DEBATES ciberseguridad TIC

Validar para resistir

Cefiros

IR A PÁGINA SIGUIENTE

Seguridad en la Nube. ¿Estás preparado para los desafíos del mañana?

La validación continua se consolida como el nuevo eje de la ciberseguridad moderna, desplazando el enfoque puramente preventivo hacia modelos de comprobación constante, automatización y respuesta. Ciberseguridad TIC, en colaboración con Cefiros, reunió a varios fabricantes especializados para analizar cómo probar, medir y reforzar las defensas en tiempo real.

Rosalía Arroyo

Durante años, las estrategias de ciberseguridad se centraron en prevenir. Pero el aumento de la complejidad tecnológica y la velocidad de los ataques han demostrado que ya no basta con proteger: hoy es imprescindible validar de forma continua si las defensas funcionan realmente. Con esa idea, Ciberseguridad TIC y Cefiros reunoines a un grupo de fabricantes especializados que representan ángulos muy distintos, pero complementarios para hacer frente a esta nueva aproximacion: desde la gestión de vulnerabilidades y protección IT (WithSecure), hasta el pentesting automatizado y la simulación realista de ataques (Horizon3, Keysight), pasando por la seguridad en entornos industriales (Radiflow) o la integración de seguridad en el ciclo de vida del software (Aikido, Plexicus).

El encuentro, moderado por Ciberseguridad TIC, sirvió para explorar una tendencia común a todos los ámbitos tecnológicos —IT, OT y DevSecOps—: pasar de las auditorías estáticas a una verificación dinámica y continua. Una evo-

lución impulsada por la necesidad de medir, probar y mejorar en tiempo real, y por la aparición de soluciones que integran análisis de vulnerabilidades, ciber range, automatización y entornos de desarrollo seguros.

Como mayorista especializado en ciberseguridad, Cefiros actúa como nexo entre fabricantes, integradores y clientes, ofreciendo soporte técnico, formación y servicios de consultoría que ayudan a trasladar esta visión de validación continua al terreno operativo.

"Las auditorías anuales dan una foto fija, pero los atacantes se mueven cada día"

Francisco Macías,
Senior Sales Engineer, **WithSecure**

De la prevención a la validación continua

Francisco Macías, senior sales engineer de WithSecure, abrió el debate recordando que buena parte de los presupuestos de ciberseguridad "sigue destinándose a la prevención, cuando lo esencial es mejorar la postura de seguridad de forma continua".

Según explicó, muchas empresas aún dependen de auditorías anuales que proporcionan "una foto fija" de su estado de seguridad; "los atacantes tardan unos quince días en explotar una vulnerabilidad. Si sólo auditamos una vez al año, dejamos una ventana enorme de oportunidad", advirtió.

La clave está en herramientas que permitan analizar vulnerabilidades en tiempo real, con visibilidad sobre todos los activos —nube, endpoints, móviles, identidades— y sin depender de revisiones puntuales. "No necesitamos una fotografía anual, sino una radiografía dinámica del riesgo", resumió.

"Medir tecnología, procesos y personas a la vez es la única forma de estar preparados"

Blas Simarro,
Enterprise Sales Manager España y Portugal, **KeySight**

Simular para aprender: el valor del ciber range

La validación también pasa por la simulación. Así lo destacó Blas Simarro, Enterprise sales manager para España y Portugal de Keysight, quien defendió el papel de los ciber range como entornos seguros para medir la eficacia de la seguridad en tres dimensiones: tecnología, procesos y personas.

“Un ciber range nos permite reproducir una infraestructura real sin poner en riesgo la producción. En él podemos comprobar si nuestros equipos saben responder, si los procedimientos son eficaces o si las herramientas hacen lo que esperamos”, explicó.

Estos entornos, añadió, son especialmente útiles en sectores industriales, donde cada cambio debe probarse antes de aplicarse. “El ciber range libera la carga de gestión del cambio en OT. Lo que validamos ahí, sabemos cómo se comportará después en producción”, explicó durante la mesa redonda.

