigma de que no podemos declarar un usuario, un dispositivo o una red como confiable simplemente porque pertenece a la empresa; lo que debe hacerse es "clasificar cada conexión, cada acceso, como no confiable y en base a ello auditar, autorizar y autenticar cada una de las

Asegura Sergio Martínez que el eslabón más débil “siempre es el usuario, que siempre va a estar expuesto a cualquier tipo de engaño. Y esto es algo a lo que tenemos que estar preparados”. Añade el directivo de SonicWall que una de las ventajas que aporta el modelo Zero Trust es, precisamente, “minimizar el impacto de un engaño”, además de reducir el impacto de un ataque en un entorno de migración absoluta a la nube en el que estamos.

¿Dónde comienza Zero Trust?

Para Sophos el viaje hacia Zero Trust empieza en el endpoint, lo que implica estar seguros de quién esta logado en el endpoint y que ese punto final no se ha visto comprometido; “con estas dos premisas y evaluándolo de forma continua podemos controlar el acceso y que el dispositivo no se utiliza de forma incorrecta”.

"La empresa española no sólo está concienciada, sino también preparada para adaptar este modelo de Zero Trust"

Pedro García Villacañas,
Head of Pre-Sales, Kaspersky Iberia

acciones que el usuario ejecuta sobre los activos de la empresa”.

Para Pedro García Villacañas, incluso penetrar y moverse en la zona de confianza se ha hecho cada vez más fácil para para los adversarios, y este es uno de los problemas que viene a solucionar el modelo Zero Trust, que se une a una serie de conceptos que han ido llegando al mercado, como hablar de superficie de protección en lugar de superficie de ataque, “una superficie más pequeña, que incluye todos los activos, todos los procesos potencialmente vulnerables”.

Desayuno ITDS

Para el directivo de Thales el viaje hacia Zero Trust parte del momento “en que la empresa empiece a enfocar sus esfuerzos, sus proyectos y sus inversiones a este nuevo paradigma”. Asegura que hay diferentes planteamientos, como puede ser el partir de una solución que esté creada y enfocada alrededor del Zero Trust.

Javier Campo prefiere hablar de ‘proyecto’ Zero Trust más que viaje, un proceso continuo, “que no es un objetivo que podamos alcanzar en un año o en seis meses, sino que es un proceso continuo en donde hay que equilibrar el escenario actual con los mecanismos de seguridad”. Añade que “tenemos que garantizar que cada actividad de nuestros usuarios, que cada dato que estos consuman, que cada recurso con el que estén interactuando esté cien por cien protegido y siempre con la premisa de que no sabemos desde dónde va a venir al ataque”.

Habla Pedro García Villacañas del origen de Zero Trust, un concepto que partió de John

#DESAYUNOITDS.
AFRONTANDO EL MODELO ZERO TRUST

CLICAR PARA VER EL VÍDEO

Kindervag, un analista de Forrester que propuso desechar la distinción entre lo externo y lo interno y centrarse en los activos, de forma que “la esencia de Zero Trust al final supone una ausencia de zonas de confianza y en donde son los usuarios, los dispositivos o las aplicaciones las que se ven sometidos a esos procesos de verificación”. Menciona el Modelo BeyondCorp de Google como una de las primeras implementaciones de modelo Zero Trust en una gran empresas, “uno de los modelo más reconocibles a nivel global” cuya implementación ha llevado a Google casi diez años.

Dibuja Sergio Martínez un modelo de seguridad por capas en el que Zero Trust añade una capa más en el acceso remoto.

Raúl D’Opazo habla de identidad digital como una de las claves de Zero Trust en tanto en cuanto son las que al final te permiten acceder al dato, que es el valor de una compañía. Al final es tomar conciencia de que ese paradigma ha cambiado,

"La pieza fundamental en la adopción de una solución Zero Trust es tener muy claro el mapeado de aplicaciones, datos y usuarios que hay dentro de la compañía, sea grande o pequeña"

Sergio Martínez,
Iberia Regional Manager, SonicWall

dice el directivo de OneIdentity, añadiendo que hay que tener en cuenta mucho elementos y que las compañías "han empezado este camino hace tiempo, quizás no con un foco muy específico, pero es un camino que tiene que continuar".

Zero Trust en la empresa española

Preguntamos a nuestro grupo de expertos si la empresa española está preparada y concienciada para la adopción de un modelo Zero Trust que mejore su posición frente a los ciberdelincuentes. Asegurando que la empresa española no tiene porqué ser particularmente diferente a las empresas de cualquier otro país, dice Guillermo Martín Soto que, "como siempre, dependiendo de del vertical concreto al que pertenezca la empresa, puede haber más o menos resistencia al cambio. Pero al final este modelo de Zero Trust es algo que se impone por sí mismo".

Coincidiendo en que la empresa española está concienciada respecto a la seguridad, apunta Javier Campo que el problema está "en su capacidad de adaptación a los tiempos actuales o a cualquier otra circunstancia", añadiendo que conocen los riesgos, "pero no les da tiempo a adaptarse en un tiempo razonable para poder expandir el concepto de Zero Trust a los diversos escenarios por los que estén pasando".

La empresa española no sólo está concienciada "sino también preparada para adaptar este modelo", ha dicho Pedro García, añadiendo que la pandemia y el impulso del teletrabajo han podido acelerar la toma de decisión en la implementación de este modelo, aunque no todas las empresas lo van a hacer al mismo tiempo o durante el mismo tiempo.

A grandes retos, grandes soluciones

Para finalizar el debate pedimos a los expertos en seguridad que hagan sus propuestas para ayudar a las empresas a hacer frente al modelo Zero Trust.

SonicWall.

Primer fruto de la inversión de la compañía en Perimeter 81, destaca Sergio Martínez el producto Cloud Edge, un ZTNA (Zero Trust Network Access) para acceso remoto desde decenas a miles de usuarios; una aplicación cloud nativa y por suscripción que se despliega en minutos, con muy baja latencia y que ofrece tecnologías muy innovadoras.

One Identity.

Para la compañía el perímetro de seguridad es la identidad, una identidad digital tanto nominal como privilegiada, como una identidad de un proceso automático, de un robot, de lo que sea... La propuesta de la compañía, híbrida, se centra en la gestión de identidades y cuentas privilegiadas, así como la securización de entornos Active Directory y Azure.

Sophos.

La compañía sigue apostando por su consola unificada Sophos Central, desde la que se gestionan los Gateways, on-premnise y nube, así como el propio Endpoint, que integra un sistema de acceso para comprobar que el usuario es el correcto y la seguridad del equipo la que debe ser.

Thales.

La compañía lleva 30 años ofreciendo soluciones de autenticación fuerte con diferentes tecnologías, pero hace cinco años se elaboró, alrededor del modelo Zero Trust, una solución para entornos cloud e híbridos que por defecto va a establecer un SSO de acceso a todas las aplicaciones y servicios de la empresa pudiendo subir o bajar el nivel de seguridad en función de la criticidad del servicio al que se está accediendo.

Netskope.

La compañía se fundó con la idea de aplicar seguridad al dato en un escenario, el cloud, en el que las empresas no eran capaces de interpretar a bajo nivel todas las actitudes de los usuarios contra dichas aplicaciones. Nosotros damos esa visibilidad y permitimos a las empresas aplicar controles granulares a través de NewEdge, la red de seguridad de la compañía.

Kaspersky.

Esta aplicación de política de confianza cero se está basada en gran medida en la visibilidad en tiempo real, y desde Kaspersky ofrece información sobre el tipo de hardware del equipo, versiones de sistema operativo, niveles de parche de aplicaciones o de vulnerabilidades, aplicaciones instaladas, qué accedo, y la detección en tiempo real de los eventos de posibles incidentes y movimiento de seguridad.

Para Sergio Martínez la empresa española está preparada para el modelo Zero Trust, “y si no lo está, lo va a estar”. Añade el director general de SonicWall para España y Portugal que según datos de Gartner el 60% de las compañías habrán migrado del modelo tradicional de VPN “al que nos abocamos el año pasado a un entorno de Zero Trust Network Access, y esto es debido a la gran inversión que va a haber en los próximos años”.

