“Fortinet Security Fabric permite al CIO tener un papel mucho más amplio e interesante”

El fabricante de soluciones de ciberseguridad Fortinet sigue creciendo. Los resultados del primer trimestre de 2024 indican que los ingresos totales de la compañía se incrementaron un 7,2% con respecto al mismo periodo del anterior, en un momento en el que ha lanzado una nueva versión de su sistema operativo FortiOS y apuesta, más que nunca por la IA en sus soluciones.
En esta entrevista Alain Sánchez, CISO de Fortinet EMEA, pone en valor el papel de Fortinet a la hora de ayudar al CIO a proteger a las empresas, al tiempo que pone en valor la relación entre CIO y CISO en las organizaciones.

Inma Elizalde

Alain Sánchez, CISO de Fortinet EMEA

Alain Sánchez destaca la evolución de la ciberdelincuencia en el mundo empresarial como una serie de sofisticaciones que han pasado del ataque de unos estudiantes, a quienes les gustaba entrar en los sistemas informáticos para ser famosos, a un negocio con grandes beneficios en el que, incluso, se ataca a los estados con el fin de destruir sus infraestructuras críticas. "Una forma de guerra digital", tal y como lo define, "en un mundo en el que la evolución del CISO ha sido más que notable ya que, si en los años 90 del siglo pasado el CISO era un poco *geek* y nunca hablaba en público, bastándole con tener un profundo conocimiento sobre seguridad y redes, en el siglo XXI entran en juego nuevas disciplinas como el ámbito legal, al tener que proteger en mayor medida al mundo digital", reflexiona. Ahora, además considera que el CISO se ha convertido en un líder de opinión. "Hablamos con los jefes de Estado, con líderes industriales…", reconoce. "El CISO del mañana será primero un especialista en sanidad cuando hablemos de hospitales o de un banco si hablamos del sector bancario, antes de ser un especialista en tecnología porque la manera de manejar la curva de riesgo depende de la cultura de la empresa, no de la tecnología", señala.

"La tendencia de hace tan sólo tres años pasaba por, en caso de tener un problema con el OT, por poner un ejemplo, reclutar a especialistas en esta materia, pero la cultura de la persona no encaja en la cultura de la empresa y más del 70 % de las transformaciones de ciberseguridad fallan por la cultura de los especialistas de tecnología y la manera de trabajar de las compañías. Por esta razón hemos creado la oficina del CISO en Fortinet", prosigue, "porque lo importante en el éxito de la transformación digital

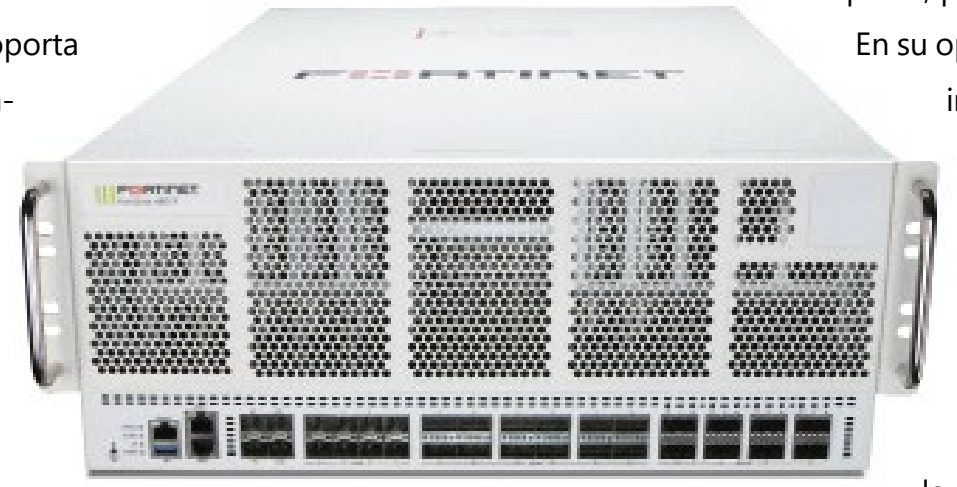
es la relación entre los imperativos estratégicos de la organización y las tecnologías. Nunca el *roadmap* de un vendedor debe influir en la manera de hacer el negocio", apunta.

