V-Valley Cybersecurity Summit: cuatro años creando conexiones, conocimiento y negocio

Consolidado ya como uno de los encuentros más valiosos del canal de ciberseguridad en España, el evento anual de V-Valley, celebrado los días 3 y 4 de abril, en la localidad de La Granja, en Segovia, alcanzó su cuarta edición con la participación de más de 170 profesionales. Un evento que apuesta por un formato que combina debates, reuniones estratégicas y muchas oportunidades reales de negocio. A10 Networks, Acronis, Allied Telesis, Check Point Software, Cloudflare, CyberArk, Elastic, Entrust, Iberlayer, Kaspersky, OpenText, ReeVo, Sectigo, SonicWall, Trellix, Trend Micro, TU, WatchGuard y Zebra fueron los fabricantes presentes en el evento; junto a Lidera Cloud y Esprifinance.

Rosalía Arroyo

Alberto López, responsable del área de ciberseguridad de V-Valley para España y Portugal, fue el encargado de abrir la jornada con un mensaje de agradecimiento a *partners* y fabricantes. Recordó que este foro, más allá del *networking*, es un espacio donde surgen sinergias concretas, y celebró el crecimiento del área de ciberseguridad: "Éramos doce personas y ahora somos 77. Hemos multiplicado por 20 nuestra facturación en siete años". Su intervención dejó clara la filosofía que impregna todo el proyecto: "Sentido común, cercanía y compromiso. Eso es lo que nos define". A partir de ahí, la jornada se articuló en cinco bloques temáticos que abordaron desde la gobernanza hasta las operaciones, pasando por arquitectura, desarrollo e inteligencia de amenazas.

La conducción del encuentro corrió a cargo del periodista y presentador de televisión José Yélamo, quien actualmente dirige el programa laSexta Xplica. Su papel fue clave para dinamizar los diferentes bloques, aportar una mirada transversal y conectar los discursos técnicos con un enfoque más cercano, crítico y divulgativo.

Gobernanza y seguridad

Lo que nació como un debate sobre la creciente complejidad regulatoria en ciberseguridad —con normativas como NIS2, DORA o GDPR como puntos de partida— acabó convirtiéndose en una conversación mucho más amplia sobre el papel de la facilidad tecnológica, el valor del integrador y la necesidad de una mayor colaboración y transparencia entre fabricantes y *partners*

David Gasca, *head of marketing & operations cybersecurity* en V-Valley, fue el encargado de abrir el bloque con una reflexión sobre el momento actual: la proliferación de regulaciones de ciberseguridad y el desafío que representa para las empresas proteger la cadena de suministro desde distintos ángulos: identidad, continuidad de negocio y resiliencia.

Rocío Martínez, responsable de Entrust Digital Identity para España, recordó cómo Europa innova a través de la regulación: "NIS2 y DORA son una oportunidad. Estamos en el centro de ambas, con un enfoque de identidad digital y criptografía". Subrayó, no obstante, la ambigüedad de estas normativas y la necesidad de contar con expertos para su interpretación y cumplimiento.

Por su parte, Aitor González, *senior solutions engineer* de Acronis, puso el foco en los proveedores de servicios como pieza clave para acompañar a las empresas en este viaje regulatorio asegurando que "nuestros clientes —los *partners*— necesitan herramientas usables, pero también formación y respaldo ante la escasez de talento técnico".

Plataformas: ¿fáciles o demasiado fáciles?

Uno de los giros claves del debate llegó cuando se planteó si ofrecer plataformas "fáciles de usar" podría devaluar el papel de los integradores. La conversación se polarizó entre quienes defendían la simplicidad como vía para mejorar la eficiencia y quienes advertían del peligro de trivializar la complejidad de la ciberseguridad.

> "El IoT está llenando la red de dispositivos que acaban participando en ataques de denegación de servicio"
>
> **Juan Asensio Muñoz, *country manager* de A10 Networks**

Karina Rojas, *channel sales manager* de CyberArk, reconoció con humor la envidia que le produce la sencillez de otras plataformas,

> "La ciberseguridad no se instala y se olvida. Requiere seguimiento, servicios y acompañamiento"
>
> **Aitor Gonzalez, *senior solutions engineer* de Acronis**

mientras Alan Vázquez, *partner account manager* de ReeVo, defendió la necesidad de soluciones que permitan aglutinar tecnologías heterogéneas de forma coherente.

