V-Valley Cybersecurity Summit: el mayorista reúne a marcas y *partners* en Segovia

"Somos el único mayorista que estamos tratando el valor de forma diferente"

La Granja de San Ildefonso, en Segovia, fue el entorno escogido por V-Valley para celebrar su V-Valley Cybersecurity Summit y poner de manifiesto que, cinco años después, el mayorista tiene mucho más que decir y un futuro brillante. Un evento en el que reunió a *partners* y fabricantes para celebrar el éxito y prepararse para el futuro. Alberto López, director de la división de seguridad de V-Valley, fue el encargado de inaugurar el evento y recordar que el camino recorrido se ha basado en la confianza.

Rosalía Arroyo

Alberto López lleva en el mundo de la distribución desde 1996 y desde hace cinco años dirige la división de ciberseguridad de V-Valley, cinco años que no han sido un camino de rosas pero que muestran unos resultados excelentes, no sólo a nivel económico, sino en lo que respecta a la relación con los fabricantes.

Hace cinco años fueron muchos los fabricantes que se quedaron. También se fueron algunos, y también se han ido sumando otros hasta "convertirnos en un jugador importante", asegura Alberto López. Agradece el directivo los cinco años pasados al señalar que los negocios son las personas; "el valor radica en las personas. Esa ha sido la clave".

Prefiere hablar de soluciones más que de marcas y explica que se busca crear un *portfolio* equilibrado. "Es verdad que siempre hay solape, porque los fabricantes tienden a hacer muchas cosas, pero se van buscando las piezas para cubrir los huecos".

En ese equilibrio de soluciones, hay marcas más potentes y reconocidas que se venden solas. Pero a Alberto López le gusta explorar otras opciones, algunas *startups* españolas que van empezando "y que cubren algo concreto y tienen algo diferenciador" y que pone de manifiesto que se apuesta por la innovación.

Dice Alberto López que el mercado de la ciberseguridad sigue creciendo porque "las amenazas están ahí, surgen continuas formas de ataque y tienen que ir cubriendo necesidades", y que es "donde más *startups* hay". Añade que la compañía ha crecido "mucho más" que el mercado gracias a "la confianza de los fabricantes en el proyecto", para lo cual ha sido clave no sólo utilizar las capacidades financieras del grupo sino "trabajar de una manera diferente". Al respecto asegura: "Somos el único mayorista que estamos tratando el valor de forma diferente. Y ese es el éxito".

Sobre la consolidación del mercado, vivida de cerca por V-Valley, aseguraba que seguirá produciéndose. De hecho, a finales de marzo se anunciaba la compra de Lidera por un valor estimado de 5,6 millones de euros y que refuerza la posición de liderazgo de Grupo Esprinet. En su opinión esta compra demuestra la apuesta por invertir en seguridad. "No solo aporta a nivel de canal sino, sobre todo, de servicios". De cara al futuro ve un mercado que no para, en el que aparecen nuevos servicios que hay que cubrir y nuevas soluciones que dan respuesta a situaciones complejas.

Habla el mercado

Durante el encuentro se organizaron una serie de mesas redondas que dieron voz a una veintena de fabricantes y que sirvieron para tomarle el pulso al mercado. La titulada "La seguridad está en la red" planteó la evolución hacia unas redes capaces de autoconfigurarse, monitorizar, corregir, defender y analizar respondiendo a preguntas como el papel del Zero Trust en la mejora de la seguridad de la red o si las VPN siguen siendo alternativas válidas.

Apostar por una seguridad preventiva fue el foco de otra de las mesas, "Vigilar y analizar es ir un paso por delante", donde se habló de visibilidad, de *deception* o de SOC de nueva generación. La seguridad del *cloud* y, sobre todo, sus "Mitos y oportunidades" fue el título de otra de las mesas de debate en las que se planteó cómo hacer que el modelo *cloud-first* sea un modelo seguro o cómo se ha pasado de hablar de CASB a CNNAP.

La última mesa redonda se centró en "El poder de la identidad y cómo luchar contra las amenazas modernas". En ella se habló de la evolución de la seguridad en torno a la identidad digital y de plataformas capaces de dar cobertura a la seguridad de la identidad, privilegiada o no.