En su opinión ser ejecutivo de una empresa significa tomar decisiones en varios escenarios de riesgo. "Tenemos que reclutar dentro del ámbito de la cultura de la compañía ingenieros más que especialistas de una tecnología, porque las tecnologías cambian pero lo que las soporta son las ciencias y la ciberseguridad es matemática, una combinación de álgebra, geometría... Aunque las tecnologías cambien, el soporte científico queda por lo que ese reclutamiento tendría que pasar por personas que sean capaces de entender las ciencias. Este sería mi consejo para reclutar con éxito", explica.

Evolución del CIO

En cuanto a la evolución del CIO, sobre todo en empresas en las que no hay CISO, señala que es importante contar con una figura que sea un reporte directo al comité ejecutivo, que tenga el papel de la seguridad de los sistemas. Al tiempo que avanza que en este momento se está dando la figura del CIO *on-demand*, el CIO *as a service*. "Es muy importante ir más allá de la eficiencia de los sistemas. Tener una dimensión legal de recursos humanos y de comunicación, independientemente del tamaño de la empresa porque a pequeña organización, grandes riesgos", recuerda. "Un *phishing* te puede matar, terminar con la compañía, por lo que es importante esa función".

"CIO y CISO tienen que tener una relación en la que entiendan el papel de cada uno"



En su opinión el rol del CIO pasa por acelerar la innovación digital, explicar qué ha sucedido y lo que está en juego. Y pasar de se un centro de costes a un centro de aportación de valor.

Binomio CIO-CISO

En cuanto a la complicada relación a la que siempre se alude entre CIO y CISO Alain Sánchez señala que "hubo un tiempo en el que el CISO era como un mal necesario para las organizaciones con una guerra abierta con otros miembros de la junta directiva, con

una doble incomprensión: antes del ataque porque al resto de la compañía no le gustaba las restricciones impuestas para evitar un ataque y en caso de producirse el mismo por no haber podido evitarlo. "El CISO pone en perspectiva lo que ocurre. CIO y CISO tienen que tener una relación en la que entiendan el papel de cada uno", apunta, al tiempo que revela que en este momento se encuentran en una nueva fase en la que no sólo se toleran, también entienden la importancia del otro porque los papeles se revelan a lo largo de los ataques, incidentes, *deepfakes*...

Y en un momento en el que los ciberdelincuentes ponen en evidencia la vulnerabilidad de las organizaciones ante los ataques, Alain Sánchez extrae una lección positiva: a medida que estos se suceden, mayor capacidad para aprender y estar más preparados, reflexiona. "Sin los ciberdelincuentes la ciberseguridad no hubiera avanzado tanto. Los fabricantes de seguridad aprendemos cada segundo de los ataques. Y, aunque para las empresas que han sido víctimas es una tragedia, una visión holística es la clave, aunque no existe la panacea como remedio universal", explica. "Es un progreso continuo y con la inteligencia artificial la velocidad de progreso aumenta cada segundo".

"FortiAI, el asistente GenAI de Fortinet, apoya y guía a los equipos de operaciones de seguridad (SecOps) y operaciones de red (NetOps)"

IA

En un entorno, el tecnológico, en el que se habla de cada tecnología en función del instante, Sánchez considera que, aunque este es el momento de la IA esta no va a desaparecer si deja de ser tendencia "porque lo que dependa de la IA toca a la manera de concebir el valor añadido de una empresa y nos fuerza a tener mayor calidad. Va a ser integrada. Una integración que cada vez será más rápida", avanza.

En su opinión esta es la segunda vez que nuestro país va a saltar a una revolución industrial. La primera fue el paso de los *mainframes* a los microcomputadores. "Fue un gran paso la capacidad de desarrollar sistemas de información avanzados". Y lo van a hacer también con la IA, dice.

Fortinet mantiene su compromiso de estar a la vanguardia de la innovación en IA. Mediante la expansión de FortiAI, su asistente GenAI contextual, continúa empoderando a los equipos de operaciones con nuevas capacidades avanzadas de procesamiento de lenguaje natural. Las últimas actualizaciones de FortiAI ofrecen nuevas e innovadoras formas de interactuar con los productos de Fortinet utilizando más de 30 lenguajes comunes para reducir la com-

plejidad y aumentar la eficiencia operativa.