Para Raúl D’Opazo la empresa española no está por detrás de otros países en seguridad, aunque reconoce que se está moviendo todo muy rápido. Identifica el Solutions Architect de One Identity algunas carencias, como

concienciarnos de que “la seguridad no sólo depende del Departamento de Seguridad, sino que es de todos”.

La empresa española “tiene que estar preparada; lo necesita”, dice Alberto Ruiz Rodas. Apunta también este directivo de Sophos que irán poco a poco, pero que, igual que han ido adaptándose o ha ido adquiriendo los nuevos sistemas de protección, adoptarán también este modelo.

¿Qué necesito para adoptar Zero Trust?

“Hay que empezar a directamente localizar dónde están nuestros activos, qué se está haciendo con ellos y cómo protegerlos”, dice el portavoz de Netskope cuando preguntamos qué necesita una empresa que quiera implementar un modelo de Zero Trust, añadiendo que no puede ser un concepto de marketing sino una verdadera apuesta por el “no me fío de nada, tengo que auditar y tengo controlado todo”.

Para Pedro García Villacañas no existe una receta, al tiempo que identifica cuatro puntos “que podrían ayudar a construir este sistema”. El primero sería la microsegmentación; en segundo lugar, acotar los privilegios, otorgando el menor número de privilegios a cada usuario; el tercer punto es la autentificación y por último el tener el mayor control posible sobre tu infraestructura.

“La pieza fundamental en la adopción de una solución Zero Trust es tener muy claro el mapeado

"El modelo Zero Trust viene a solucionar, sobre todo, los problemas de seguridad tradicional"

Alberto Ruiz Rodas, Presales Engineer for Spain and Portugal, Sophos

"La identidad digital es una de las claves de Zero Trust en tanto en cuanto son las que al final te permiten acceder al dato, que es el principal valor de una compañía"

Raúl D'Opazo, Solutions Architect, One Identity

de aplicaciones, datos y usuarios que hay dentro de la compañía, sea grande o pequeña", asegura Sergio Martínez, añadiendo que "no es algo trivial". A partir de este mapeado, "darle valor a los datos y saber quién accede a qué en cada momento".

Para Raúl D'Opazo es fundamentar empezar analizando qué es lo que tienen. Tampoco es algo trivial, ya que son muchas las empresas que no saben cuántas aplicaciones tienen ni quiénes son los responsables de esas aplicaciones.

Coincide Alberto Rodas en que es primordial tener en cuenta ese inventariado y qué permisos necesito, "y luego tener claras las consecuencias de, por ejemplo, permitir un acceso desde un ordenador que no es el habitual". También hay que tener en cuenta que se trata de un modelo que se va a ir implementando poco a poco.

Coincidiendo con sus compañeros de debate, dice Guillermo Martín Soto que lo que deben tener en cuenta las empresas para implementar un modelo de Zero Trust "son tres cositas que parecen fáciles de definir conceptualmente, pero cuya ejecución no es algo trivial". Se necesita saber qué usuarios tengo, y qué tipo de usuarios son, a qué aplicaciones pueden acceder, en función de

"Dependiendo del vertical concreto al que pertenezca la empresa puede haber más o menos resistencia al cambio, pero al final este modelo de Zero Trust es algo que se impone por sí mismo"

Guillermo Martín Soto,
Regional Sales Manager, Spain, Portugal
& North Africa - IAM, Thales

qué dispositivos… y con esas variables ir creando políticas de acceso.

¿Dónde encuentro el mejor proveedor de Zero Trust?

"Que no espere encontrar un único proveedor de Zero Trust porque no existe", dice Pedro García Villacañas cuando planteamos qué tiene que buscar a la hora de escoger un proveedor para hacer frente a la adopción de un modelo de Zero Trust. "Va a requerir de la colaboración de muchos departamentos internos y de la relación con distintos proveedores", asegura el directivo de Kaspersky.

Coincide Sergio Martínez en que Zero Trust "es un concepto de marketing que va cristalizando poco a poco en determinadas estrategias de producto y de servicio", y añade que poco a poco irán apareciendo, dentro de portfolio de todos los fabricantes herramientas que incorporan filosofías de Zero Trust.

El concepto de Zero Trust se está utilizando a nivel de marketing, "pero realmente no hemos sacado un nuevo producto para hacer Zero Trust", dice Raúl D'Opazo, explicando que lo que se necesita es buscar un buen partner tecnológico que lo acompañe en su camino.

"La adopción de Zero Trust empieza localizando dónde están nuestros activos, qué se está haciendo con ellos y cómo protegerlos"

Javier Campo Azofra, Sales Engineer, Netskope

Para Alberto Ruiz Rodas "puede ser interesante que los clientes busquen compatibilidades con sus actuales sistemas", de forma que puedan ampliarse las capacidades de lo que ya se tiene "para facilitar esta adaptación tecnológica a este nuevo paradigma".

Coincidiendo es que sería necesaria la participación de más de un proveedor de Zero Trust, apunta Guillermo Martín que dentro de esa selección se pusiera foco en "la generación de políticas en torno al usuario, las aplicaciones y los dispositivos", añadiendo que debe buscarse un equilibrio entre la seguridad "y hacerle la vida fácil al usuario".

Teniendo en cuenta que el dato es el activo más importante de la empresa, lo que sugeriría Javier Campo a una empresa que busca proveedor de Zero Trust es que "se centre en proteger ese dato", añadiendo que es importante "no bloquear los accesos que tienen los usuarios a ciertas aplicaciones cloud, a ciertos sitios web". it

Enlaces de interés...

- La seguridad 'Zero Trust' moverá 51.600 millones de dólares en cinco años
- Zero Trust ¿Quién le pone el cascabel al gato?

Compartir en RRSS

it User
TECH & BUSINESS

Cada mes en la revista, cada día en la web.

La importancia de DevSecOps

Hace tiempo que las organizaciones adoptaron el modelo DevOps para respaldar ciclos de desarrollo y lanzamiento de aplicaciones extremadamente rápidos capaces de satisfacer las demandas de la transformación digital. Pero sin incorporar pruebas de la seguridad a las aplicaciones en estos procesos de DevOps, el riego que corren estas organizaciones, y los usuarios y empresas que utilizan este software, es considerable. DevSecOps viene a mejorar la seguridad en ese modelo de desarrollo de aplicaciones.

La mayoría de las organizaciones están cambiando hacia arquitecturas de confianza cero para hacer que sus entornos de aplicaciones sean más seguros al tiempo que la adopción de DevSecOps continúa acelerándose. Según el informe The 2021 State of DevSecOps, el 75% de las empresas con una facturación de más de mil millones de dólares, han implementado procesos de DevSecops en el desarrollo actual de aplicaciones. Entre las razones que lo impulsan destacan la mejora de la seguridad y calidad de las aplicaciones (54%) o poder llevas las aplicaciones más rápido al mercado (30%). Los encuestados también mencionaron los principales obstáculos a los que se enfrenta DevSecops, como son los desafíos técnicos (60%), el coste (40%), falta de formación (38%) o falta de habilidades (36%)

Se prevé que todas las organizaciones adoptarán las mejores prácticas de DevSecOps, ¿pero a qué ritmo? La cantidad de aplicaciones que las organizaciones están implementando continúa acelerándose, pero la confianza en las mejores prácticas de DevSecOps para garantizar la seguridad y el cumplimiento sigue siendo desigual, en el mejor de los casos. Las organizaciones más grandes que tienen los recursos necesarios para financiar estas iniciativas tienden a estar más avanzadas en su proceso de adopción. Sin embargo, no existe una correlación entre el tamaño de la organización y la capacidad de crear e implementar aplicaciones seguras.

DevSecOps ofrece la visibilidad, automatización y colaboración mejoradas que necesitan para garantizar la seguridad y confiabilidad de sus aplicaciones ahora y en el futuro

Pero empecemos por el principio, cuando durante el desarrollo de aplicaciones la seguridad era el último elemento a tener en cuenta durante el proceso. Es más, la seguridad de las aplicaciones ni siquiera era responsabilidad del desarrollador, sino del equipo que testaba el código y reportaba posibles problemas, tanto de ejecución y funcionalidad, como de seguridad. Eran los tiempos de desarrollo siguiendo el Waterfall Software Development Life Cycle (SDLC), un modelo de ciclo de vida secuencial lineal rígido con seis etapas: Requisito, Recopilación (análisis), Diseño, Desarrollo (codificación), Pruebas, Operaciones de mantenimiento.

