DOCUMENTOS SiC
Nº 40
SEPTIEMBRE 2023

elastic

La analítica de datos, en el corazón de la ciberseguridad

- Capacidades XDR a través del SIEM, protegiendo endpoints y nube
- Ciberprotección avanzada con un ADN innovador en IA
- Velocidad, escalabilidad y flexibilidad

María Campos
Regional VP South EMEA de Elastic

Más de 20.000 organizaciones usan su tecnología en todo el mundo

Elastic: ciberseguridad centrada en la analítica del dato con un ADN innovador en IA

Desde su fundación en el año 2012, Elastic se ha convertido en uno de los referentes mundiales en ciberseguridad con un enfoque diferenciador en la protección del dato y una propuesta transversal a través de su tecnología de búsquedas, observabilidad y la aplicación intensiva de la inteligencia artificial y el *machine learning* al SIEM, protección del punto final y la red, con orquestación y capacidades anticipativas.

Vivimos en un mundo impulsado por los datos. Ya lo decía el escritor Arthur Conan Doyle, 'padre' de Sherlock Holmes, cuando destacaba que sin datos no hay nada: es como intentar "hacer ladrillos sin arcilla". Y pocas multinacionales representan tan bien el valor de los datos en ciberseguridad como la estadounidense Elastic, uno de los grandes referentes mundiales en tecnología de búsquedas -para "que todos encuentren las respuestas que importan"-, observabilidad y, también, protección cibernética de última generación.

Su historia comenzó en 2004, en un apartamento de Londres, cuando su fundador y CEO, **Shay Banon** desarrolló un innovador motor de búsqueda para facilitarle el trabajo a su mujer, que necesitaba encontrar recetas de cocina en Internet para sus clases en la prestigiosa escuela de cocina Le Cordon Bleu. Una idea que pronto se convirtió en el corazón de una empresa, fundada en 2012, cuya tecnología permite "encontrar instantáneamente información relevante y procesable", a través de la búsqueda, la observabilidad y la seguridad en el ámbito corporativo. En definitiva, un éxito que la compañía ejemplifica con una frase que resume su objetivo y buen hacer: "Buscar. Observar. Proteger".

Reinventando la ciberseguridad

Y las cifras de negocio lo avalan. Con más de 20.000 clientes en todo el mundo y cotizando en la Bolsa de Nueva York desde 2018, Elastic superará los 80.000 millones de euros de facturación en 2023 –casi el doble que hace cinco años–, de los cuales, 23.000 millones provendrán de su negocio de ciberseguridad. Un éxito que, en el mercado de ciberprotección, se basa en una propuesta completa orientada a los requisitos de las actividades y negocios, que permite analizar grandes cantidades de datos logrando resultados relevantes, en tiempo real, para contar con capacidades proactivas de ciberprotección. Para ello, la compañía ofrece a través de su plataforma una solución escalable, en tiempo real, en una única pila de tecnología abierta que se puede implementar en cualquier lugar. "Miles de organizaciones en todo el mundo ya la usan para encontrar instantáneamente información procesable de cualquier tipo de datos y potenciar sistemas de misión crítica", recuerdan desde la organización. Este enfoque le ha permitido ganar en pocos años destacados clientes como Auchan, Booking y Airbus, en el área de búsquedas, Telefónica y Zurich en observabilidad, y Personal Capital, Proficio, Entel, el Mando de Combate Aéreo de EE.UU., NetApp y la Universidad de Oxford, entre otras, en ciberprotección. Gracias, entre otros aspectos, a lo que conlleva en eficiencia de inversión, reducción de costes y, también, velocidad a la hora de integrar soluciones

Con su plataforma unificada de búsqueda, observabilidad y ciberseguridad, Elastic brinda la posibilidad de despliegue en modo SaaS (Azure, Google, AWS...), facilitando los entornos de colaboración DevSecOps.

para unificar y optimizar los flujos de trabajo para poder bloquear ataques complejos en el menor tiempo posible.
Elastic, además, está comprometida con la transparencia y la apertura con la comunidad de ciberseguridad, "y este es el principal motivo por el que creamos y mantenemos nuestra lógica de detección de forma pública junto con todos los que estén interesados", resaltan desde la organización.