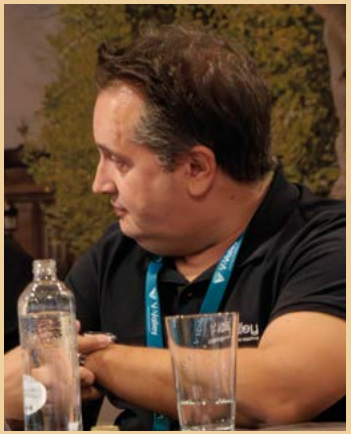
V-Valley
v-valley.es

Juan Asensio, *country manager* de Iberia de A10 Networks

En opinión de Juan Asensio, llevarse la tecnología al *cloud* y crear un mundo híbrido supone un desafío para la mayoría de las empresas. "Queremos acompañar en esa transición hacia la nube y permitir la comunicación entre la *cloud* privada y la pública", destacando la importancia de mantener los mismos criterios de seguridad en un entorno *multicloud*.

Preguntado por la evolución de los ataques de DDoS, una de las grandes amenazas de la red, explica que "hoy en día los ataques son más sutiles y van muy orientados tanto a las aplicaciones como a los elementos de red", lo que se consigue mediante ráfagas de microataques que tumban los servicios, las aplicaciones, los *firewalls*, los balanceadores, etcétera. Su propuesta es colocar un dispositivo de detección y mitigación analizando el tráfico, "dado que es ahí donde se puede identificar que se están recibiendo esas microráfagas y en microsegundos bloquear esos ataques".

> "Hoy en día los ataques son más sutiles"



David Sánchez, *technical presales consultant* de V-Valley

"Sí, todo el mundo presta la debida atención a la recuperación", asegura David Sánchez, consultor preventa de V-Valley en representación de Backbox, una compañía que se dedica a la automatización. La respuesta, añadía, era la corta, porque la respuesta larga "nos da una foto bastante distinta de cómo está funcionando el mundo del *compliance* y cómo está la infraestructura de nuestros clientes".

Recordaba que una vez que automatizas y has podido conectar todas las máquinas de una infraestructura de tus clientes, "puedes empujar cualquier tipo de *script*, cualquier tipo de automatización". Todo el mundo quiere automatizar, algo que es "fácil de decir y difícil de hacer" y que lo que vende Backbox "no es la distribución de *scripts*, sino el *knowhow*".

> "Automatizar es fácil de decir y difícil de hacer"

Juan Francisco Ruiz, *regional sales manager* de Broadcom

Preguntado por el impacto que pueden tener los niveles de seguridad en la red en la experiencia de usuario, tiene claro Francisco Ruiz que "impactar, impacta" y que "tenemos que conocer cuál es el impacto" a través de una Digital Experience Management "que mide la experiencia del usuario final después de implementar las prácticas de seguridad".

Para Ruiz el futuro de la seguridad de la red se basa en tres pilares. Teniendo en cuenta que Broadcom es también fabricante de *chips*, la seguridad de la red "ya se implementa desde la fabricación". El segundo pilar tiene como base conceptos como Zero Trust y SASE que se integran en el desarrollo de un protocolo "que permite que sólo se establezcan comunicaciones entre entidades que se conocen entre sí". El último pilar es un mensaje: "No muramos implementando políticas de seguridad si matamos el negocio".

> "Hay que conocer el impacto que la seguridad de la red tiene en la experiencia del usuario"

Eusebio Nieva, director técnico de Check Point Software

Planteado si las empresas entienden el modelo de responsabilidad compartida cuando hablamos de la seguridad del *cloud*, respondía Nieva que el problema no es que las empresas lo entiendan, que lo entienden, "sino que todos los miembros de la empresa lo entiendan, porque lo habitual es que no se piense en la seguridad cuando los servicios se publican en la nube".

Planteaba el directivo acerca de quién está implementando los entornos de nube, para responder que son los programadores, figuras que "no tienen entre sus objetivos incorporar la seguridad, sino hacer el código lo más eficiente y rápido posible para lanzar el servicio lo antes posible".

> "Las empresas sí entienden el modelo de responsabilidad compartido en la nube"

A su juicio, "la nube añade un grado superior de complejidad a lo que ya teníamos". Es complicado encontrar quién pueda dar una seguridad adecuada para una tecnología o una forma de consumir el servicio. "La solución por la que está apostando el mercado pasa por contar con una serie de herramientas que permitan realizar un control unificado de todo ello".

Paloma Cano, *head of partnerships and alliances* de Cloudflare

Apostaba Paloma Cano por el modelo Zero Trust como respuesta a la pérdida de perímetro. El modelo de confianza cero "va a permitir a las empresas verificar los accesos de los usuarios y del dispositivo, eliminar los privilegios de acceso con más control, porque sabemos que todos los días recibimos ataques". Los CISO son los primeros que están planteando migrar a la nube para tener acceso a una tecnología que les va a permitir controlar "desde dónde se está accediendo, cómo se está accediendo y cómo van a poder proteger el dato".