La rigidez de este modelo se puso de manifiesto durante la década de los 90, según explica en un post Ayush Singh, Global Manager de K2 Cybersecurity. La siguiente fase fue buscar un modelo que permitiese el desarrollo continuo y no necesariamente lineal.

Este nuevo modelo se encontró en el Snowbird Ski Resort de Utah, donde un grupo de líderes de la industria crearon el Manifiesto Ágil, compuesto por cuatro secciones que determinan:

- **Individuos e interacciones sobre procesos y herramientas**
- **Software de trabajo sobre documentación completa**
- **Colaboración con el cliente sobre la negociación de contratos**
- **Responde al cambio sobre el siguiente plan**

it whitepapers

5 CONSEJOS CLAVE PARA PASAR FÁCILMENTE A DEVSECOPS

Con el propósito de adentrarse en los procesos DevOps, la seguridad debe ser rápida, precisa y, lo más importante, automatizada. En este documento encontrarás cinco claves para crear un entorno DevSecOps.

Los marcos de DevSecOps tienen numerosos beneficios cuando se integran en la cultura empresarial y las mejores prácticas

El cambio con respecto al modelo Waterfall, que dependía en gran medida de la documentación y la planificación excesiva, con una participación mínima del cliente, fue bienvenido. Con el nuevo manifiesto, que llegó en un momento de gran demanda de aplicaciones con nuevas capacidades debido al crecimiento de Internet, las aplicaciones podrían entregarse a un ritmo más rápido, lo que convirtió al tiempo en un elemento importante en el desarrollo de aplicaciones.

El proceso de desarrollo ágil ofrece una serie de ventajas respecto al modelo anterior de desarrollo rígido en cascada. La metodología Ágil mejora la calidad del producto al fomentar el enfoque proactivo de los miembros del equipo en la búsqueda de la excelencia del producto. Además, la integración, comprobación y mejora continua de las propiedades del producto mejora considerablemente el resultado final. Por otra parte, el cliente está más satisfecho al verse involucrado y comprometido a lo largo de todo el proceso de desarrollo. La división del trabajo por distintos equipos y roles junto al desarrollo de reuniones frecuentes permite una mejor organización del trabajo. No hay que olvidar que las métricas utilizadas para estimar parámetros como tiempo, coste, rendimiento, etc. son normalmente más reales en proyectos ágiles que en los tradicionales. Gracias a la división en pequeños equipos y fases podemos ser más conscientes de lo que está sucediendo.

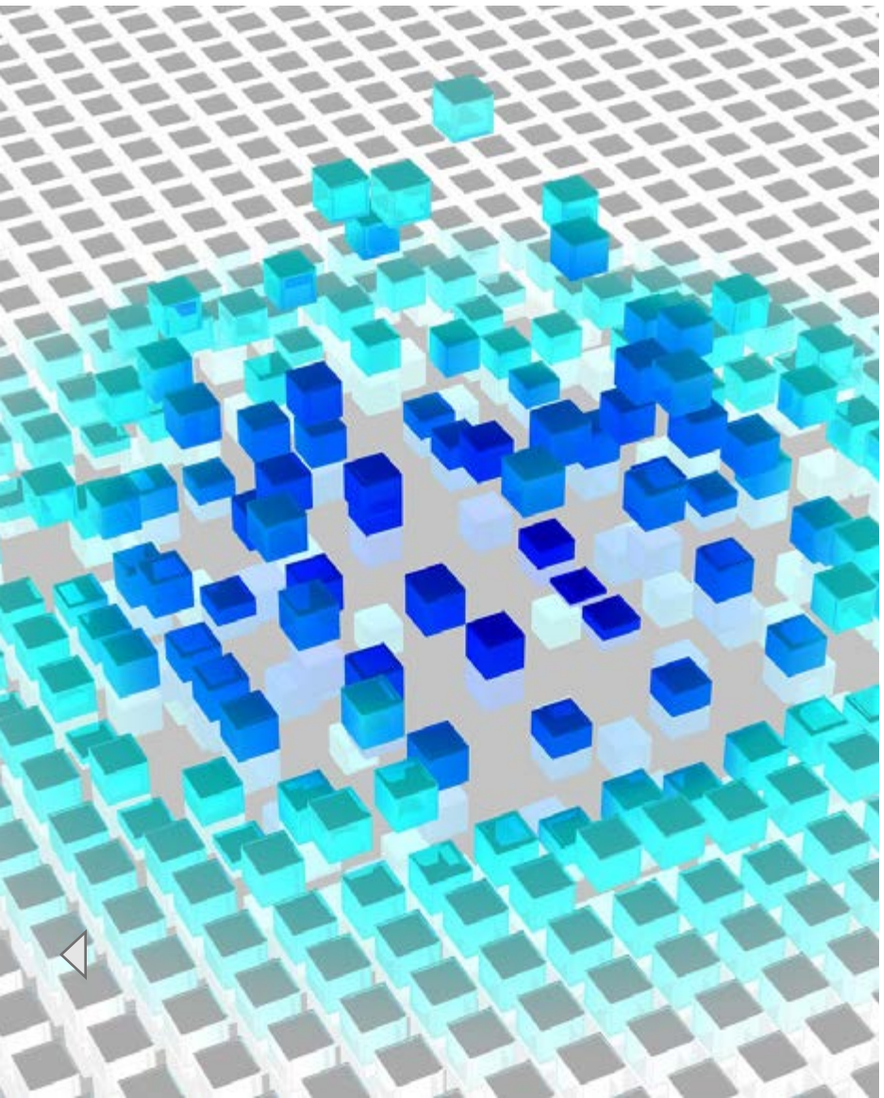
La metodología creada en el Snowbird Ski Resort de Utah ofrece la oportunidad de revisar y adaptar el producto a lo largo del proceso ágil, permite a todos los miembros del proyecto ejercer un mayor control sobre su trabajo, cosa que permite mejorar la capacidad de predicción en tiempo y costes. Y finalmente, la gestión ágil del proyecto elimina prácticamente la posibilidad de fracaso absoluto en el proyecto, porque los errores se van identificando a lo largo del desarrollo en lugar de esperar a que el producto esté acabado y toda la inversión realizada.

El marco Agile es una mejora del SDLC, pero la seguridad aún no estaba presente como elemento protagonista. El mercado empezó a darse cuenta de que la seguridad seguía siendo una ocurrencia tardía en la implementación e integración continuas de Agile para el desarrollo de aplicaciones.

DevOps

Lo que comenzó con el modelo Waterfall, pasó a la metodología Agile SDLC, seguía evolucionando hacia una nueva cultura de desarrollo. Llegaba la

DevSecOps (Development Security Operations) es la práctica de incorporar seguridad de forma continua a lo largo del ciclo de vida del desarrollo de la aplicación



¿QUÉ ES DEVOPS Y DEVSECOPS? **CLICAR PARA VER EL VÍDEO**

era de DevOps, una abreviatura de la combinación de Desarrollo y Operaciones.

Explica Ayush Singh que, si bien las metodologías Waterfall y Agile eran lineales y mapearon las actividades del proyecto en diferentes fases secuenciales respectivamente, DevOps allanó el camino para un nuevo ecosistema de equipos de desarrollo y operaciones que trabajan juntos para un SDLC proactivo.

DevOps no sólo es un cambio en los modelos de desarrollo, es un cambio cultural. La cultura DevOps, que proviene de una plataforma similar a los flujos de trabajo de productividad de TI de Agile, tiene el objetivo de eliminar la latencia entre departamentos aislados, que están plagados de falta de comunicación, departamentos desincronizados y partes interesadas dispares. DevOps es la unión de personas, procesos y productos diseñados para permitir la entrega continua de valor a los usuarios finales.

DevOps se basa en tres principios continuos: integración, entrega e implementación. Con la

¿Qué se prioriza en AppSec en 20121?