Tecnología para todo tipo de entornos

A través de una plataforma unificada de búsqueda, observabilidad y seguridad, la empresa brinda la posibilidad de despliegue en modo SaaS, en cualquier nube pública (desde Azure hasta Google y AWS) facilitando la integración, en este ámbito, de los equipos de desarrollo, operaciones y seguridad. Entre las razones de su crecimiento

La multinacional aplica la IA, de forma intensiva, a la gestión de amenazas, la capacidad de contar con alertas automatizadas y de disponer de *chatbots* de ciberprotección.

está que permite contar con altas capacidades de detección y respuesta extendidas (XDR), basándose en el SIEM, la seguridad del *endpoint* y la nube. Todo bajo una premisa: que la ciberseguridad es un problema de datos. Buena prueba de ello es que, en una de las más recientes actualizaciones de Elastic Security, se han incluido más de 1.100 reglas prediseñadas para que sus usuarios configuren y pongan en marcha sus detecciones y monitorización de protección lo antes posible. Todo ello con una apuesta decidida por la innovación y tecnologías como su Elasticsearch Relevance Engine (ESRE), su motor para la "democratización de la IA". Y es que la multinacional aplica la IA, de forma intensiva, a todas sus soluciones y, en el caso de ciberseguridad, a la gestión de amenazas, la capacidad de contar con alertas automatizadas y en disponer de *chatbots* de ciberprotección.

Reconocida por los analistas

Todo ello ha permitido que, en muy poco tiempo, su negocio de ciberseguridad experimente un crecimiento exponencial, siendo reconocida por analistas como Gartner, situándola como líder en el 'cuadrante mágico' de Insight Engines; Forrester, que la nombró líder en The Forrester Wave: Security Analytics Platforms, Q4 2022; así como IDC, que la situó como actor principal en su IDC MarketScape: Worldwide SIEM 2022 Vendor Assessment.

Elastic Security Labs: lucha contra el cibercrimen compartiendo inteligencia

Disponer de capacidades anticipativas es clave para alcanzar una ciberseguridad madura. Por ello, la compañía cuenta con una unidad especializada en ciberinteligencia denominada 'Elastic Security Labs'. Se trata de un equipo de más de 40 ingenieros de ciberprotección, profesionales e investigadores "que comen y respiran seguridad". "Es nuestra pasión", destacan desde la organización, a la vez que recuerdan que investigan temas de seguridad, *malware*, *ransomware*, tácticas, grupos de actividad, adversarios y todo lo relacionado con la seguridad cibernética. Un trabajo que plasman en informes publicados de forma habitual sobre grupos adversarios, amenazas emergentes o nuevos patrones de ataque, así como las últimas vulnerabilidades descubiertas. "Los recursos de inteligencia ante amenazas, como el 'Reporte global de amenazas de Elastic 2022', son fundamentales para que los equipos corporativos puedan evaluar sus capacidades y experiencia en la identificación y la prevención de amenazas", destacan sus integrantes de esta unidad.

Una propuesta para calcular con precisión el valor de la ciberseguridad

Elastic quiere hacer la ciberseguridad simple. Entre sus últimas iniciativas para conseguirlo destaca su 'Calculadora de valor' aplicada a la ciberprotección. Se trata de una "herramienta interactiva con la que se puede cuantificar rápido las eficiencias financieras", que la compañía ofrece a cada empresa a través de cómo mejorar "los KPI en torno al riesgo, los costes y la productividad. Los números cuentan la historia: lograr una visibilidad holística reduce el riesgo, mejora la productividad e impulsa el ahorro de costes y la recuperación de ingresos", destacan desde la organización. En definitiva, se trata de mostrar cómo desde la compañía se "ayuda a cualquier organización a descubrir algunas de esas incógnitas desconocidas con datos", explica la CISO de la empresa, **Mandy Andress**. "En Elastic, observamos el gran valor que nuestros clientes han logrado al usar nuestra tecnología. Al proporcionar esta herramienta de cuantificación, esperamos ayudarles a lograr una comprensión de cuánto valor podrían generar ellos también", recuerdan desde la multinacional que ofrece esta herramienta a través de su web.