Por su parte, Eusebio Nieva, director técnico de Check Point Software, recordó que "todas las plataformas son fáciles... hasta que pasa algo". Para él, el verdadero valor del integrador está en ser ese "pegamento" entre soluciones heterogéneas, ofreciendo personalización y cobertura real a los clientes.

La voz del canal: una mirada desde la experiencia

Profesionales del sector destacaron durante el encuentro la necesidad de una perspectiva crítica sobre ciertos mensajes de los fabricantes. Uno de ellos señaló la falta de claridad en las referencias al cumplimiento de DORA, mencionando cómo la promesa de soluciones "con un par de clics" dificulta el trabajo de los integradores.

Otro profesional, tras una intensa prepara-

ción para obtener una certificación técnica, enfatizó la importancia de que el cliente valore esa dedicación, advirtiendo que el mensaje de plataformas "fáciles de usar" podría perjudicar a los *partners*.

Desde una perspectiva práctica, se añadió que la aparente sencillez de algunas soluciones lleva a los clientes a buscar ayuda profesional ante incidentes como el *ransomware*, subrayando que la seguridad requiere acompañamiento experto en todas las etapas del proyecto.

Más allá del producto: cultura de seguridad y eficiencia operativa

Elena García-Mascaraque, directora *worldwide partner ecosystem growth* de WatchGuard Technologies, amplió el foco recordando que la mediana empresa también necesita ciberseguridad, pero con presupuestos ajustados y pocos recursos técnicos. Por eso, las plataformas deben ser eficientes, sí, pero también adaptables a la realidad de cada cliente: "Vamos con Ferraris, repletos de prestaciones, a clientes que no saben cómo manejarlos. Necesitamos soluciones ajustadas al perfil de cada empresa".

> "Antes de hablar de seguridad, hay que entender cómo funciona una red OT"
>
> **Fernando Ruiz,**
> ***presales manager* Iberia de Allied Telesis**

Javier Barandiarán, *cybersecurity alliance and partner manager* de Opentext Cybersecurity, añadió un apunte clave sobre la cadena de suministro y el uso de librerías *open source*, especialmente en aplicaciones de IA, "como un nuevo vector de riesgo que los *partners* también deben ayudar a mitigar".

Aunque la agenda inicial ponía el foco en re-

> "El integrador es quien tiene que estar ahí cuando todo lo demás falla"
>
> **Eusebio Nieva, director técnico de Check Point Software**

gulación, identidad y gobernanza, el debate evolucionó hacia una reflexión más profunda sobre cómo fabricantes e integradores deben colaborar de forma más honesta, estratégica y realista. La tensión entre "facilidad de uso" y "valor del integrador" quedó claramente expresada, así como la necesidad de construir un discurso conjunto frente al cliente, que combine tecnología, servicios y experiencia operativa.

OT, IoT y un nuevo paradigma de protección

En el segundo bloque, el foco se desplazó hacia los entornos IT/OT y la necesidad de repensar las arquitecturas de seguridad ante la explosión del IoT y la creciente digitalización de infraestructuras críticas. La digitalización de las infraestructuras críticas, el crecimiento del IoT y la convergencia de entornos IT y OT han transformado radicalmente la superficie de exposición de las organizaciones. Esta evolución exige una revisión profunda de los modelos de protección, una mayor especialización y una colaboración constante entre fabricantes e integradores.

Fabricantes y expertos coincidieron en que la visibilidad, la segmentación, el control de identidades máquina y la aplicación del modelo Zero Trust son hoy más relevantes que nunca.

David Gasca abrió el bloque destacando la necesidad de comprender cuáles son los activos conectados, dónde están las vulnerabilidades y cómo debe evolucionar la estrategia de protección.

Andrés Peñarubia, *alliance manager* de Elastic, insistió en la importancia de la visibilidad. A través de una analogía sencilla pero eficaz, explicó que tener visores apuntando a puntos críticos no garantiza un control total si se ignora lo que ocurre entre ellos. "No hay forma de proteger lo que no se ve", concluyó.