PortSwigger es una empresas dedicada a ofrecer soluciones para mejorar la estrategia de la seguridad de aplicaciones. Asegurando que los eventos de 2020 crearon un catalizador para la adopción de tecnología en todos los niveles de negocio, dice la compañía que han aparecido una serie de nuevas preocupaciones de seguridad que deben conciliarse. Para comprender dónde se encuentran en su viaje de madurez de seguridad y dónde se veían en los próximos 12 meses, PortSwigger realizó una encuesta cuyos resultados se agrupan en tres tendencias en la seguridad de las aplicaciones:

DevSecops es un viaje, no un destino en el que las empresas deberían embarcarse para encontrar y replicar eficiencias e introducir la automatización en el proceso de desarrollo de software. Enfocado de esta manera, proporciona un marco de productividad que puede acelerar el avance de un negocio. El 18% de los encuestados indicaron que se prepararán para comenzar DevSecOps en los próximos 12 meses. Un 28% adicional informó que ya tiene un programa DevSecOps maduro. Otro 50% de las empresas tiene indicadores tempranos de preparación para DevSecOps y ya han integrado capacidades de prueba de seguridad en sus canales de desarrollo.

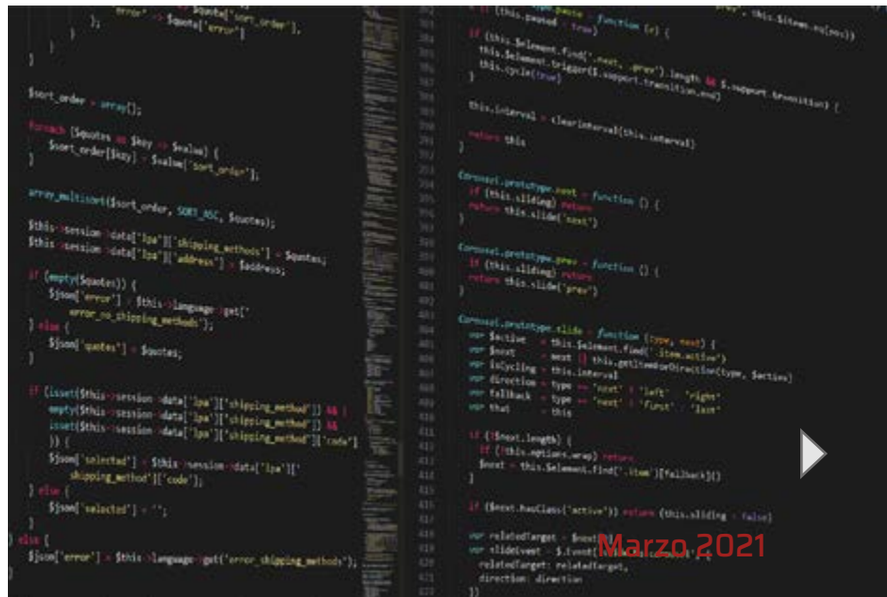
La automatización es el mapa del viaje DevSecOps. Dice PortSwigger que no se puede saber qué camino hay que tomar mientras no se sepa dónde se encuentra y que con el fin de aumentar las capacidades de seguridad de las aplicaciones, las empresas invertirán su presupuesto en automatización, elemento clave para permitir que las grandes empresas escalen el escaneo en sus grandes propiedades web. Al automatizar más actividades manuales, las empresas también liberarán tiempo y recursos de seguridad de las aplicaciones (58%) que se pueden implementar para servir a los equipos de desarrollo (44%) y ahorrar costes (42%), todo mientras escalan el escaneo en una mayor cantidad de aplicaciones (56%).

¿Quién tendrá éxito en el viaje? Más de un tercio de las empresas encuestadas informaron que su equipo de AppSec es responsable de más de 200 aplicaciones; al automatizar los análisis que alguna vez fueron una actividad manual y, por lo tanto, que consumía mucho tiempo, los líderes de AppSec tienen tiempo para concentrar sus esfuerzos en vulnerabilidades complejas y más difíciles de encontrar. Al introducir la automatización de esta manera, las vulnerabilidades que requieren un pensamiento lateral y una explotación guiada por humanos pueden convertirse en la prioridad clave. Casi dos tercios de las empresas encuestadas están invirtiendo en capacitación y perfeccionamiento de los miembros de su equipo de seguridad existente.

integración continua vienen las actividades de desarrollo básicas que incluyen codificación, diseño, construcción, integración y pruebas. La entrega continua incluye la entrega regular de aplicaciones y actualizaciones de software, y se realiza con una implementación continua o un flujo de trabajo automatizado.

Llegados a este punto, innovaciones como contenedores y microservicios han allanado el camino para la automatización, lo que ayuda a garantizar que la seguridad sea parte del proceso y garantiza que la seguridad también se integre en las fases posteriores del ciclo de vida del desarrollo de la aplicación.

Recordemos que antes de la era de Devops, la seguridad era una ocurrencia tardía. Encontrar y minimizar las vulnerabilidades no era tarea de los desarrolladores. En un enfoque tradicional de DevOps, las pruebas de seguridad se realizan cerca del final del proceso de desarrollo, generalmente



una vez que la aplicación se ha implementado en un entorno de producción. Esto se debe a que las tareas relacionadas con la seguridad, como la gestión segura de la configuración y el análisis de vulnerabilidades, pueden consumir bastante tiempo, lo que ralentiza el proceso de desarrollo.

DevSecOps

DevSecOps (Development Security Operations) es la práctica de incorporar seguridad de forma continua a lo largo del ciclo de vida del desarrollo de la aplicación, lo que garantiza que la seguridad sea una parte fundamental de la aplicación y no una función incorporada.

Aunque mantener las pruebas de seguridad hasta una fase avanzada del ciclo de desarrollo aumenta la velocidad general del proceso, las vulnerabilidades dentro de la aplicación no se identificarán hasta que la aplicación esté casi completa, lo que obligará al equipo de DevOps a retroceder y abordar estos problemas de seguridad. Esto requiere que las organizaciones repitan todo el proceso de desarrollo para abordar las vulnerabilidades de seguridad, lo que va en contra de la teoría misma de DevOps, que se centra en ciclos rápidos de desarrollo y lanzamiento.

De forma que en un enfoque de DevSecOps, la seguridad está integrada en cada parte del ciclo de vida de DevOps. Las tácticas clave para una correcto planteamiento de un modelo de DevSecOps parte por incorporar profesionales de seguridad dentro del equipo de DevOps para supervisar la agenda de seguridad dentro del ciclo de vida del desarrollo; Elevar el conjunto de habilidades de seguridad del equipo de TI para comprender los riesgos cibernéticos y las mejores prácticas para que cada miembro pueda considerar las implicaciones durante el proceso de desarrollo y escribir código teniendo en cuenta la seguridad; Automatizar determinados procesos y tareas de ciberseguridad, como las pruebas de vulnerabilidades de seguridad, para permitir un flujo de trabajo ágil; y desarrollar procesos y herramientas de seguridad diseñados específicamente para admitir tecnologías ágiles, como la nube, los contenedores y los microservicios.

La importancia de DevSecOps

DevSecOps nunca ha sido más crítico que ahora. Los últimos meses se ha visto una aceleración de la transformación digital, un drástico incremento de aplicaciones cloud. La importancia de la seguridad nunca caló tanto como el año pasado, y nunca ha

> Antes de la era de DevOps la seguridad era una ocurrencia tardía. Encontrar y minimizar las vulnerabilidades no era tarea de los desarrolladores

Mejores prácticas para implementar DevSecOps

La integración exitosa de la seguridad en las canalizaciones de DevOps a través de DevSecOps requiere la adopción de ciertas herramientas, recursos y prácticas que pueden unir a los equipos de desarrollo, operaciones y seguridad en el ámbito de la cultura DevSecOps.

1. Determinar qué debe asegurarse

El código es código: a menos que tenga un valor específico como propiedad intelectual para la empresa, no tiene valor. Sin embargo, los datos que trata el código son los que diferencian a una organización de sus competidores. Y aquí es donde reside el valor. Por lo tanto, el enfoque debe ser proteger los datos. Un servicio bien codificado debería poder separar diferentes flujos de datos dentro de sí mismo.