María Campos,
Regional VP South EMEA de Elastic

Con más de dos décadas dedicadas a ciberseguridad, situándose en primera línea de grandes multinacionales, María Campos desembarcó hace un año y medio en Elastic para responsabilizarse del Sur de Europa. Un reto para el que sus habilidades de liderazgo, ventas y comprensión técnica, le están permitiendo trasladar con éxito al mercado la estrategia de una compañía que apuesta por un enfoque donde prima la protección del dato a través de una plataforma que combina la búsqueda y la observabilidad, capacidades muy demandadas especialmente en entornos de nube.

"Elastic permite encontrar entre todos los datos los que de verdad interesan y lo hace en tiempo real y a escala, sin importar su formato o ubicación"

– Cuenta con más de 20 años en ciberprotección. ¿Qué es lo que más ha cambiado y cuál será el enfoque que permitirá proteger el mundo hiperconectado y complejo al que nos aventuran la IA, el 5G, *blockchain*…?

– La ciberseguridad ha ido siempre de cómo proteger los datos, las aplicaciones, los sistemas y cómo asegurar la resiliencia del negocio. Lo que ocurre es que el contexto ha cambiado mucho: los datos, las aplicaciones, los sistemas ya no están solamente dentro de los límites de nuestras organizaciones. Vivimos en un mundo hiperconectado, que además es híbrido y multi-*cloud*. Si echamos un vistazo a todo lo que está por venir en el campo de IA, la situación se complica aún más con los llamados *adversarial attacks,* que pueden aprovecharse de engañar al comportamiento humano y hacer mejor ingeniería social. El número de dispositivos conectados sigue incrementándose exponencialmente, así como los datos generados y las propias aplicaciones. La democratización de las nuevas herramientas y su disponibilidad de acceso para todos, buenos y malos, hace que el *gap* en protección siga creciendo. Como consecuencia la ciberresiliencia debe ser foco continuo y prioritario. Y para ello la visibilidad es clave. Si puedo monitorizar y entender lo que pasa en mi entorno, puedo actuar. Necesitamos trabajar para ser más ciberresilientes.

– Elastic es un referente en analítica de datos y motores de búsquedas. ¿Cuál es su valor diferencial respecto a su competencia?

– Nuestro motor de analítica de datos destaca por varios motivos: por cómo ha sido creado (solución *on-prem* y solución multi-*cloud*); por su código abierto con todo el poder de la Comunidad; por su concepto de plataforma (que evita la duplicidad de datos al integrar multitud de herramientas disponibles bajo un mismo paraguas); por su capacidad de ingesta de datos de cualquier formato; por su forma de licenciamiento (que permite afrontar el crecimiento sin disparar los costes); y, entre otros, por su arquitectura de datos (que permite ir enfriando el dato desde capas *hot* a *frozen* con tiempos de respuesta muy bajos y períodos de retención de años). Es una de las plataformas más abiertas y potentes que existen en el mundo del *data lake*.

– ¿Cuándo decidieron aplicar estas capacidades a la ciberseguridad y con qué enfoque?

No es algo nuevo. Elastic, como empresa que viene del mundo Open Source, ha contado con la ventaja de que millones de usuarios han construido casos de uso para múltiples disciplinas y una de ellas ha sido ciberseguridad. Muchos usuarios empezaron a utilizar Elastic

como *data lake* de seguridad hace años y comenzamos a ver el valor de integrar distintas capacidades sobre la plataforma: reglas, gestión de casos, *workflows* especializados, *dashboards*, etc. Creemos que hay que aproximarse a la ciberseguridad como un problema de datos: es necesario entender quién está haciendo qué en mi red, qué ocurre en mis aplicaciones y que todo esto pase en tiempo real. Si correlacionamos todos los datos de seguridad y los alimentamos con *feeds* de inteligencia, podremos entender posibles anomalías.