Del *edge* al *cloud*: nuevas amenazas, nuevas responsabilidades

Juan Asensio, *country manager* de A10 Networks, centró su intervención en el papel cada vez más crítico del IoT, que se ha convertido en una puerta de entrada para ataques distribuidos: "El aumento de *bots* conectados está impulsando ataques DDoS

> "No podemos instalar agentes en los dispositivos IoT, pero sí podemos aplicar Zero Trust en el *router* que los conecta"
>
> **Juan Molina, *partner solutions engineer* de Cloudflare**

masivos". Denunció que muchas organizaciones están externalizando responsabilidades al migrar a la nube, lo que transforma también el rol del integrador, y aseguró que "del destornillador a la consola en la nube, el integrador también se reinventa".

José Miguel Domínguez, director de la unidad de negocio de Auto-ID de V-Valley, en representación de Zebra, puso el foco en el hardware como eslabón crítico de la cadena de seguridad, asegurando que "hay una oportunidad de negocio inmensa en entornos como almacenes, mataderos u hospitales, donde abunda el IoT basado en Android", insistiendo en la importancia de contar con dispositivos que cumplan normativas y sean interoperables con las plataformas del *partner*.

Redes OT: reducto olvidado que pide integración

Fernando Ruiz, *presales manager* para Iberia de Allied Telesis, propuso una mirada histórica sobre la evolución de las redes, del aislamiento al multiservicio, y advirtió que las redes OT siguen siendo un "reducto" difícil de integrar. Afirmando que los responsables OT viven de espaldas a IT por miedo a los riesgos, "y con razón", propuso tender puentes, pero desde el respeto a los protocolos y particularidades de cada entorno. "Antes de hablar de seguridad, hay que entender cómo funciona una red OT".

> "Por cada identidad humana hay 45 no humanas"
>
> **Karina Rojas,**
> ***channel sales manager* de CyberArk**

Asegurando que "el 5G abre un espectro nuevo de amenazas" y que tenemos que anticiparnos con herramientas que permitan evaluaciones constantes, Jorge Villaescusa, *sales engineer* de Trend Micro, abordó el impacto del 5G privado y la necesidad de

mantener visibilidad continua ante una diversidad creciente de dispositivos conectados.

Identidades máquina: una amenaza subestimada

Karina Rojas, responsable de canal de CyberArk, aportó una estadística reveladora: "Por cada identidad humana hay 45 no humanas", lo que implica que, más allá de los usuarios, existen infinidad de dispositivos y sensores con credenciales que deben ser protegidas. "Muchos clientes no saben ni cuántas identidades de máquina tienen. Ahí es donde el *partner* tiene que liderar".

> "No podemos estigmatizar el *open source*. Todo funciona sobre Linux, incluso los sistemas críticos"
>
> **Andrés Peñarubia, *alliance manager* de Elastic**

Pedro David Marco, fundador y CEO de Iberlayer, ejemplificó el problema con un caso real: un casino estadounidense fue *hackeado* a través del termómetro *wifi* de un acuario. Preguntando si realmente era necesario que ese termómetro tuviera *wifi*, planteó que, a veces, "el problema no es lo que no se protege, sino lo que nunca debió estar conectado".

Juan Molina, *partner solutions engineer* de Cloudflare, ahondó en las posibilidades de aplicar Zero Trust incluso en entornos sin agentes al tiempo que alertaba sobre el auge de ataques impulsados por IA: "Ya no hace falta una red zombi de millones de dispositivos. Con pocos servidores inteligentes se puede hacer mucho daño".

El cliente: informado, pero no preparado

Defendiendo la especialización como vía para acceder a un mercado que sigue siendo reacio, José Antonio Morcillo, director de canal de Kaspersky en España y Portugal, aportó una visión desde el canal: "Los clientes saben

> "Vamos a tener cientos de agentes que contarán como empleados. ¿Cómo protegemos una empresa con 400.000 agentes virtuales?"
>
> **Rocío Martínez, responsable de Entrust Digital Identity para España**

que necesitan seguridad OT, pero no están viendo integradores especializados", lo que, aseguraba, "genera desconfianza".