El sector de la ciberseguridad se enfrenta a un importante déficit de profesionales, con cerca de cuatro millones. La GenAI aborda este reto aumentando la necesidad de competencias técnicas. FortiAI, el asistente GenAI de Fortinet, apoya y guía a los equipos de operaciones de seguridad (SecOps) y operaciones de red (NetOps) para que puedan configurar y gestionar los cambios en su red e investigar y resolver las amenazas más rápido que nunca. Su interfaz intuitiva permite a las personas, independientemente de su experiencia, interactuar utilizando el lenguaje natural, lo que reduce significativamente la escasez de personal cualificado en el sector.

Universal SASE

En cuanto a SASE recuerda que en lugar de conectar sólo la conectividad pura, se añaden servicios de seguridad dentro de esa conexión. Y, aunque reconoce que ha evolucionado el concepto, afirma que queda la idea. "Es decir, comprar un ordenador es menos im- portante que ver cuál es el servicio de conectividad, de seguridad y de distribución del software", manifiesta. Además, afirma que la arquitectura, la tipología de los sistemas de información en nuestro país está muy distribuida por lo que España está muy bien posicionada para coger el tren del SASE.

"Fortinet dispone de una plataforma holística en la que se tiene en cuenta el cloud, el edge, el centro de datos, el OT y el IT"

Su propuesta de valor en torno a SASE, Universal SASE, funciona como Fortinet Security Fabric, señala, con una sola tecnología y con un alto nivel de seguridad. "Ese es el progreso más importante de Universal SASE, no tener un conjunto de tecnologías", admite.

El papel del *firewall*

En cuanto al papel que está jugando y va a jugar el *firewall* en el mundo de la ciberseguridad considera que es el supercentro neurálgico de las decisiones de ciberseguridad pero debe ser integrado en el resto. "Es decir, es todavía un papel central porque prohibir o autorizar una trama de información es vital en una

empresa pero se van a añadir un mayor número de funcionalidades", explica. "Cuando las empresas compran un FortiGate el SD-WAN que va dentro es gratuito. Esto prueba que la red y la seguridad están en modo de convergencia, algo que existe en FortiGate hace mucho tiempo pero se añaden otras dimensiones como el OT o la IA, ya integrada en el proceso central que maneja el FortiOS", finaliza.

A tener en cuenta

- **"Fortinet dispone de una plataforma holística en la que se tienen en cuenta el cloud, el edge, el centro de datos, el OT y el IT. "Hay que proteger todo este ecosistema, correlacionar todo lo que ocurre entre todos ellos para detectar las amenazas y ver las diferencias entre un falso positivo y un ataque real", recuerda Alain Sánchez. "De esta frontera depende la eficiencia de la empresa, su seguridad y competitividad. Tenemos que manejar esa fina línea entre el riesgo y la seguridad".**
- **¿Cómo ayuda Fortinet a un CIO con Fortinet Security Fabric? En primer lugar podemos tener un enfoque holístico de componentes que nunca se habían integrado entre ellos, señala Sánchez. "Podemos ser un superintegrador de todos los elementos fundamentales de un sistema de información incluyendo el inalámbrico, el 5G, el 6G y el centro de datos. Cuando tenemos esa visión podemos proteger lo que vemos y hacer que las correlaciones entre estos eventos se conviertan en leyes de autenticación, detección, análisis y respuesta porque nuestro papel no sólo incluye el análisis y la identificación, también la respuesta. Fabric permite actuar en equipamientos de Fortinet o de otras marcas. Por otro lado aliviamos las tareas repetitivas a las personas que trabajan en los SOC. En tercer lugar integramos el conjunto de nuevas tecnologías que se encuentran al servicio de la estrategia de la empresa. En definitiva, Fortinet Security Fabric permite al CIO tener un papel mucho más amplio e interesante, también al resto de ejecutivos porque todos están involucrados en la estrategia. A todos les afecta la seguridad", enfatiza.**
- **Fortinet acaba de lanzar FortiOS 7.6, la última versión de su sistema operativo FortiOS con la que sus clientes pueden mitigar mejor los riesgos, reducir la complejidad y obtener una experiencia de usuario superior en toda su red.**