– Elastic apuesta por una ciberprotección abierta, colaborando con comunidades de desarrollo y operaciones, ya que considera que "ser abiertos es la esencia de todo lo que hacemos". ¿Cómo lo ponen en práctica?

– Podemos integrarnos con todas las plataformas y contribuir con estándares abiertos (por ejemplo, OpenTelemetry). Esto conlleva abrir nuestro código fuente y ser más eficientes ante posibles ataques derivados, por ejemplo, de la manipulación de dicho código. También, que la comunidad contribuya a mejorar la plataforma y que abordemos el *gap* de talento en ciberseguridad con plataformas abiertas, democratizando el acceso al conocimiento.

– En su propuesta también destaca el uso de la Inteligencia Artificial. ¿Qué características específicas presentan sus algoritmos en este ámbito?

– En IA uno de los retos es entrenar los modelos y mantener la privacidad de los datos. La aplicación de la IA a través de modelos preconfigurados que identifican problemas de seguridad sin tener que preocuparse por cómo entrenar el modelo o disponer de equipos de ciencia de datos, permite automatizar la detección de anomalías y el análisis de causa raíz, lo que reduce el MTTR. Gracias a la integración con ChatGPT, se desarrollan casos de uso para automatizar la identificación y respuesta a incidentes de seguridad y facilitar el trabajo de los CSIRT. Pero esto sólo es el principio, porque Elastic acaba de lanzar un motor para potenciar la IA en aplicaciones de búsqueda.

– ¿Con qué fortalezas cuenta la compañía para reclamar su hueco en el mercado de ciberseguridad?

– La propuesta de ciberseguridad de Elastic se apoya en tres pilares: SIEM, EDR (Endpoint Detection and Response) y protección *cloud*, aglutinadas en una aproximación XDR (Extended Detection and Response), concebida como una solución de SecOps moderna y más ágil para el analista.

Elastic se diferencia por su versatilidad en entornos híbridos y multi-*cloud.* El SIEM puede 'ingestar' datos de cualquier entorno, proporcionar visibilidad unificada y actuar sobre los datos allá donde estén. Resuelve con ello la problemática de *performance* frente al coste.

"La propuesta de ciberseguridad de Elastic se apoya en tres pilares: SIEM, EDR y protección *cloud*, aglutinadas en una aproximación XDR, concebida como una solución de SecOps moderna y más ágil para el analista"

– ¿Cuántas personas dirige usted en España y en qué principales áreas está focalizada Elastic en nuestro mercado?

– Elastic es una empresa muy distribuida con equipos basados en prácticamente todos los países. En España cuenta con más de 100 personas; además del equipo comercial, canal, preventa, *customer success*, servicios, desarrollo de negocio, disponemos de un equipo de ingeniería, *product management* y soporte. Es una fortaleza poco habitual tener equipos técnicos tan amplios hablando español y en nuestra zona horaria.

– ¿Cómo pueden acceder las compañías a sus soluciones y en qué modalidad?

– Somos una empresa de canal (con una red de *partners* globales y locales) con un foco importante en el movimiento hacia la nube. También, comercializamos nuestra plataforma a través de los *marketplace* de los tres hiperescalares (Azure, Amazon Web Services y Google Cloud Platform). Como creemos que el mundo no es ni puramente *on-prem* ni 100% *cloud*, sino híbrido, ofrecemos soluciones en local y en la nube, tanto en IaaS como SaaS, en nuestra Elastic Cloud.

– ¿Qué objetivos se ha marcado a corto y medio plazo, y qué sectores y tipos de empresa son más susceptibles de adquirir sus soluciones?

– Queremos potenciar la divulgación de nuestra propuesta de ciberseguridad y llegar a ser tan reconocidos en este ámbito como en el mundo de la observabilidad y de la búsqueda. Distintas consultoras ya nos sitúan entre los tres líderes en analítica de seguridad.