Fernando Ruiz volvió a intervenir para diferenciar entre OT e IoT, recordando que muchas veces se tratan como sinónimos. "Son mundos distintos, con riesgos distintos. En IoT el problema es que casi nada está diseñado con la seguridad en mente". Puso como ejemplo el riesgo en universidades donde miles de estudiantes conectan sus dispositivos a la red institucional: "¿Quién protege eso?".

> "En ocasiones, el problema no es lo que no se protege, sino lo que nunca debió estar conectado"
>
> **Pedro David Marco, fundador y CEO de Iberlayer**

En su intervención de cierre, David Gasca reivindicó la necesidad de repensar las arquitecturas desde la base, considerando todos los vectores de ataque, desde el *cloud* hasta el dispositivo más inesperado. Juan Asensio y Juan Molina coincidieron en la importancia de actuar cerca del origen del problema, controlando el tráfico y aplicando políticas de Zero Trust.

El mensaje final fue claro: la seguridad no puede seguir siendo una reacción. Debe ser una estrategia compartida entre fabricantes, integradores y clientes. Y eso exige tecnología, visión y mucha más colaboración.

Aplicaciones, desarrollo y seguridad en la era del *multicloud*

El tercer bloque abordó uno de los puntos más críticos y menos visibles de la ciberseguridad moderna: el desarrollo seguro del software. Con una creciente dependencia de entornos *multicloud*, una explosión de API, una adopción masiva de librerías *open source* y un número creciente de desarrolladores con acceso a entornos híbridos, la conversación abordó los riesgos estructurales del ecosistema digital moderno. Desde la gestión del código hasta la protección de identidades privilegiadas, pasando por la trazabilidad del software y el impacto de la inteligencia artificial, el debate dejó claro que el software —más que nunca— es la primera línea de defensa (y de exposición).

Cloud y *multicloud*: más flexibilidad, más complejidad

David Gasca abrió el bloque con una reflexión que sintetiza el desafío: "Las empresas se están exponiendo más. Nos protegemos, sí, pero luego trabajamos en entornos híbridos, *multicloud*, con coordenadas de seguridad norte-sur, este-oeste, y eso cambia las reglas del juego".

Eusebio Nieva fue claro en su diagnóstico: "No se puede proteger la nube como se protege un entorno *on-premise*. Hay que cambiar el paradigma". Apostó por tecnologías de seguridad comunes que permitan simplificar la protección en distintos entornos, evitando soluciones fragmentadas. Al ser preguntado por la diferencia entre empresas nativas *cloud* y tradicionales, fue rotundo:

> "El cliente sabe que necesita seguridad OT, pero no ve expertos preparados para ayudarle"
>
> **José Antonio Morcillo, director de canal de Kaspersky en España y Portugal**

> "El 48 % de las empresas está usando IA con datos públicos o preentrenados"
>
> **Javier Barandiarán, *cybersecurity alliance and partner manager* de Opentext Cybersecurity**

"Los nativos *cloud* suelen equivocarse menos. Tienen mejor interiorizado el modelo y son más conscientes de los riesgos". Aun así, recordó que en todos los casos el éxito depende de tres pilares: "Tecnología, procesos y personas".

Durante su intervención Javier Barandiarán puso sobre la mesa datos concretos: "El 80 % de las brechas de seguridad tienen origen en el software de aplicación". Explicó cómo su compañía ha apostado por crear alianzas tecnológicas para cubrir todas las etapas del desarrollo seguro: desde el análisis estático y dinámico, hasta la detección de vulnerabilidades en librerías *open source* (como con Sonatype) o el entrenamiento de desarrolladores mediante gamificación (Secure CodeWarrior). "Muchos clientes nos piden cubrir más. Y eso requiere plataformas que integren todo. No pueden seguir gastando el 4 % del presupuesto de ciberseguridad solo en integrar herramientas dispares".

Open source: ni ángel ni demonio

Andrés Peñarubia defendió el valor del software libre asegurando que no se le puede estigmatizar al tiempo que recordaba que hoy "todo está montado en Linux, incluidos los sistemas críticos. No lo habrán hecho tan mal". Insistió en que el problema no es la tecnología en sí, sino cómo se integra, cómo se gestiona y si se mantiene la trazabilidad en toda la cadena. Su defensa del enfoque DevSecOps apuntó a la necesidad de continuidad entre desarrollo, operaciones y seguridad porque "no pueden ser mundos separados".

