ThreatQuotient o cómo anticiparse a las ciberamenazas

Una plataforma de ciberinteligencia es el eje fundamental para dar respuesta a los incidentes. ThreatQuotient, compañía especializada en plataformas de operaciones de ciberinteligencia, ha abierto oficina en nuestro país de la mano de Eutimio Fernández, su *country manager*, a principios de año. Tras una primera labor de evangelización, la compañía se encuentra inmersa en pruebas de valor en grandes compañías.

Inma Elizalde

Eutimio Fernández, *country manager* de ThreatQuotient

ThreatQuotient abrió oficina en España en enero como parte de su estrategia de expansión. ¿Cuáles son las fortalezas que han visto en nuestro país para ello?

Somos una compañía que se creó como multinacional y como tal está creciendo. En el caso de Europa estamos teniendo datos de crecimiento muy buenos y hacía falta dar un salto. Una vez cubierto Inglaterra, Alemania y Francia hay que ir al sur de Europa. El mercado de la ciberseguridad en España es creciente. Vimos que por el estado de madurez que había, estaba en el punto para abrir oficina y empezar a cubrir este mercado antes que otros. Era la oportunidad de ser la primera empresa invirtiendo aquí, un mercado grande que empieza a madurar y donde podíamos crecer bastante bien.

¿Cuáles son las expectativas puestas en nuestro país?

IR A PÁGINA SIGUIENTE

De momento crecer en la gran cuenta. Nuestro foco va dirigido hacia las empresas que están poniendo en práctica la ciberinteligencia. Hoy en día las compañías que más la están usando y necesitan dar el siguiente paso son las grandes cuentas. Y todos los proveedores de servicio, porque vemos un mercado muy grande de empresa mediana, que necesita de ese tipo de servicios y no se lo puede permitir. Creemos que podemos ayudarles a mejorar su perfil en ciberseguridad, ser más eficaces y reducir los costes.

¿Se van a dirigir solo a las empresas del IBEX-35?

Son nuestro foco principal y en todos ellos vemos un gran interés. Pero también nos dirigiremos al gobierno, sobre todo al área de defensa.

Durante el primer trimestre del año han llevado a cabo una gran labor de evangelización, ¿cuáles son los siguientes pasos que van a dar y cómo lo van a llevar a cabo?

Ya tenemos abiertas pruebas de concepto, pruebas de valor. Estamos en diferentes compañías demostrando cómo implantar no solo la tecnología, porque no hablamos solo de tecnología, sino cómo implantar esta práctica.

No venimos vendiendo un producto. Nos metemos en el *core* de la compañía. Cómo mejorar procesos, el flujo de información entre cada una de las personas y de los estamentos que deben tener información de ciberseguridad. Cómo realizar estas operaciones para adelantarnos a los adversarios e ir un paso por delante.

Estamos trabajando con diferentes empresas para ver cómo pueden mejorar sus procesos, su tecnología, para que la información fluya mejor...

ThreatQuotient es una compañía referente en plataformas de operaciones de ciberinteligencia. Este mercado está aumentando a un ritmo de un 21 % a nivel global según Frost & Sullivant, pero ¿cuál es la situación actual en España?

España está bastante inmadura. Cuando voy a hablar a las grandes compañías de tecnologías cómo las plataformas de inteligencia y como implantar este proceso en las empresas, percibo que todavía estamos un paso por detrás de muchos países europeos.

Las empresas que implantan las plataformas de ciberinteligencia como tal, integrando procesos, personas, información de calidad que fluya y que sea la misma en todas partes, son mínimas.

Es algo que esperamos ir cambiando poco.

¿Podemos decir que los CISO españoles no cuentan con ellas dentro de su estrategia de ciberseguridad?

Se podría decir que sí, aunque se está llegando a soluciones parciales. Están creciendo según se va viendo la necesidad.