Nos proponemos seguir creciendo a ratios del +40% en Elastic Cloud. La flexibilidad de nuestra plataforma permite construir todo tipo de casos de uso. Cualquier organización *data-driven* que requiera extraer más valor de sus datos es susceptible de ser cliente de Elastic. Y si su filosofía es híbrida y/o multi-*cloud*, somos sin duda una de las mejores opciones.

"Cualquier organización *data-driven* que requiera extraer más valor de sus datos es susceptible de ser cliente de Elastic. Y si su filosofía es híbrida y/o multi-*cloud*, somos sin duda una de las mejores opciones"

– ¿Con que frase resumiría el valor del I+D+i en su compañía?

– Elastic sigue avanzando para encontrar entre todos los datos (seguridad, negocio, observabilidad) los que de verdad importan y lo hace en tiempo real (milisegundos) y a escala (multi peta-byte), sin importar el formato o la ubicación. ●

Visión holística, escalabilidad e integración de soluciones orientadas al SOC

Elastic Security aúna altas capacidades XDR, a través de SIEM, seguridad de *endpoints* y protección de la nube en una plataforma unificada, abierta e integrada

Con un enfoque de ciberseguridad centrado en el dato, aplicando potentes capacidades de protección, procesamiento y visualización, Elastic Security permite contar con el contexto necesario y poder extraer información valiosa de seguridad. Para ello, su propuesta pasa por ofrecer capacidades tanto listas para usar como definidas por el usuario, escalables, en tiempo real, y aunadas en una única plataforma que se puede implementar según las necesidades de cada cliente.

Más del 90% de los datos que existen en el mundo han sido creados en los últimos dos años. Y su incremento es imparable: se calcula que, para 2025, se generarán más de 175 zettabytes, lo que supone diez veces más de los registrados hace una década, según IDC. Por ello, el dato se ha convertido en uno de los activos más críticos y valiosos para las organizaciones. También en ciberseguridad donde las diversas fuentes de datos permiten contar con el contexto crítico necesario en detecciones, búsquedas, investigaciones y respuesta a incidentes. Y pocas compañías entienden mejor este enfoque que Elastic, cuya propuesta se basa en considerar "la ciberprotección como un desafío de datos". Por ello, su oferta, bajo el paraguas de Elastic Security, pasa por ofrecer altas capacidades de detección y respuesta extendidas (XDR), abarcando soluciones SIEM, seguridad de punto final y protección en la nube, en una plataforma unificada, abierta e integrada.

En ella, la compañía aplica todo el potencial de sus reconocidas capacidades de búsqueda, análisis y observabilidad de grandes volúmenes de datos para proporcionar protección, detección y respuesta de amenazas complejas en cualquier entorno, aplicando el uso del *machine learning* (ML) e IA de forma transversal.