> "Acabaremos tratando a la IA como a un empleado más: con permisos, privilegios y controles"
>
> **Alan Vázquez,**
> ***partner account manager* de ReeVo**

Barandiarán matizó que el riesgo no está sólo en la seguridad; también en la sostenibilidad de las librerías utilizadas: "El 80 % de las librerías *open source* están mantenidas por una o dos personas. Eso es un riesgo empresarial enorme".

API, JavaScript y Zero Trust: proteger lo invisible

Juan Molina abordó el problema desde la capa de aplicación explicando que muchas brechas se producen por falta de control sobre las API y componentes de terceros como el JavaScript: "Necesitas saber si un JS *open source* ha cambiado sin tu permiso" porque si algo falla, "el responsable eres tú". Reivindicó herramientas *cloud* que permitan monitorizar y gestionar todos estos elementos al tiempo que defendía el uso de plataformas de Zero Trust con capacidades CASB para integrar entornos multinube bajo políticas comunes.

Identidades y privilegios: un punto ciego común

Karina Rojas aprovechó la coincidencia con el Día Mundial de la Protección en Cloud para resaltar el problema de los accesos privilegiados en entornos de desarrollo recordando que hay muchos desarrolladores con muchos accesos a muchas nubes. "El cliente no sabe cuántos ni qué privilegios tienen". Subrayó la oportunidad de negocio que representa esta problemática poniendo como ejemplo que en CyberArk hay más de 1.000 desarrolladores que "no son administradores, pero tienen privilegios críticos. Ahí hay negocio para los *partners*". También alertó sobre la necesidad de no incomodar al desarrollador, porque "si le complicas un paso, buscará cómo saltárselo".

El bloque dejó claro que la seguridad del desarrollo no puede seguir tratándose como una capa adicional. Debe estar integrada desde el inicio, con herramientas unificadas, políticas coherentes y especialización. En un entorno donde el software se compone de miles de piezas conectadas, con múltiples orígenes y responsables, la visibilidad y la colaboración son fundamentales. Un entorno en el que el papel del *partner* vuelve a ser esencial: como asesor, como integrador y como catalizador de una cultura de desarrollo seguro.

> "No basta con orquestar, hay que tener capacidad de ejecutar con inteligencia detrás"
>
> **Javier Fernández,**
> ***enterprise regional sales manager* de Sectigo**

Threat Intelligence: entre la anticipación y la IA ofensiva

El cuarto bloque del encuentro se adentró en un terreno donde la tecnología y el análisis se cruzan con la estrategia y la intuición: el universo de la Threat Intelligence. Dámaso Ramos, responsable de servicios en V-Valley, abrió la conversación con una pregunta provocadora: "¿Queremos ser inteligentes o simplemente listos?". Una reflexión que sirvió para enmarcar el debate: anticiparse es tan importante como saber reaccionar y, para ello, tanto la inteligencia humana como la artificial tienen un papel esencial.

Alan Vázquez explicó cómo el SOC de ReeVo utiliza inteligencia, tanto preventiva como reactiva, integrando datos de múltiples fuentes para protegerse de amenazas de día cero. Destacó el uso de SOAR y SIEM para bloquear IP maliciosas detectadas en la *deep* y *dark* web explicando que son capaces de "ver IP atacando vulnerabilidades conocidas y las cortamos antes de que lleguen. Eso no lo pueden hacer ni medio millón de humanos".

> "El cibercrimen tiene todo el tiempo del mundo. Y ahora, también, todas las herramientas"
>
> **Sergio Martínez,**
> **director general de Sonicwall en Iberia**

Por su parte, José Antonio Morcillo recalcó la importancia de estar presentes en los foros donde realmente se gesta el cibercrimen. "El 85 % de las amenazas proviene de zonas como Rusia, China o Corea. Si no estás allí, no sabes lo que viene", al tiempo que subrayaba que la verdadera Threat Intelligence requiere "infiltración, experiencia y capacidad de anticipación".