2. Mantener la seguridad entre servicios

Una arquitectura basada en microservicios dependerá de las interfaces de programación de aplicaciones (API) entre los diversos servicios involucrados. La seguridad de las API, tanto en la forma en que el equipo de desarrollo escribe el código de servicio como en los servicios externos a los que se llama, debe mantenerse y comprobarse continuamente. Los desarrolladores deben incluir la seguridad adecuada en todo el código de servicio y el equipo de operaciones debe asegurarse de que las API sean monitorizadas para mantener comunicaciones seguras en todo momento.

3. Implementar las herramientas adecuadas

No asuma que las herramientas DevOps existentes administrarán la seguridad por usted. Para adherirse a las mejores prácticas de DevSecOps, busque herramientas que puedan verificar la seguridad del código frente a problemas conocidos y, preferiblemente, problemas de día cero en tiempo real.

4. Garantizar la seguridad entre el dispositivo de acceso y los servicios de back-end

Observe cómo el dispositivo de acceso y su cliente acceden a los servicios de back-end y adopte autenticación multifactor, utilice cifrado para flujos de datos y vincule la identificación del usuario en un sistema de directorio granular basado no solo en el nombre y la función de la persona, sino también en dónde se encuentra, el tipo de conexión que se utiliza y el nivel de valor definido en cuanto a los datos a los que se accede.

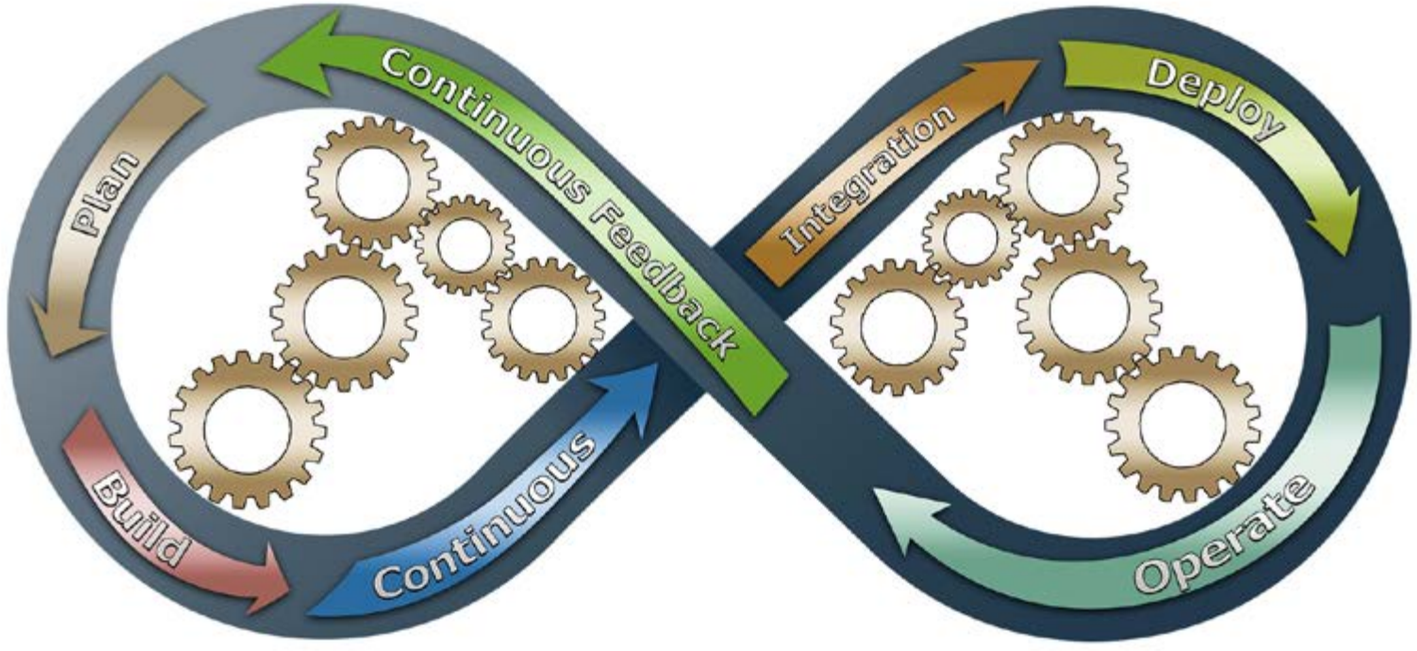
DevSecOps ayuda a los equipos a tomar mejores decisiones desde el principio de sus proyectos, ya que a medida que se introducen nuevas funciones o componentes de un proyecto, los equipos trabajan juntos para garantizar que todas las capas de protección necesarias se introduzcan correctamente y sean escalables.

Una realidad importante en el panorama digital actual es que todos participan en la protección de los datos. Esto incluye empresas, sus equipos de DevOps y socios externos. El estado actual de la industria y los estándares de cumplimiento que la rigen exigen que las empresas fomenten una cultura transparente y responsable. DevSecOps ayuda a lograr esto al reunir a las personas, los procesos y las herramientas necesarias para cambiar la seguridad a una posición más prominente.

quedado tan en evidencia que con la brecha de seguridad de SolarWinds.

Como hemos dicho, DevSecOps consiste en desarrollo, seguridad y operaciones. Es un marco empresarial diseñado para integrar la seguridad en cada fase del ciclo de desarrollo de software. Es decir, integra la seguridad en las fases de construcción, prueba, lanzamiento, soporte y mantenimiento del proceso de desarrollo.

Los marcos de DevSecOps tienen numerosos beneficios cuando se integran en la cultura empresarial y las mejores prácticas. Para empezar,



A medida que el mundo continúa evolucionando y remodelando la forma en que los proveedores ofrecen aplicaciones y servicios a sus clientes, es vital que las empresas informen a sus desarrolladores sobre los riesgos. Las brechas de ciberseguridad continúan afectando a las empresas en casi todas las industrias, y el daño que causan al nombre de una marca puede ser difícil de recuperar. Sin embargo, mediante el uso de un marco DevSecOps y la construcción de un nuevo estándar en la conciencia de seguridad para los equipos de desarrollo, las empresas pueden reforzar la importancia de la protección en todos los niveles. Al confiar en un enfoque de DevSecOps, puede mejora la velocidad y la agilidad de la seguridad; automatizar mejor en cada nivel del ciclo de vida del desarrollo de software; mejorar la comunicación y el trabajo en equipo entre departamentos; detectar los riesgos de codificación con anticipación e incrementar la productividad y el cumplimiento.

La forma en que se hacen los negocios a escala global está cambiando rápidamente. La necesidad de velocidad y seguridad en todas las áreas comerciales nunca ha sido tan grande. Las empresas necesitan adaptar rápidamente sus aplicaciones para seguir siendo viables en este nuevo clima, y DevSecOps ofrece la visibilidad, automatización y colaboración mejoradas que necesitan para garantizar la seguridad y confiabilidad de sus aplicaciones ahora y en el futuro.

> El marco Agile era una mejora del SDLC, pero la seguridad aún no estaba presente como elemento protagonista

Los retos de adopción de DevSecOps

Un informe reciente descubrió que el mercado de herramientas de seguridad de aplicaciones experimentará un crecimiento explosivo hasta 2025. El estudio también analiza las razones por las que las herramientas de AppSec no se utilizan como cabría esperar.

Más herramientas no equivalen a menos problemas. A medida que las empresas evolucionan sus procesos de desarrollo de software, pasando de Agile a DevOps a DevSecOps, es inevitable que se compren varios escáneres, monitores, cortafuegos y todo tipo de herramientas de AppSec en el camino. Con presupuestos y recursos de expertos cada vez más limitados, tratar de deshacer el desorden y encontrar la mejor ruta de herramientas a seguir se ha convertido en una tarea abrumadora, y el código que necesita escaneo y corrección sigue llegando. La conclusión es que un conjunto de herramientas inmanejable, sin importar cuán nuevo y brillante sea, no permite que una organización adiopte el 'plug&play' en un proceso funcional de DevSecOps.