Búsqueda avanzada para reducir el riesgo

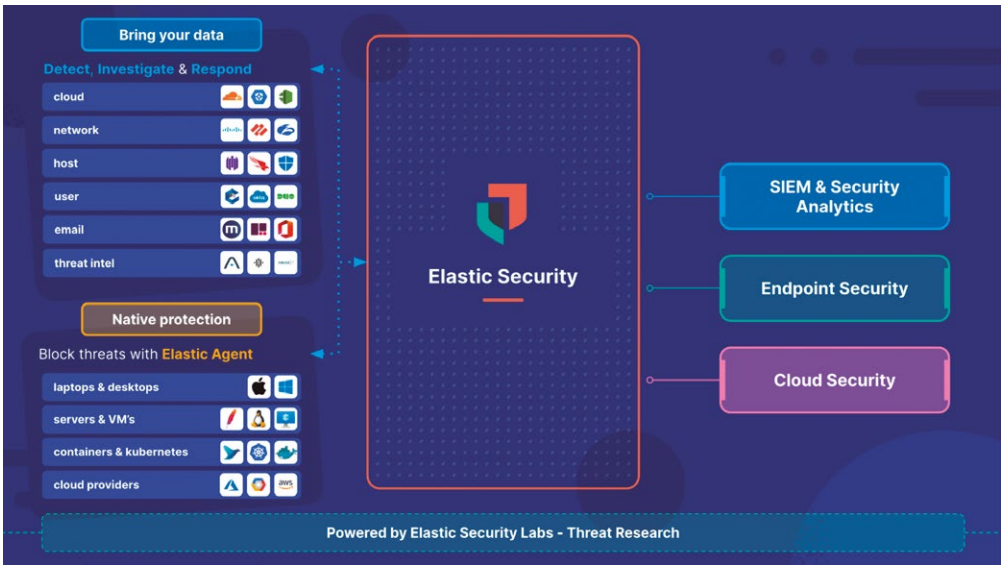
Elastic Security se basa así en Elastic Stack, un conjunto de herramientas de código abierto que proporciona grandes capacidades de búsqueda, análisis y visualización, que desde hace muchos años es utilizado por los equipos de seguridad como su base de datos para extraer información valiosa, y en cuyo núcleo se encuentra la tecnología de Elasticsearch. Para la compañía, una tecnología de búsqueda veloz, precisa y eficaz es clave para brindar una visibilidad holística, reduciendo el riesgo.

"Los datos pueden ayudar a identificar si un activo tiene una vulnerabilidad conocida e identificar dispositivos potencialmente vulnerables en una red", explican. Además, la búsqueda permite acelerar y refinar la detección de amenazas y limitar el daño de los ataques de *malware*, entre otros aspectos.

Por ello este tipo de plataformas se están convirtiendo en una herramienta imprescindible para los CISO.

Casos de uso

Todo ello permite disponer, con un único *data lake*, de potentes capacidades de protección, procesamiento y visualización de datos, y del contexto necesario para extraer información de seguridad valiosa. Los SOC pueden beneficiarse de casos de uso como la **monitorización continua** de la infraestructura local y basada en la *cloud*, la **búsqueda de amenazas** con información obtenida de análisis avanzados, así como **investigación y respuesta a incidentes** a través de la exploración de datos rápidamente y a escala, y la **protección automatizada contra amenazas,** impidiendo ataques complejos con ML y analíticas de comportamiento. ●



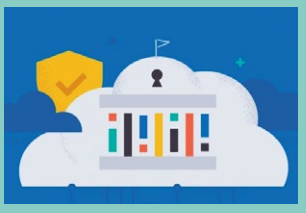
Protección completa del *endpoint*

Su plataforma también incluye, de forma unificada, la protección de puntos finales con su **Elastic Security para**

Endpoint. Con ella, la compañía ofrece una solución que bloquea el *ransomware* y el *malware*, interrumpe amenazas avanzadas con prevención sin firma y analíticas de comportamiento, además de contar con detección centralizada, reducción de falsos positivos y respuesta rápida y a escala, a través de una correlación *ad-hoc*. Entre sus características, destaca que reúne contexto detallado con OSquery e invoca acciones de respuesta remota en todos los *endpoints* distribuidos.

Seguridad de la nube

Para 'ir más allá' en su propuesta, Elastic presentó en 2022 **Elastic Security for Cloud**, con la que la compañía permite cumplir con la postura de protección para entornos híbridos y nativos *cloud* con detección y respuesta de infraestructura (IDR), para proporcionar a las empresas visibilidad profunda de las cargas de trabajo en la nube y contenedores, y ofrecer prevención, detección y respuesta. Entre otras capacidades permite la integración de la seguridad y observabilidad en una sola plataforma, disponiendo de la monitorización de los riesgos



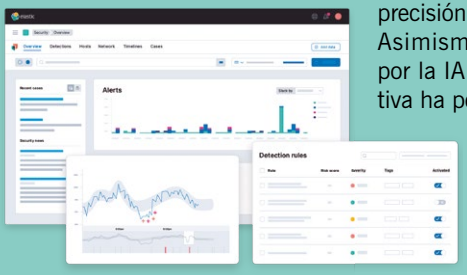
en procesos de implementación y las amenazas en tiempo de ejecución.