OT e IT: dos mundos que deben converger

Para Pablo Carrasco, sales manager director para Iberia & LatAm de Radiflow, uno de los mayores desafíos sigue siendo la brecha entre los entornos IT y OT.

Apuntó el directivo que, en IT “lo más importante es la confidencialidad”, mientras que en OT es la disponibilidad. “Si una línea de producción se detiene, el impacto económico es inmediato”, apuntó.

Carrasco recordó que las redes industriales son “más heterogéneas, con muchos equipos obsoletos, IoT sin control y escasa segmentación”. En su experiencia, “el 80 % de los incidentes en OT se originan desde IT”, lo que hace esencial definir estrategias conjuntas que combinen automatización, priorización y cumplimiento normativo.

> “En IT preocupa la confidencialidad; en OT, la disponibilidad. Ambos mundos deben converger”
>
> **Pablo Carrasco,**
> Sales Manager Director para Iberia & LatAm, **Radiflow**

“Normativas como NIS2 o DORA afectan ya a ambos mundos. La convergencia no es opcional, es el camino para garantizar la continuidad operativa”, concluyó.

DevSecOps: integrar seguridad sin frenar el desarrollo

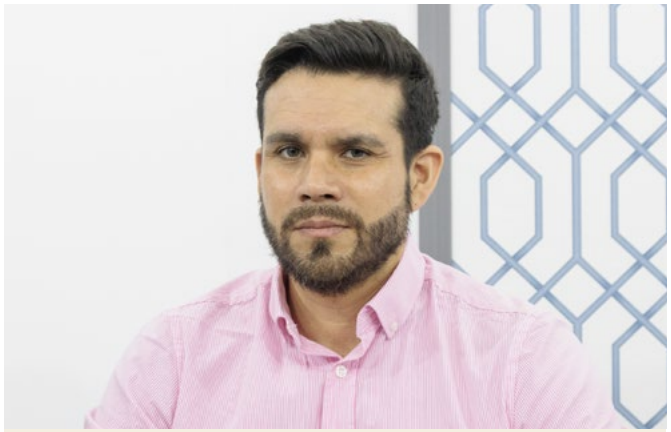
El paso de DevOps a DevSecOps fue analizado por José Ramón Palanco, CEO y Cofundador de Plexicus, quien reconoció que el reto “no es sólo técnico, sino cultural”.

“Si las herramientas no se integran bien en los pipelines o generan ruido y falsos positivos, el proceso se bloquea. Para que la seguridad forme parte del ciclo de desarrollo, hay que automatizar y reducir la fricción”, afirmó.

Joost de Jong, RVP Iberia + LatAm de Aikido, coincidió: “Si introduces la seguridad al final del ciclo, ya llegas tarde. Hay que integrarla desde el inicio, como parte natural del desarrollo”.

Defendió que el objetivo es facilitar la vida al desarrollador mediante inteligencia artificial y herramientas que prioricen los riesgos sin ralentizar la publicación del código.

“El desarrollador no tiene que ser experto en seguridad; su trabajo es producir código rápido y de calidad. Nuestra labor es ofrecerle solucio-



> “Las herramientas tradicionales generan ruido; si no reducimos falsos positivos, no hay DevSecOps posible”
>
> **José Ramón Palanco,**
> CEO y Cofundador, **Plexicus**

nes que le acompañen y automaticen la protección”, subrayó.

Pentesting automatizado: de la foto a la película

La conclusión más visual del debate la aportó Víctor Arroyo, CTO y Sales Specialist de Horizon3 para Iberia y LatAM de Cefiros, al afirmar: “No quiero una foto de mi seguridad, quiero una película”.

Explicó el directivo que el pentesting automatizado y continuo permite pasar de auditorías aisladas a un seguimiento evolutivo, donde los resultados cambian con cada modificación de la infraestructura.