El modelo SASE es la base del futuro de la seguridad de la red. "Permite unificar los servicios de red y de seguridad en una arquitectura que está basada en la nube para tener el control de los usuarios, de los datos y de los dispositivos". SASE, recordaba, es un concepto, no una solución, "que va a permitir a los CISO tener una gestión mucho más agilizada y, sobre todo, más unificada". SASE no implica "una desaparición inmediata de la protección perimetral, aunque la tendencia es apostar por este modelo".

> "SASE es la base del futuro de la seguridad de la red"

Conrado Crespo, *senior sales engineer* de Countercraft

Conrado Crespo cree que hay un mayor interés por acercarse al adversario, que no siempre viene de fuera, sino que está dentro de las empresas. Aseguraba que se necesitan herramientas adicionales que permitan ser más proactivos y que hay un interés mayor en cómo articular la práctica del engaño, de la *deception*, "que requiere de un cierto cambio de mentalidad", como el uso de la inteligencia de amenazas y la capacidad de poder perfilar al adversario para saber "quién puede hacerme más daño". Explicaba que la tecnología del engaño "es una práctica que está acompañada de una serie de tecnologías, que tienen múltiples facetas y que requiere especialistas". Es una tecnología que completa "lo que se tiene, no lo reemplaza".

> "La *deception* requiere de astucia y especialistas"

Estas tecnologías de engaño suponen asumir la brecha y explicaba que no tratan de negar el acceso. "No están basadas en firmas o patrones, sino en el comportamiento esperado por parte de un adversario humano que ha conseguido hacer una brecha".

Miguel Carrero, *vice president, managed security service providers & strategic accounts at* WatchGuard Technologies

Para Miguel Carrero hay muchas cosas que han evolucionado en el mercado del SOC, pero que lo relevante es tener la concienciación de que un servicio de seguridad es la intersección de procesos, personas y tecnologías. "No todas las compañías tienen la capacidad de tener un SOC que combina estos tres vectores y que aquellas que no la tengan estarán mejor asesoradas si contratan seguridad como servicio".

> "La complejidad es el enemigo número uno de la ciberseguridad"

Asegurando que "la complejidad es el enemigo número uno de la ciberseguridad", destacaba la importancia de la simplificación del componente tecnológico, que en los últimos años se está abordando a través de plataformas "que simplifican la necesaria integración y el mantenimiento de las diferentes tecnologías". Apostaba por las plataformas unificadas de tecnologías capaces de automatizar y que liberen capacidad de las personas a hacer cosas más avanzadas, "pero siempre asumiendo que un *partner* está cercano al cliente final y es el que realmente da esa solución específica".

Rocío Martínez, responsable de Entrust Digital Identity

Cuando se habla de la seguridad de la identidad entran en juego temas como las identidades privilegiadas, la gobernanza e incluso de un *identity security posture management* (ISPM). ¿Por qué soluciones están adoptando las empresas? Para Rocío Martínez la pérdida de perímetro ha llevado a las empresas a darle más importancia "a cómo proteger las necesidades digitales y cómo asegurar que los usuarios acceden con la ley del mínimo privilegio o lo que ahora todo el mundo llama Zero Trust". Aseguraba que, a pesar de que llevamos mucho tiempo hablando de *passwordless*, "seguimos viendo mucha contraseña".

> "Seguimos viendo mucha contraseña"

La tendencia de apostar por plataformas unificadas también se ha trasladado al mundo de la gestión de identidades, que pueden ser privilegiadas o no, y donde se deben tener presentes aspectos como la gobernanza de la identidad, los certificados, etc. Trabaja Entrust en la línea de ofrecer a los clientes la capacidad de gestionar las identidades de una manera unificada.

Alfonso Ramírez, *general manager* Iberia de Kaspersky

"España es un país de pymes: más del 95 % de las empresas tienen menos de diez empleados", recordaba Alfonso Ramírez, añadiendo que estas empresas van muy por detrás y que les cuesta adquirir determinadas tecnologías. Son muchos los clientes que siguen operando una solución de seguridad *endpoint* tradicional. "Poco a poco están empezando a migrar a un EDR, con las dificultades que eso conlleva porque no sólo es incorporar la tecnología EDR, es operarla". En esa evolución, "el siguiente paso lógico es buscar profesionales que puedan gestionar ese tipo de herramientas", lo que dará paso al MDR (Managed Detection and Response).