Capacidades SOAR nativas

También cabe destacar que, en su apuesta por capacitar a los SOC modernos para optimizar las operaciones de los analistas a través de la automatización, Elastic también anunció, en agosto de 2022, capacidades nativas de seguridad, orquestación, automatización y respuesta (SOAR) a través de Elastic Security. La solución está impulsada por su Elastic Agent y ofrece capacidades nativas de remediación y respuesta para todos los usuarios, así como alertas configurables e integración con otros proveedores de SOAR, lo que permite a las organizaciones implementar SOAR sin necesidad de comprar productos adicionales. Con ella, potencia el crecimiento de casos de uso 'con un solo clic' en cientos de fuentes de datos, al igual que la gestión de su software de protección de seguridad del *cloud* y *endpoints*.

Más allá del SIEM tradicional

Sobre la base del éxito de la compañía en tecnología de búsqueda y análisis de



grandes volúmenes de datos, Elastic creó una propuesta de soluciones con una aproximación XDR en cuyo corazón está el SIEM. Bajo la premisa de que "tu SIEM es tan bueno como los datos que ingesta y analiza", Elastic ofrece un enfoque de SIEM evolucionado, a través del cual, da acceso a todos los datos de seguridad, independientemente del tamaño, la escala o la ubicación, con visibilidad en todo el entorno, para detectar y responder a las amenazas más rápidamente y con mayor precisión.

Asimismo, su apuesta por la IA y la IA generativa ha permitido a Elastic hacer que estas capacidades estén disponibles para todos los analistas de seguridad, a través de su **Elastic AI Assistant**, impulsado por Elasticsearch Relevance Engine (ESRE), que permite interactuar con Elastic Security para investigación de alertas, respuesta a incidentes y generación o conversión de consultas utilizando lenguaje natural, incorporando numerosas indicaciones predefinidas para facilitar el trabajo de los usuarios, según sus necesidades.

Una estrategia diferencial

La plataforma unificada de Elastic, abierta e integrada con ingesta de datos flexible y soporte de la comunidad *open source*, sin bloqueo de proveedor, la ha permitido posicionarse en muy poco tiempo como uno de los referentes del mercado en este ámbito.

Para ello ofrece un valor diferencial apalancado en sus capacidades de protección nativa, con cientos de prevenciones, detecciones y reglas de respuesta mapeadas por MITRE, impulsadas por ML y complementadas con las investigaciones de su Elastic Security Labs.

Junto a ello, también destaca el hecho de estar construida para responder a las necesidades de escalabilidad de las empresas de una manera eficiente, así como la información automatizada a través, por ejemplo, de *runbooks* creados por expertos, enriquecimiento automatizado y gestión del riesgo integrado. A ello se suma que Elastic Security se puede utilizar en local y en la nube de AWS, Azure,

GCP, eliminando la necesidad de *backhaul* de datos.

Además, la manera en la que se licencia es reseñable ya que no se realiza por volumen de datos, sino por los recursos que se van a necesitar usar en el *clúster,* de forma que si se optimiza se consiguen modelos muy eficientes y competitivos en el sector.

Elastic de un vistazo

NYSE: ESTC

Somos la plataforma líder para soluciones impulsadas por tecnologías avanzadas de búsqueda, y ayudamos a todos –las organizaciones, sus empleados y sus clientes– a encontrar lo que necesitan más rápido, mientras mantenemos las aplicaciones funcionando sin problemas y protegiendo contra las amenazas cibernéticas.

Fundada en 2012

+ de 3.000 empleados

Presentes, con plantilla, en **más de 40** países

+ de 20.200 clientes

+ 54% de las compañías de Fortune 500 confían en Elastic

Para más información, comuníquese con nuestro equipo de ventas local en **elastic-revista-sic@elastic.co**