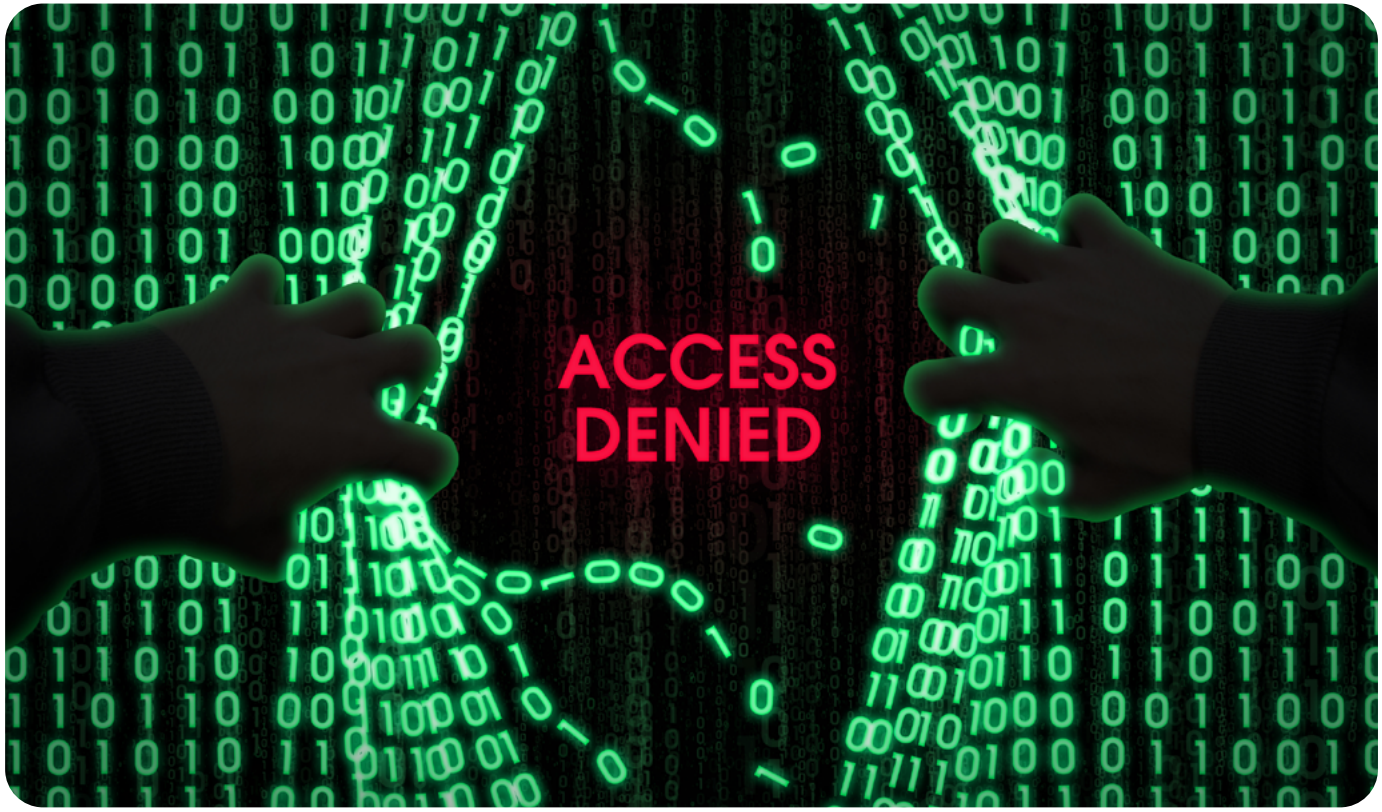
¿Podemos decir que es un mercado virgen en el que tenéis todo por desarrollar?

Hay mucho por desarrollar, sí. No sé si es virgen o digamos poco maduro porque, como he comentado, los CISO tienen conciencia de ello. Pero sus departamentos no han ido evolucionando a la misma velocidad que otros. Se están haciendo cosas, pero a medias. Pasar a la anticipación requiere automatizar, ir tres pasos por delante, que mis defensas estén pensando en lo que puede venir. Y todo esto, si no se automatiza y los procesos no están bien engranados, es complicado.

Estamos en esta fase en la que estamos haciendo cosas. Las compañías ya compran datos de ciberinteligencia. Ya cuentan con empresas externas que les ayudan, pero todavía no han dado el paso de decir lo implanto yo con todos los beneficios que me va a dar. Ese salto se está dando ahora. Creo que hemos llegado en un momento bastante bueno.

ThreatQuotient cuenta con la plataforma ThreatQ. ¿Cuáles son sus principales características? ¿Cómo funciona?

Automatiza lo que hemos comentado. Por un lado, somos capaces de absorber toda la información sobre ciberamenazas. Somos capaces y tenemos conectores para copiar toda la información y para que sea entendible la unimos en un mismo formato, por lo que cada vez que hay una amenaza, sabemos dónde mirar y de qué manera. Cruzamos esta información con la información interna, lo que nos dicen los otros sistemas que están con nuestros *firewalls*, nuestro SIEM. Nos encontramos con millones de piezas de información que tenemos que analizar.