Las herramientas de escaneo son lentas, lo que impacta en la agilidad. Lograr seguridad mientras se codifica a alta velocidad se ha convertido en un gran desafío para muchas organizaciones, y todavía estamos tratando de hacerlo bien incluso cuando instamos a un enfoque DevSecOps. La revisión manual y meticulosa del código podría haber funcionado como

DevSecOps integra la seguridad en las fases de construcción, prueba, lanzamiento, soporte y mantenimiento del proceso de desarrollo

seguridad a prueba de fallas en la década de 1990, pero en un momento en el que estamos produciendo líneas de código por cientos de miles de millones, es demasiado lento y no muy efectivo.

Ninguna herramienta única encuentra todas las vulnerabilidades, y hay algunos problemas evidentes con los resultados que normalmente recibe un equipo de seguridad después de un escaneo, como la existencia de demasiados falsos positivos. Además, los escáneres detectan problemas, no los solucionan.

Por lo tanto, incluso en una organización que está haciendo todo lo posible para cumplir con las mejores prácticas de ciberseguridad e incluir la seguridad en cada etapa del proceso, si su dependencia está en los escáneres, no alcanzarán el verdadero éxito de DevSecOps.

Es difícil lograr un equilibrio entre herramientas y personas. Las empresas que adoptan DevSecOps se esfuerzan por hacer de la seguridad una responsabilidad compartida, y para las organizaciones que crean el software que impulsa nuestras vidas, desde la red eléctrica hasta nuestros timbres, deben llevar a todos en el viaje para garantizar un mayor nivel de seguridad.

Las herramientas no lo harán todo, y ni siquiera es la forma más barata. Los mejores resultados se logran trabajando para mantener la seguridad en la mente del equipo de desarrollo, capacitándolos y construyendo una cultura de seguridad positiva dirigida por humanos, con un conjunto de herramientas que funciona para complementar sus esfuerzos.

nderlo". Como reto índice también el directivo de ExtraHop que estas soluciones no son baratas, pero que "en cinco años ninguna empresa importante va a vivir sin un NDR porque cada vez hay más ataques que sólo se pueden evitar a nivel de red".

Sin una herramienta NDR la posibilidad de que se produzcan compromisos e infracciones no detectados es un riesgo continuo. El caso de negocio para una plataforma NDR es simple: la evolución de los métodos de ataque justifica el uso de plataformas de detección de ciberseguridad que no pueden ser ignoradas por actores nefastos.

Enlaces de interés...

- DevSecOps Org.
- W 5 consejos clave para pasar fácilmente a DevSecOps
- Los cinco imprescindibles para implementar DevSecOps con éxito

Compartir en RRSS

it Reseller
TECH&CONSULTING
nº 65
MARZO 2021
Los ordenadores AiO se afianzan entre las tecnologías más demandadas
Evolución de los modelos de impresión y gestión documental, a debate
El gasto en tecnología en España para 2021 rozará los 45.300 millones de euros
Marketplaces:
nuevos modelos de venta de TI
it Reseller
TECH&CONSULTING
Cada mes en la revista,
cada día en la web.

ANETT MÁDI-NÁTOR

PRESIDENTA DE WOMEN4CYBER FOUNDATION

Actualmente responsable de Desarrollo Estratégico de Negocios en Cyber Services Plc., Anett Mádi-Nátor tiene más de una década de experiencia en niveles estratégicos y administrativos de seguridad de la información y ciberdefensa, tanto como experta en la materia del sector privado como representante del gobierno. Ahora es responsable del Desarrollo Comercial Estratégico en un proveedor de servicios de ciberseguridad especializado que opera a nivel internacional. Además, es presidenta de la Iniciativa y Fundación Women4Cyber lanzada por la Organización Europea de Seguridad Cibernética y la Comisión Europea.

Women4Cyber Spain
en el Día Internacional de la mujer

Women4Cyber es una fundación privada europea sin ánimo de lucro cuyo objetivo es promover, fomentar y apoyar la participación de las mujeres en el ámbito de la ciberseguridad.

El campo de la ciberseguridad sufre una enorme escasez de habilidades. La brecha, que se prevé que alcance los 1,8 millones en todo el mundo para 2022 y 350.000 solo en Europa, se ve agravada por la falta de representación femenina, ya que las mujeres representan solo el 11% de la fuerza laboral, según la investigación “Mujeres en ciberseguridad”. En Europa, el porcentaje es aún menor: 7%.

Las mujeres deberían contribuir a cerrar la brecha de habilidades, tanto desde el punto de vista de la igualdad de género como desde el punto de vista práctico. Las mujeres no pueden quedar al margen

Compartir en RRSS

Hoy aplaudimos a todas las mujeres y hombres que unen sus fuerzas para asegurar que en cuestión de tiempo se logre la neutralidad de género en la ciberseguridad

en este campo que ofrece salarios competitivos, oportunidades de crecimiento, seguridad laboral, emocionantes tareas diarias y la oportunidad de marcar la diferencia. Desde un punto de vista práctico, la escasez de habilidades simplemente no se puede salvar sin involucrar a la mitad de la fuerza laboral disponible.

Women4Cyber nació como una iniciativa de ECSO (European Cyber Security Organization Working) Group 5 - que se centra en la educación, la formación, la concienciación y los rangos cibernéticos. La Fundación tiene como objetivo ayudar a llenar la brecha de género de los profesionales de la ciberseguridad en Europa. El objetivo principal es alentar y promover la capacitación, la mejora y la recapacitación de niñas y mujeres hacia la educación y las profesiones en seguridad cibernética.

Para apuntar al campo de la ciberseguridad, intrínsecamente complejo, y satisfacer la creciente demanda de profesionales de la ciberseguridad en Europa, estamos trabajando en seis líneas de trabajo que son:

1. **Sensibilización, mejores prácticas y modelos femeninos**
2. **Programas de formación personalizados para mujeres**
3. **Mujeres en el mercado laboral de la ciberseguridad**
4. **Mujeres en la investigación e innovación en ciberseguridad, tecnologías emergentes y desafíos cibernéticos**
5. **Políticas nacionales y de la UE en consonancia con los mensajes de Women4Cyber**
6. **Asociaciones nacionales e internacionales**

Siguiendo la primera línea de trabajo, lanzamos la campaña Role Model, para presentar modelos femeninos en el campo de la ciberseguridad. La segunda parte de esta campaña es el “Libro 100 mujeres en ciberseguridad en Europa”. El libro se publicará en la segunda mitad de 2021, en el libro mostraremos y destacaremos a más de 100 mujeres y sus logros, con la esperanza de inspirar a más mujeres a unirse al campo de la ciberseguridad.

Además, en colaboración con la DG CNECT de la Comisión Europea, lanzamos el Registro de

Expertos Women4Cyber en julio de 2020 para identificar y mostrar una comunidad europea de mujeres profesionales en el campo de la ciberseguridad. El Registro de Expertos Women4Cyber reúne a mujeres de diferentes perfiles y puede servir como punto de referencia para grupos de expertos, organizadores de eventos y medios de comunicación, así como para oportunidades de colaboración y negocios. El Registro fue respaldado por la Vicepresidenta Ejecutiva de la Comisión Europea, Margrethe Vestager, la Vicepresidenta Margaritis Schinas y el Comisario Thierry Breton.

Otro de nuestros mayores logros es el establecimiento y coordinación de asociaciones nacionales e internacionales. Como somos conscientes de que cada ecosistema de ciberseguridad es diferente, fomentamos la creación de Capítulos del W4C que sean capaces de implementar activamente la misión y estrategias de la organización. Dado que los capítulos cuentan con expertos locales, están en una posición ideal para determinar las prioridades y los enfoques más adecuados para implementar nuestra misión en su área de acción.

En los últimos cinco meses, hemos aprobado siete capítulos nacionales, ¡de los cuales 5 ya se han lanzado!