> "Ir por delante de los cibercriminales es tremendamente difícil"

El directivo lanzaba varios mensajes: dedicar tiempo a formar y capacitar a los empleados e incorporar una solución de seguridad acorde a lo que se pueda manejar lo más avanzada posible. "Y si no lo pueden manejar, que lo deleguen". También lo importante que es tener un plan de contingencia "para que el día en el que sean atacados sepan cómo actuar".

Javier Barandiaran, ISV & *security partner manager* de Micro Focus

"En proyectos de despliegue de identidades, de control de acceso o de autenticación avanzada, no encontramos las barreras que había hace nueve o diez años", aseguraba. Añadía que no sólo se debe proteger al usuario sino tener un control respecto a los datos a los que se accede.

> "Cuando estás en *cloud* y tus aplicaciones están basadas en microservicios, la complejidad se multiplica"

Planteado el impacto que la transformación digital ha tenido en aspectos como la gestión de identidades, la seguridad de los datos o la modernización de aplicaciones recuerda que su empresa es experta en esto último, "que consiste en tomar los sistemas *legacy* y llevarlos al mundo distribuido". Cuando se está en *cloud* y las aplicaciones están basadas en microservicios, la complejidad se multiplica, igual que la superficie de ataque. "Cuando se acompaña a un cliente en esta modernización no solo se tienen en cuenta las identidades o los datos, sino que necesito tener mucha más conciencia de la seguridad de las aplicaciones y buscar las vulnerabilidades".

Sergio Martínez, Iberia *regional manager* de SonicWall

Preguntado por el mito de que los entornos *onpremise* son más seguros que la nube, respondía que no hay entornos *onpremise* o *cloud* seguros per sé, sino que depende "de las medidas que se hayan aplicado y de la estrategia de ciberseguridad que estés utilizando".

Los ciberdelincuentes "son cada vez más sutiles y sofisticados" y está habiendo un incremento exponencial del *ransomware*, de los ataques IoT y de los intentos de intrusión. En términos generales, los ataques proceden de todas partes. "Cada vez hay más vulnerabilidades, también más software y más dispositivos, lo que, a su vez, genera más fallos; y es en este entorno donde tenemos que desplegar ciberseguridad". Con la expansión de la movilidad y la conexión a los entornos híbridos, con una superficie de exposición aumentando, la estrategia pasa por "poner en marcha una defensa por capas"; añadiendo que hay que tener visibilidad y control de todo lo que se ha puesto en marcha, "así como compartimentar, detectar y responder".

> "Los ciberdelincuentes son cada vez más sutiles y sofisticados"

Patricio Jiménez, *channel manager* de Skyhigh

Recordando que el modelo Zero Trust pone foco en el control del acceso, de quién, cómo y cuándo se accede a los recursos, "las tecnologías de acceso han evolucionado" y que la capa adicional de seguridad que proporciona Skyhigh "controlando la fuga de información es una evolución lógica hacia la que se irá en los próximos años". Lo importante no sólo es "acompañar a las empresas con el control de acceso, sino con el control de navegación de los usuarios".

> "Las tecnologías de acceso han evolucionado"

Nacida en 2011 como una empresa puramente CASB (Cloud Access Security Broker), Skyhigh evolucionó hacia el SASE "y en 2022 hemos aglutinado cuatro soluciones dentro del *portfolio* SSE (Security Service Edge)", contaba. Entre las soluciones hay una parte de Proxy, otra de CASB y una de CNAPP (Cloud Native Application Protection Platform), que es la última evolución para proteger y dar visibilidad al *cloud*. "Proporciona información sobre cómo poder tener esa infraestructura correctamente protegida".

José Antonio Paramio, *major account manager* de Trellix

"La seguridad es una cadena muy amplia y se deben tener en cuenta todos los eslabones que forman parte de ella". Una cadena que tiene eslabones en la nube y en los entornos *onpremise*. "Hay que ver la seguridad desde un punto de vista holístico que tenga en cuenta no sólo la tecnología sino los procesos y procedimientos; y, sobre todo, las personas, porque son el punto más débil de toda la cadena".

Hay que buscar los datos para tener todos los modelos de incidencias. "Si se tiene una consola unificada puedes ayudar a mejorar la productividad de los usuarios". Apuntaba que no todos los clientes están preparados para gestionar un modelo de detección y respuesta avanzado; "para eso se encuentran los *partners*", que son quienes tienen los SOC y las personas. Los *partners* necesitan herramientas que sean simples, unificadas, que les permitan recoger información desde diferentes fuentes y que estén soportadas por modelos de inteligencia.