> "La IA no puede reemplazar el juicio humano, pero sí ayudarnos a digerir la telemetría imposible"
>
> **David Baldomero,**
> ***senior systems engineer* de Trellix**

IA: aliada, amenaza y reto filosófico

La conversación pronto derivó hacia el uso de la inteligencia artificial. David Baldomero, *senior systems engineer* de Trellix, destacó su valor en tareas de detección, investigación en lenguaje natural y reducción del ruido: "Tener una IA como copiloto nos permite centrar el esfuerzo donde realmente hay un problema", comentaba, al tiempo que planteaba la cuestión emergente de la IA contra IA, anticipando un nuevo tipo de enfrentamiento técnico.

Jorge Villaescusa apeló a la necesidad de una inteligencia proactiva, capaz de identificar patrones antes de que se materialicen en un ataque: "Parece ciencia ficción, pero es real: podemos actuar antes de que el ataque ocurra". Sergio Martínez, director general de SonicWall, alertó de que los atacantes también están aprovechando la IA para detectar vulnerabilidades con mayor precisión, encadenar ataques de manera más eficiente y ofuscar y borrar rastros. "El cibercrimen tiene todo el tiempo del mundo. Y ahora, también, todas las herramientas".

IA generativa: empleados virtuales y nuevos vectores

Rocío Martínez abrió un nuevo frente: la IA generativa como fuerza laboral. "Vamos a tener cientos de agentes que contarán como empleados. ¿Cómo protegemos una empresa con 400.000 agentes virtuales?". Propuso adoptar una mentalidad de brecha asumida (*assume breach*) y repensar los métodos de defensa.

"Usamos IA para ayudar a los administradores a ser más ágiles y seguros", decía Karina Rojas, al tiempo que recordaba que la IA también puede facilitar la configuración de productos complejos como los sistemas de gestión de privilegios.

Asegurando que la IA no existe, sino que lo que hay son sistemas de aprendizaje sin supervisión, Pedro David Marco recordó que pueden ser envenenados "para que acepten como legítimo lo que debería ser bloqueado". Subrayando el papel de los integradores para acompañar a los clientes en una adopción segura, Javier Barandiarán alertó sobre la inseguridad inherente a los modelos generativos: "El 48 % de las empresas está usando IA con datos públicos o preentrenados. Sólo el 20 % entrena con datos propios".

> "Parece ciencia ficción, pero es real: podemos actuar antes de que el ataque ocurra"
>
> **Jorge Villaescusa,**
> ***sales engineer* de Trend Micro**

Volver a la esencia: conocer al enemigo

David Gasca insistió en centrar la atención en la inteligencia de amenazas como servicio estructurado, con fuentes fiables, experiencia y enfoque colectivo.

Morcillo volvió a intervenir para recordar que, sin visibilidad global, no hay defensa efectiva: "Si los ataques son globales y tú solo ves lo que pasa en España, vas con los ojos vendados". También señaló que el verdadero valor del MDR reside en la inteligencia, más que en la tecnología de detección.

Elena García-Mascaraque apostaba por combinar inteligencia colectiva, automatización sensata y experiencia: "Primero hay que entender los procesos, luego automatizar y, sobre todo, aplicar experiencia. Ser listos también es parte de la inteligencia".

El bloque concluyó con una sensación de ambivalencia. La IA ofrece herramientas sin precedentes, pero también plantea riesgos y retos éticos. La Threat Intelligence requiere acceso, experiencia y contexto, pero también un ecosistema de colaboración. Como apuntó Juan Molina, la combinación de Zero Trust con MFA sigue siendo un escudo robusto, incluso ante amenazas simuladas por IA. Cerró Alan Vázquez: "Acabaremos tratando a la IA como a un empleado más: con permisos, privilegios y controles. Solo así evitaremos que se convierta en el eslabón más débil".

Seguridad de las operaciones: automatización, talento y nuevos modelos SOC

En el último bloque del encuentro, la conversación se centró en la seguridad de las operaciones. Lejos de tratarse de una discusión puramente técnica, el debate giró en torno a modelos de SOC, gestión del talento, automatización y los desafíos operativos que enfrentan hoy los equipos de ciberseguridad. Dámaso Ramos, responsable de servicios de V-Valley, abrió el bloque apuntando directamente a tres ejes claves: la compartición de inteligencia, la automatización que algunos

> "Primero hay que entender los procesos, luego automatizar y, sobre todo, aplicar experiencia"
>
> **Elena García-Mascaraque, directora *worldwide partner ecosystem growth* de WatchGuard Technologies**

empiezan a cuestionar y la dificultad para retener profesionales cualificados.