El primer capítulo y el más activo hasta ahora ha sido el Capítulo español. Fue lanzado en octubre por su presidenta y fundadora Eduvigis Ortiz. La junta directiva está compuesta por un extraordinario grupo de mujeres expertas de alto nivel que trabajan en ciberseguridad en España: como Mar López Gil, Vicepresidenta; Rosa Díaz Moles, Vicepresidenta; Idoia Mateo, vicepresidenta; María de Miguel, Secretaría; Concepción Cordón, Daniela Kominsky, Maica Aguilar, Eva Roman, Julia Perea, Begoña García Pérez, Elena García Diez, Ana Ayerbe, Soledad Antelada y Beatriz Soto. El capítulo nacional obtuvo una inmensa respuesta desde su lanzamiento, mostrando el interés y el afán de la comunidad por contribuir a que la

A pesar de que el mundo ha logrado un progreso sin precedentes, ningún país ha logrado la igualdad de género

Enlaces de interés...

- Women4Cyber
- ‘Hay una voluntad real de que haya más diversidad’ (Eduvigis Ortiz)

El 8 de marzo es un día especial para todas las mujeres, y más aún para quienes trabajan en temas de género

ciberseguridad en España tenga un mayor equilibrio de género.

El 8 de marzo es un día especial para todas las mujeres, y más aún para quienes trabajan en temas de género. El Día Internacional de la Mujer es una ocasión para celebrar el progreso realizado hacia el logro de la igualdad de género y el empoderamiento de la mujer, pero también para reflexionar críticamente sobre esos logros y luchar por un mayor impulso hacia la igualdad de género en todo el mundo. Es un día para reconocer los actos asombrosos de mujeres que han desempeñado un papel extraordinario en la historia de sus países y comunidades, y para unirse, como una fuerza unida, para promover la igualdad de género en todo el mundo. Porque a pesar de que el mundo ha logrado un progreso sin precedentes, ningún país ha logrado la igualdad de género.

Hoy aplaudimos a todas las mujeres y hombres que unen sus fuerzas para asegurar que en cuestión de tiempo se logre la neutralidad de género en la ciberseguridad. Las estadísticas no mienten, el cambio ya está sucediendo. Seguramente, una o dos generaciones necesitan crecer e ingresar a la industria, pero cuanto más hacemos, cuanto más avanzamos, más mujeres podremos incluir.

¿Cuál es el futuro del mercado de almacenamiento?

¿Qué tecnologías son las más adecuadas para las empresas?

Descubra las últimas tendencias en el Centro de Recursos it User

Almacenamiento it

Con la colaboración de: FUJIFILM Value from Innovation Western Digital.

MARIO VELARDE BLEICHNER

GURÚ EN CYBERSEGURIDAD

Con más de 20 años en el sector de la CiberSeguridad, Mario Velarde Bleichner, Licenciado en Ciencias Físicas con especialidad en Calculo Automático y PDG por el IESE, ha participado en el desarrollo de esta industria desde la época del antivirus y el firewall como paradigma de la Seguridad IT, dirigiendo empresas como Trend Micro, Ironport, Websense, la división de Seguridad de Cisco Sur de Europa y la división Internacional de Panda Software.

Los Ciudadanos Digitales son nueva Humanidad del Antropoceno:

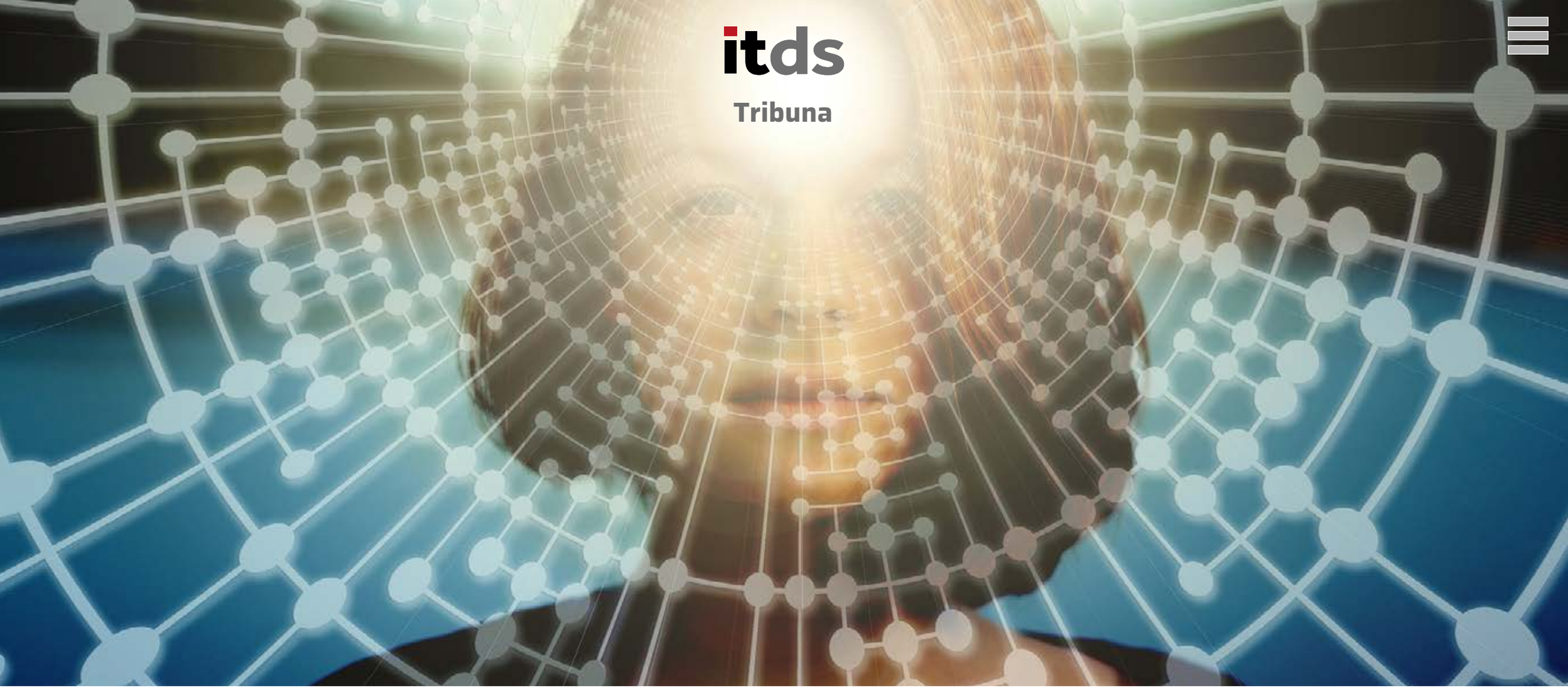
el inicio del Antropoceno Digital

Desde su introducción por el premio Nobel de Química Paul Crutzen el año 2000, el término Antropoceno ha ido ganando popularidad, aunque no es reconocido oficialmente por los organismos reguladores de la Ciencia Geológica.

El caso es que, oficialmente reconocido o no, describe perfectamente el desarrollo de la humanidad desde sus principios hasta la actualidad, especialmente en su relación con GAIA, nuestro planeta, durante al menos los últimos 15.000 años, desde que empezamos, como cazadores, las extinciones de animales para alimentarnos, hasta este último período de la Revolución Industrial con los terribles efectos del cambio climático.

En este período, la Humanidad ha llegado a tener casi 8.000 millones de individuos conviviendo al mismo tiempo con serias expectativas de llegar a 10.000 millones, y, en los últimos 50 años, ahora ya llamada Revolución Digital, ha realizado avances tecnológicos inimaginables tan solo hace 100 años.