“La seguridad no puede basarse en la confianza, sino en la comprobación. Solo así sabremos si nuestras defensas realmente funcionan”, afirmó Víctor Arroyo, añadiendo que, además de aportar visibilidad y precisión, este enfoque reduce costes frente a los análisis tradicionales y ofrece a los CISOs “un mapa de exposición que permite priorizar acciones y medir el progreso real”.

Validar para resistir: una visión de conjunto

La conversación dejó un mensaje unánime: prevenir ya no basta.

Cada uno de los expertos coincidió en que el futuro de la ciberseguridad pasa por medir, probar y aprender de manera continua, cada uno desde su ámbito de especialidad.

Para Francisco Macías, de WithSecure, la prioridad es detectar y corregir vulnerabilidades con rapidez, porque “solo una visión continua evita dejar puertas abiertas”.

Blas Simarro, responsable de Keysight en España, subrayó que la simulación es el mejor entre-

> “El desarrollador no tiene que ser experto en ciberseguridad, sino contar con herramientas que le acompañen”
>
> **Joost de Jong,**
> RVP Iberia + LatAm, **Aikido**

namiento: “Las organizaciones que practican sus respuestas en entornos controlados son las que luego reaccionan con eficacia ante una crisis real”.

Desde el ámbito industrial, Pablo Carrasco, de Radiflow, insistió en la necesidad de alinear IT y OT bajo una estrategia común, donde “la automatización y la segmentación sean el punto de partida para reducir riesgos”.

José Ramón Palanco, fundado de Plexicus, recalcó que el gran desafío es cambiar la cultura del desarrollo, integrando la seguridad desde el diseño y “evitando que el ruido o los falsos positivos frenen la innovación”.

Joost de Jong, portavoz de Aikido, defendió el papel de la inteligencia artificial como aliado para simplificar y acelerar la detección de vulnerabilidades “sin frenar a los equipos de desarrollo”.

Y Víctor Arroyo (Horizon3 / Cefiros) cerró recordando que la validación continua es el camino hacia la confianza real: “La seguridad no puede basarse en suposiciones, sino en evidencias medibles”.

La era de la validación continua

La ciberseguridad ya no puede limitarse a levantar muros: debe aprender a mirarse a sí misma, medirse y mejorar cada día. Ese es, en el fondo, el mensaje que deja este debate: la necesidad de pasar de un modelo reactivo a una cultura de comprobación continua, donde las defensas no se dan por válidas, sino que se prueban y ajustan constantemente.

> “La seguridad no puede basarse en la confianza, sino en la comprobación constante”

Víctor Arroyo, CTO y Sales Specialist de Horizon3 para Iberia y LatAm, **Cefiros**

La validación se convierte así en el nuevo lenguaje común entre IT, OT y desarrollo. Permite a las organizaciones entender cómo se comportan sus sistemas frente a un ataque real, descubrir debilidades antes de que lo haga un adversario y convertir cada simulación en conocimiento práctico. En ese proceso, la tecnología aporta automatización, pero el verdadero cambio llega cuando las empresas asumen que la seguridad no es un estado, sino un proceso.

El encuentro impulsado por Cefiros puso de relieve que esa evolución ya está en marcha. Los fabricantes apuestan por modelos más medibles y dinámicos; los integradores buscan trasladarlos al día a día de las empresas; y los responsables de seguridad empiezan a ver el valor de comprobar antes de confiar.

La conclusión es clara: validar para resistir no es una tendencia, sino una forma distinta de pensar la seguridad. Una que une prevención, simulación y aprendizaje continuo para construir organizaciones más conscientes y preparadas frente a lo imprevisto. CST

Validar para confiar

Con el fin de facilitarle el acceso a los diferentes puntos del debate, lo hemos desglosado en varios apartados con el fin de que elija el que más le interese, haciendo click para dirigirle al contenido relacionado.
También es posible ver el vídeo completo e ir avanzando o retrocediendo gracias a la barra de tiempo situada en la parte inferior.