> "No todos los clientes están preparados para gestionar un modelo de detección y respuesta avanzado"

Leandro Piovi, *strategic alliances & partnerships* de Trend Micro

"Sí, las empresas avanzan en la mejora de su postura de seguridad y en tener una visibilidad clara de su superficie de ataque", aseguraba Leandro Piovi. Los fabricantes apuestan por la detección y respuesta, y por la inteligencia de amenazas, pero el cliente "sigue viendo la ciberseguridad como un coste y no como una inversión". Lo más preocupante es "el *gap* que tenemos en talentos en ciberseguridad", al tiempo que aseguraba que en Trend Micro "seguimos apostando por proteger las infraestructuras complejas de los clientes" a través de propuestas de XDR que son capaces de automatizar las respuestas.

> "La vulnerabilidad es el inicio de todo"

"La vulnerabilidad es el inicio de todo". El número de vulnerabilidades sigue creciendo. La propuesta de la compañía es el parcheado virtual, un concepto que ya está muy adoptado y que reduce la ventana de exposición de meses a días.

Néstor Serravalle, *global chief sales officer* & VP Europe de VU Security

"En este momento no hay una visibilidad clara de cómo vamos a ir resolviendo los diferentes problemas que van surgiendo en torno a la identidad digital", explica Néstor Serravalle. VU es fabricante de productos de identidad y fraude. "No hay posibilidad de defender las identidades sin tener un manejo del fraude muy adecuado". La identidad está "absolutamente fragmentada", lo que genera un gran problema de consistencia.

> "La identidad está absolutamente fragmentada"

"El primer paso para ordenar el ecosistema son las aplicaciones tipo CIAM", entendidas tanto como Customer Identity Access Management como Citizen Identity Access Management, porque "no sólo consigo un gobierno de la identidad, sino la capacidad de mantener unificada la identidad y aumentar la privacidad".

Carlos Vieira, *country manager* de Iberia de WatchGuard

Preguntado Carlos Vieira por las principales amenazas que impactan en las empresas enumera dos: *phishing* y *ransomware*, a las que se pueden sumar muchas más, como las referidas a la denegación de servicio o las persistentes avanzadas.

Interrogado por el impacto que XDR está teniendo en la seguridad de la red, explicaba que se trata de una tendencia por la que apuesta WatchGuard: "Por extender cada vez más la correlación, sincronización, descripción de políticas, etc.". Añadía que los clientes están aceptando el concepto, recordando tendencias pasadas como las apuestas por la unificación del UTM o el paso de los EPP a los EDR, y más recientemente a los XDR, que "serán un buen generador de ingresos en los próximos años".

> "El perímetro es más difuso, pero no ha desaparecido"

Félix Martos, director de desarrollo de negocio de Wizzie

Destacaba Félix Martos la capacidad de acceso a una capacidad de computación casi ilimitada como una de las grandes oportunidades de la nube. Además de tener la capacidad "de escalar horizontalmente y gestionar los datos de los clientes", estar en la nube permite "no solo soportar muchos fabricantes de infraestructura de redes, de seguridad, etcétera, sino también diferentes tipos de sistemas de los que recibimos esos datos".

> "La mayor ventaja de la nube es la facilidad de implantar"

A su juicio la mayor ventaja de la nube es la facilidad de implantar, "no tener que desplegar nada en la infraestructura local hace que los tiempos de despliegue se reduzcan". Además de la escalabilidad y de probar los servicios antes de afrontar un proyecto grande, poder transformar el capex en opex "es otra de las grandes ventajas".

Kar Buffin, vicepresidente de ventas de SEUR, CEUR y África de XM Cyber

Kar Buffin cree que existe una falsa sensación de seguridad: "No estamos viendo el problema con los ojos de un atacante, lo estamos viendo con los de un defensor". La problemática de la ciberseguridad debe afrontarse de manera amplia, "con una combinación de criterios en la misma ecuación", en la que tanto "la seguridad del directorio activo como la gestión de identidades son parte de la ecuación".

> "El atacante llega con el arsenal completo"

Planteado el impulso que Zero Trust está dando a la protección de la identidad, Buffin cree que "está impulsando la seguridad en general". Sobre el modelo opina que ni es fácil de poner en marcha ni de mantener, y que, si bien ayuda a hacer "una progresión fuerte en la gestión de la identidad", la pregunta es si te resuelve el problema. La puesta en marcha, cree, no es obvia y en ocasiones el mercado lleva a los clientes a implementar cosas que no necesita. "Lo primero es entender los problemas reales de los clientes".