Compartir en RRSS

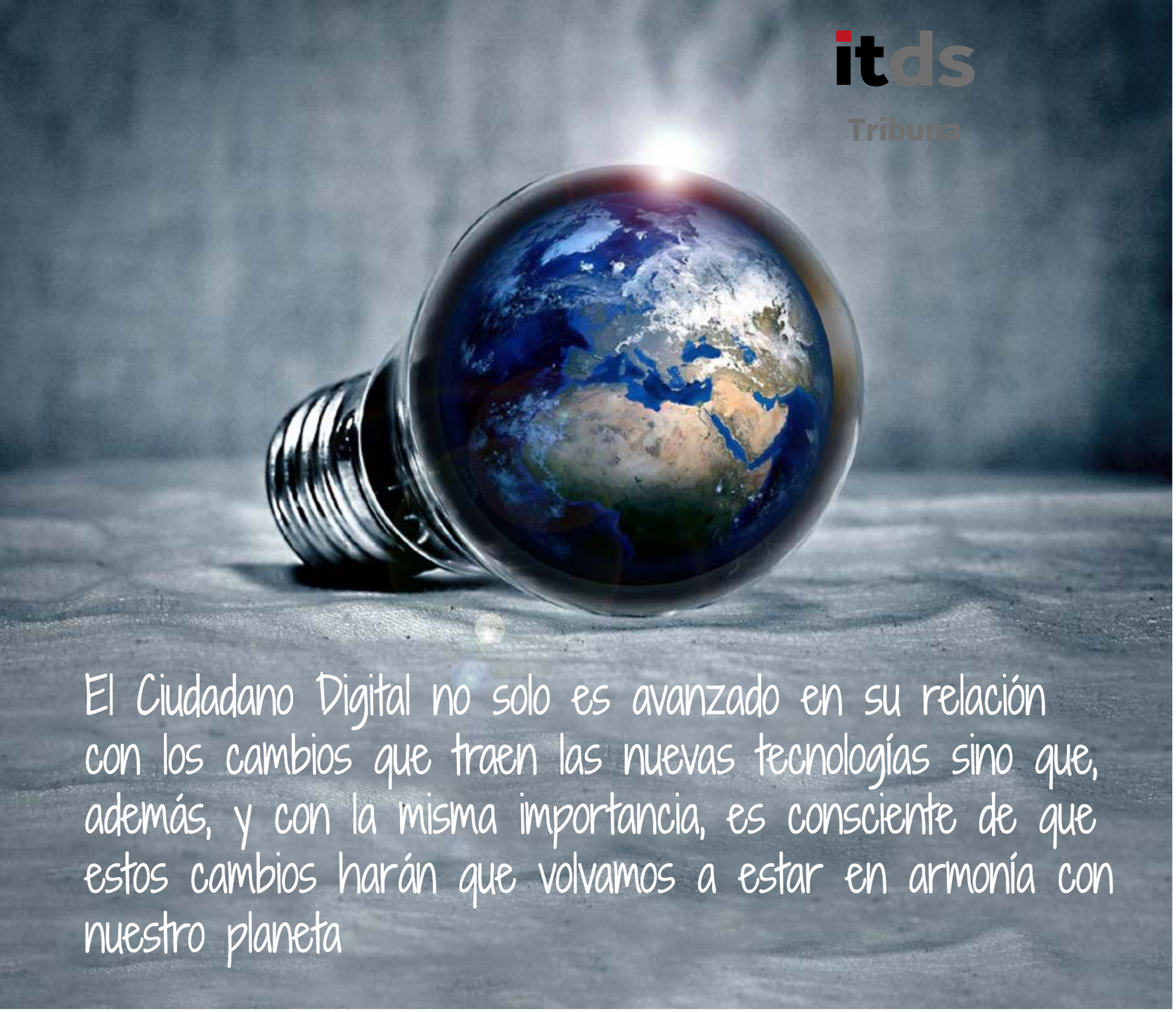


No digamos ya lo inimaginable que les resultaría la tecnología digital actual a los humanos en el inicio del Antropoceno Antiguo, hace 15.000 años, que tenían una población al borde de la extinción y cuyas mayores tecnologías eran las herramientas de piedra, el fuego, la caza y la recolección, y aún les quedaban otros 5.000 años antes de iniciar el gran cambio hacia la sociedad sedentaria que ha dado lugar a lo que somos ahora.

Podemos decir que con las grandes transformaciones digitales que han ocurrido en lo que va del siglo XXI y las expectativas de lo que va a ocurrir en lo que queda de este siglo, podríamos dar por finalizado el Antropoceno Antiguo y dar la bienvenida al Antropoceno Digital.

Las tecnologías digitales están haciendo posible el cambio en el paradigma de la movilidad, no solo dotando a los vehículos del futuro sino también en su capacidad de conexión las redes eléctricas

El Antropoceno Digital es parte de una era mucho más amplia que podría denominarse Antropoceno Moderno, y que en siglos venideros llevará a la Humanidad a avances inimaginables que hagan que nuestra realidad contemporánea quede tanto o más retrasada tecnológicamente que nuestros antepasados de hace 15.000 años lo están con respecto a nosotros.



El Ciudadano Digital no solo es avanzado en su relación con los cambios que traen las nuevas tecnologías sino que, además, y con la misma importancia, es consciente de que estos cambios harán que volvamos a estar en armonía con nuestro planeta

El Antropoceno Digital no solo es puro avance tecnológico que podría llevarnos a sociedades no sostenibles, es, entre otras cosas muy importantes, el cambio por la toma de conciencia de toda la Humanidad respecto a la salud nuestra Madre Tierra, para lo cual ya han llegado o están a punto ser viables otras muchas de las nuevas tecnologías que acompañaran a este cambio, como, son por ejemplo, las energías renovables, el reciclamiento de recursos en su modelo global incluyendo el agua, el aire, los residuos y cualquier otro recurso que nuestra Madre Tierra nos haya proporcionado en el pasado y en la actualidad para permitir el avance de la Humanidad hasta donde hemos llegado ahora.

Las tecnologías digitales darán el soporte para la realización de todos estos procesos de retorno a una relación simbiótica positiva con Nuestro Paneta y permitirán abordar problemas que se consideraban insolubles. En su avance mediante el buen uso de la Inteligencia Artificial, podrá ir proporcionando información vital para ayudar a tomar las mejores decisiones en las encrucijadas a las que la Humanidad tenga que hacer frente en el futuro.

Las tecnologías digitales harán posible el cambio para un mejor y más eficiente uso de la energía, desde el más básico transporte de la energía eléctrica en redes modernas, que no solo serán de distribución sino también de producción individualizada, como todo en el mundo digital de colaboración entre todos los Ciudadanos Digitales.

Las tecnologías digitales están haciendo posible el cambio en el paradigma de la movilidad, no solo dotando a los vehículos del futuro, que serán eléctricos o alguna otra energía renovable, de la conectividad que ya vamos viendo en los vehículos actuales, sino también en su capacidad de

El Antropoceno Digital es parte de una era mucho más amplia que podría denominarse Antropoceno Moderno, y que en siglos venideros llevará a la Humanidad a avances inimaginables

Enlaces de interés...

- ¿Qué es el Antropoceno?

conexión las redes eléctricas y con la llegada de los vehículos autónomos, tecnología IA, la utilización de vehículos compartidos… reduciendo el número de vehículos necesarios al hacer desaparecer el vehículo privado por su ineficacia económica, ya que solo tiene una utilización promedio durante su período de vida aproximadamente un 20%, estando el resto 80% ocupando vías urbanas y aparcamientos sin más utilidad disfrute que su belleza estética.

Qué decir de lo que están haciendo las tecnologías digitales en una de las actividades humanas más importantes, la Salud. Los sistemas sanitarios actuales en su infancia digital ya van permitiendo que se empiecen a tener datos reales de la salud de la población cubierta. Cuando los sensores, ejemplo actual y aún muy primitivo el iWatch de Apple, en el futuro suministren en tiempo real información continua de todos los individuos vivos se podrán prevenir muchas incidencias médicas antes de que ocurran con el importantísimo ahorro en vidas humanas y además de costes ya que todos sabes que es más barato prevenir que curar. Como se hará esto? Con las plataformas de redes socio sanitarias y el apoyo de la Inteligencia Artificial.

Si sigo enumerando áreas donde las tecnologías digitales cambiaran la sociedad del futuro podría no terminar nunca; tal vez me pueda dedicar el resto de mi vida solo a esto.

El Ciudadano Digital no solo es avanzado en su relación con los cambios que traen las nuevas tecnologías sino que, además, y con la misma importancia, es consciente de que estos cambios harán que volvamos a estar en armonía con nuestro planeta haciendo posible la transformación de la Humanidad para llegar una nueva era de renacimiento, paz y prosperidad planetaria.

El mercado de impresión ha experimentado una profunda transformación ayudando a las empresas en sus procesos de digitalización.

¡Descubra en nuestro

Centro de Recursos itUser

cómo está evolucionando un sector clave en la Transformación Digital!

ImpresiÓN Digital

Con la colaboración de: brother