02.47 WithSecure. ¿Cómo ayudáis a las empresas a priorizar qué vulnerabilidades son críticas y a resolverlas de manera rápida?

05.10 Keysight. ¿Qué valor real aportan a los equipos de seguridad cuando se enfrentan a amenazas cada vez más sofisticadas?

08.50 Radiflow. ¿Cuáles diríais que son las diferencias más claras entre proteger un entorno OT y un entorno IT tradicional?

11.02 Plexicus. Desde vuestra experiencia, ¿qué obstáculos son los más difíciles de superar para que la seguridad forme parte del proceso desde el inicio?

13.02 Aikido. ¿Cómo se puede integrar la seguridad en ese flujo ágil de desarrollo sin frenar a los equipos?

18.10 Horizon3. ¿En qué se diferencia de una auditoría de seguridad tradicional que se hace de vez en cuando?

23.08 WithSecure. ¿Qué problemas concretos os encontráis en este terreno y cómo se pueden abordar?

25.41 Keysight. ¿Cómo contribuye el testing preventivo a evitar fallos en servicios esenciales?

29.38 Radiflow. En vuestros análisis de riesgos en entornos industriales, ¿qué vulnerabilidades críticas son las que aparecen con mayor frecuencia?

32.33 Plexicus. ¿Qué resistencias culturales o de procesos os encontráis más a menudo en las organizaciones?

35.54 Aikido. Hoy en día dependemos mucho de librerías externas y dependencias de terceros. ¿Qué riesgos estáis viendo aquí y qué buenas prácticas recomendáis para gestionarlos?

41.03 Horizon3. Cuando simuláis ataques, lo interesante es que sean lo más realistas posibles. ¿Cómo os aseguráis de que las simulaciones reflejan lo que haría un atacante real, incluso usando IA?

45.00 Todos. ¿Creéis que la validación continua —ya sea en IT, OT o DevOps— se convertirá en un estándar obligatorio en cualquier estrategia de ciberresiliencia?

“La seguridad y la calidad de código son dos caras de la misma moneda”

“La seguridad no puede llegar al final del desarrollo: debe estar integrada desde la primera línea de código”, afirma Joost de Jong, Regional Vice President para Iberia y Latinoamérica de Aikido.

La compañía propone una plataforma ASPM (Application Security Posture Management) que unifica análisis de código, dependencias open source, contenedores, APIs y nube en un único flujo automatizado. “La seguridad y la calidad de código son dos caras de la misma moneda”, explica. Su objetivo: reducir fricciones entre desarrollo y seguridad, alineando ambos equipos en torno a los mismos datos y prioridades.

A través de IA y autofix, Aikido permite detectar, corregir y validar vulnerabilidades en tiempo real, impulsando una seguridad integrada y continua que acompaña todo el ciclo de vida del software.

Joost de Jong, RVP Iberia + LatAm, **Aikido**

aikido

“Democratizar el pentesting es hacer la seguridad accesible para todos”

“No quiero una foto, quiero una película de mi seguridad”, afirma en el vídeo Víctor Arroyo, CTO y Sales Specialist de Horizon3 para Iberia y Latinoamérica en Cefiros. Horizon3 impulsa un modelo de pentesting continuo y automatizado que permite validar las defensas en tiempo real y medir la evolución del riesgo. “La seguridad no puede basarse en la confianza, sino en la comprobación constante”, señala el directivo.

Frente a las auditorías puntuales y costosas, Horizon3 apuesta por democratizar la validación, ofreciendo una solución accesible que reproduce ataques reales sin comprometer los sistemas. Gracias a la inteligencia artificial, las organizaciones pueden priorizar vulnerabilidades, anticipar fallos y justificar inversiones con datos objetivos. En un entorno en cambio permanente, comprobar deja de ser opcional: es la única forma de saber si realmente estamos protegidos.