Decidimos qué prioridad tienen nuestras fuentes. Ponemos procedimientos para lo que es crítico. Automatizamos el despliegue de esta inteligencia a todos los elementos. Y aseguramos que la información fluye en toda la empresa.

Es habitual que haya diferentes perfiles en las compañías: alguien que da respuesta a los incidentes, alguien que hace *threat hunting*, el CIO, el CISO... y cada uno tiende a alojar su información formateada para el trabajo que hace. Pero el CISO quiere saber cuál es su nivel de riesgo, qué medidas se están implantando, y si está funcionando bien. Este tipo de flujos también los automatizamos.

Eso, de forma estándar, a una compañía le lleva muchísimo tiempo. Lo que hace la plataforma es coger el flujo masivo de información, priorizarla y que estos flujos de información corran de forma correcta para anticiparnos a un potencial ataque que pueda venir, a la gestión de incidencias que podamos tener.

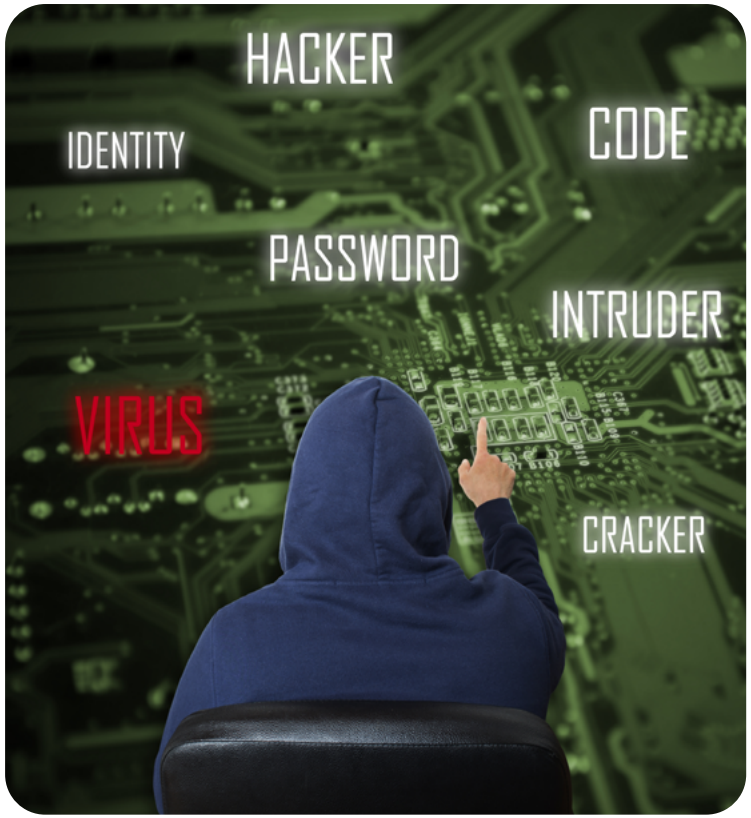
Las empresas cuando implantan soluciones quieren ahorrar tiempo y dinero. ¿En qué manera ThreatQ facilita esto?

Cada dólar que se invierte en la plataforma son ahorros que se cogen en el resto de prácticas.

El ROI es muy amplio. Ahorramos no solo en el coste de adquisición, también en tiempos, en procesos, en definitiva, en todas las áreas.

Además, cuentan con la primera sala de situaciones de ciberseguridad de la industria, ThreatQ Investigations y ThreatQ Exchange. ¿Qué aporta cada una?

ThreatQ Investigations permite que los equipos puedan colaborar en la investigación de una amenaza. Concentrar de forma gráfica todo el análisis y por parte de todo el equipo. Dibujar cuál ha sido el avance de la amenaza. Esto queda plasmado de forma visual para que cualquiera puede entender cómo ha sucedido la amenaza, los pasos que se han ido dando para que sea fructífera o no y las medidas que se están demandando.



"Nuestro foco va dirigido hacia las grandes empresas"

ThreatQ Exchange es la forma que tenemos para que la información se disemine por todos los elementos de seguridad. Garantizar que mis elementos de protección están mirando que protegen lo que para mí es realmente importante.

¿A partir de ahora y tal y como están especializando los cibercriminales sus ataques, podríamos decir que las empresas que no cuenten con este tipo de soluciones de seguridad se quedarán cojas en su estrategia de ciberdefensa?

Podemos decir que no serán capaces de anticiparse. Hoy en día todas las operaciones que estamos viendo son reactivas. Y la bandera de la anticipación es la que estamos echando en falta. Estamos proponiendo el salto hacia la anticipación.