Javier Fernández, *enterprise regional sales manager* de Sectigo, reflexionó sobre el valor de la inteligencia compartida entre entidades públicas y privadas, y el papel que puede desempeñar una red nacional de SOC. "Lo importante es tener una entidad que permita colaborar entre todos para estar preparados ante cualquier ataque, venga de donde venga", aseguró, añadiendo un matiz interesante sobre el SOAR: "No basta con orquestar, hay que tener capacidad de ejecutar con inteligencia detrás".

Reafirmó que la seguridad 100 % no existe, porque el eslabón más débil sigue siendo el humano. Por ello, aunque la inteligencia artificial puede filtrar grandes volúmenes de eventos, "siempre tiene que haber un humano que diga: hasta aquí ejecutamos", explicó Fernández.

David Baldomero reforzó esa idea asegurando que la IA "no puede reemplazar el juicio humano, pero sí ayudarnos a digerir la telemetría imposible y señalar dónde actuar".

El reto del talento: retención, fatiga y motivación

Uno de los temas recurrentes fue la fuga de talento. Elena García-Mascaraque reivindicó la experiencia como factor diferencial y propuso una redefinición del modelo SOC: "Cada vez vemos modelos más híbridos, distribuidos geográficamente, incluso con colaboración entre MSP y fabricante". Apuntó que uno de los principales factores de fuga es la repetitividad del trabajo del analista, lo que se traduce en fatiga profesional. "Cuanto más tedioso es el trabajo, más probable es que se vayan". Su solución: herramientas diseñadas para liberar al

analista de tareas repetitivas y aumentar el valor de su trabajo.

Javier Barandiarán compartió una experiencia similar: "Los SOC pierden talento porque les damos tareas que antes hacía una máquina. Hay que invertir en automatización para evitar quemar a los analistas". Explicó cómo tecnologías de auto-triaje permiten reducir la carga operativa, especialmente en la gestión de vulnerabilidades de aplicaciones.

Replantear el modelo: menos gente, mejor pagada y más motivada

David Gasca cerró el bloque con una propuesta tan sencilla como potente: "Si eliminamos las tareas repetitivas con herramientas, necesitaremos menos personas. Y a esos pocos, podremos pagarles más y ofrecerles un trabajo más estimulante".

Una conclusión pragmática que pone el foco en la necesidad de rediseñar los equipos SOC no solo desde la tecnología, sino desde la gestión del talento y el bienestar profesional.

Este último bloque consolidó una idea presente en todo el encuentro: la tecnología es necesaria, pero insuficiente. Automatizar, compartir información, usar inteligencia artificial... todo suma. Pero si no se cuida al profesional que está al otro lado de la consola, cualquier arquitectura de seguridad será siempre vulnerable por su eslabón más humano. La seguridad de las operaciones, en definitiva, es un equilibrio entre herramientas, procesos y personas.

Más allá de la tecnología, un reto de colaboración y propósito

A lo largo de los cinco bloques, quedó patente que la ciberseguridad ya no es sólo una cuestión técnica. Es un desafío de gestión, de estrategia y de confianza. Las plataformas pueden ser más fáciles de usar, pero el papel del integrador sigue siendo imprescindible. La inteligencia artificial ofrece herramientas sin precedentes, pero también plantea nuevos riesgos. El talento técnico

> "Allí donde veáis un almacén, un matadero o un hospital, hay una oportunidad de negocio en OT"
>
> **José Miguel Domínguez, director de la unidad de negocio de Auto-ID de V-Valley, en representación de Zebra**

es escaso y valioso, pero también difícil de retener si no se crea un entorno profesional más atractivo.

Desde el *compliance* hasta las operaciones, pasando por el desarrollo seguro o el Threat Intelligence, los temas tratados evidencian una necesidad común: cooperar más, compartir más, escuchar más. Fabricantes, distribuidores y *partners* tienen en sus manos la posibilidad de crear un ecosistema más eficiente, más transparente y más humano. Como quedó claro en La Granja, la ciberseguridad no se vende: se construye. Y para eso, nada mejor que sentarse a hablar. Juntos.