Víctor Arroyo, CTO y Sales Specialist de **Horizon3** para Iberia y LatAm, **Cefiros**

HORIZON3.ai
TRUST BUT VERIFY

“El testing es la única forma de saber si una defensa funciona”

Javier Armesto apuesta por una estrategia de seguridad cloud centrada en el dato como eje fundamental. Recuerda que la nube no es un entorno uniforme, sino una combinación de arquitecturas híbridas, usuarios descentralizados y múltiples formas de acceso a la información. “La mejor estrategia para securizar la nube es una estrategia que esté centrada en el dato”, afirma. Esa protección debe seguir al dato en todo su recorrido, desde dispositivos gestionados o no, aplicaciones cloud, correo electrónico o entornos shadow IT.

Ante esta complejidad, defiende la necesidad de un conjunto integrado de tecnologías como DLP, proxies cloud, control de accesos y protección de endpoint. “Necesitamos una solución que sea capaz de securizar todos esos movimientos, independientemente del dispositivo, el tipo de usuario o la infraestructura en la que esté el dato”.

Blas Simarro, Enterprise Sales Manager España y Portugal, **KeySight**

KEYSIGHT TECHNOLOGIES

“La inteligencia artificial debe ayudar al desarrollador, no sustituirlo”

Asegura José Ramón Palanco, CEO y Cofundador de Plexicus, que la IA la IA “debe integrarse en el ciclo DevSecOps como un compañero de trabajo”. La compañía aplica IA generativa para automatizar la corrección de vulnerabilidades y reducir los falsos positivos sin frenar los ciclos de desarrollo. “Nuestra IA actúa como un desarrollador experto: analiza, propone y valida cambios seguros”, explica.

Su enfoque se extiende más allá del código, abarcando contenedores, dependencias y entornos cloud para garantizar una protección integral. Palanco defiende que la clave está en integrar la seguridad en la cultura DevSecOps, haciendo que forme parte natural del proceso creativo. “Si la seguridad se convierte en un obstáculo, los equipos la esquivan; si la integramos con inteligencia, la adoptan.”

José Ramón Palanco, CEO y Cofundador, **Plexicus**

PLEXICUS

“La validación continua permite medir la resiliencia industrial en tiempo real”

En opinión de Pablo Carrasco, Sales Manager Director para Iberia & LatAm de Radiflow, “la automatización y la inteligencia de amenazas son claves para reducir el riesgo en entornos OT”. Explica en el vídeo que la compañía, especializada en ciberseguridad industrial, ayuda a las organizaciones a visualizar y priorizar sus riesgos mediante plataformas que detectan y evalúan de forma continua todos los activos de red. “No todas las amenazas son igual de relevantes; lo importante es saber cuáles te afectan realmente”, señala.

Radiflow impulsa la convergencia entre IT y OT con un enfoque que combina automatización, interoperabilidad y validación constante. En sectores críticos como energía o transporte, su objetivo es claro: garantizar la continuidad operativa reduciendo el riesgo de forma inteligente y medible.

Pablo Carrasco, Sales Manager Director para Iberia & LatAm, **Radiflow**

Radiflow

“La seguridad no se demuestra una vez al año, se valida todos los días”

Francisco Macías, Senior Sales Engineer de WithSecure, defiende en el vídeo que la ciberseguridad debe medirse cada día, no una vez al año. La compañía finlandesa, pionera en detección avanzada y gestión de la exposición, impulsa un modelo de validación continua que permite comprobar en tiempo real la eficacia de las defensas y anticipar riesgos antes de que se materialicen.

“Las auditorías anuales ofrecen una foto fija, pero los atacantes se mueven a diario”, recuerda Macías, añadiendo que desde su posición en Europa, WithSecure combina tecnología, inteligencia y servicios para fortalecer la resiliencia digital de las empresas. “Validar no es desconfiar —añade—, es la única forma de saber que todo sigue funcionando como debería”.

Francisco Macías, Senior Sales Engineer, **WithSecure**