“Ayudamos a las empresas a poner en marcha procedimientos para que ‘hunters’ independientes puedan enviar vulnerabilidades con las garantías legales necesarias”

José Ramón Palanco

CEO de EPIC BOUNTIES

>Por **José Manuel Vera**
>Fotografía: **Jesús A. de Lucas**

Con casi 40 años, este emprendedor español, ingeniero de telecomunicaciones, se ha embarcado en un nuevo reto: conseguir que la malagueña Epic Bounties, fundada en 2020, sea la plataforma mundial de referencia, de habla hispana, en el disputado mercado de los programas de recompensa por fallos de ciberseguridad (comúnmente conocidos por el anglicismo Bug Bounty), una apuesta a la que se han sumado reconocidos especialistas como Jaime Andrés Restrepo (fundador de la comunidad DragonJar), entre otros. Dentro de sus valores diferenciales destaca su pretensión de contar con los mejores investigadores españoles e iberomericanos, prestar servicios a través de los principales MSSP y, también, el cumplimiento de los estándares normativos europeos.

– Hay grandes ‘gigantes’, estadounidenses y europeos, competiendo en el mercado del Bug Bounty. ¿Por qué fundar una empresa priorizando, además, el habla hispana?

– Las razones son varias. No existe ninguna compañía así en el mercado hispano; pero sí hay una fuerte demanda que termina en proveedores de otros países, con lo que supone en cuanto a limitaciones de idiomas o de localización. Para los investigadores (*hunters*), permitimos eliminar la barrera de aquellos que, quizá, están buscando un jugador en el mercado que les hable en su mismo idioma. Además, a las compañías estadounidenses les cuesta cumplir con las normativas europeas: directiva de prevención de blanqueo de capitales, RGPD... En el caso de los europeos no tienen la misma cercanía y, sobre todo, la mayor parte de su comunidad no está formada por investigadores de España y Latinoamérica. En Epic Bounties, además de adecuarnos al cumplimiento de las normativas europeas, ofrecemos a las organizaciones a los mejores investigadores locales, así como un trato mucho más cercano.

– ¿Qué es lo más complicado para hacerse hueco en este mercado?

– Es un paradigma completamente nuevo, pero, sin duda, lo importante es que los responsables entiendan que no deben tener miedo a los investigadores que trabajan en nuestra plataforma, sino a los que cada día intentan, de manera ilegal, encontrar vulnerabilidades. Y solo les podemos hacer frente con este tipo de iniciativas. Me gusta compararlo con las primeras empresas, en España, que ofrecían *hacking* ético, a principios de los 2000, y a las que por descono-

cimiento se las tenía miedo.

– ¿Cuáles son las principales amenazas que se pueden evitar con estos programas?

– Las que más habitualmente se detectan son configuraciones erróneas de servidores, exposición de datos, acceso a servidores no mantenidos... Pero lo interesante del Bug Bounty es que permite encontrar vulnerabilidades totalmente inesperadas, ese es el verdadero reto de los *hunters*.

– ¿Y ante cuáles no ofrecen la protección necesaria?

– De momento, no animamos a participar a organizaciones con activos en infraestructuras críticas, pero sí en entornos réplica. Lógicamente, también consideramos que las revisiones de *hardware* son más complicadas; si bien sí se puede hacer un programa privado y enviar *hardware* a los investigadores, es inviable hacer un programa público en estos casos.

– ¿Qué diferencia a Epic Bounties respecto a su competencia?

En nuestro modelo de negocio hemos incluido a los MSSPs como pieza clave. A parte de que una empresa puede participar individualmente en nuestra plataforma, apostamos por los principales MSSPs para poder entregar un valor añadido a las organizaciones. Y es que son ellos los que mejor conocen a sus clientes, pueden hacer una buena clasificación de activos, seleccionar a los mejores *hunters* y cuentan con capacidades de triaje y remediación. En definitiva, ayudamos a las empresas a poner en marcha los procedimientos necesarios para que investigadores independientes puedan enviar vulnerabilidades con las garantías legales necesarias.

– Un lema que defina el talento y experiencia de Epic Bounties…

– El departamento de Marketing definió perfectamente lo que somos y lo que estamos dispuestos a hacer: "*It's time to be epic*" (Es momento de ser épicos).

– ¿Qué le aporta a un CISO programas como los que ofrecen?

– Permiten detectar vulnerabilidades que no han aparecido ni con soluciones automáticas, ni con auditorías manuales, ya que los *hunters* suelen hacer herramientas a medida, mientras que las automatizadas son muy genéricas y no valen para todos los escenarios. En una auditoría, el equipo suele ser pequeño y tiene una duración muy limitada, mientras que los *hunters* pueden encontrar vulnerabilidades 365 días al año y la comunidad es extensa. Además, los CISOs valoran, de forma importante, que estos programas les permiten optimizar su presupuesto de ciberseguridad, además de su efectividad y garantía de éxito, por los recursos y profesionales que participan.

– Cada vez se contratan más para ayudar al cumplimiento normativo…

Los programas de Bug Bounty también permiten mejorar el cumplimiento normativo de la misma forma que otros métodos que permiten identificar y gestionar vulnerabilidades desconocidas.

"Nuestro modelo de negocio incluye a los Proveedores de Servicios Gestionados de Ciberseguridad (MSSP) como pieza clave, aparte de que una empresa puede participar individualmente en nuestra plataforma"

– ¿Qué retorno tiene el Bug Bounty respecto a otras opciones?

– La principal diferencia es que ellos, tras pagar el *fee* de uso de la plataforma, solo se van a abonar a los fallos de seguridad encontrados. La clave para utilizarlo con éxito consiste en definir cómo de grave sería encontrar una vulnerabilidad en un activo y poner una recompensa razonable. Por poner un ejemplo: si el impacto de una vulnerabilidad puede tener un coste de varios millones, y la recompensa es de miles de euros, el Retorno de la inversión en Seguridad de la Información (ROSI) va a ser mucho mayor que el de una auditoría, que no garantiza encontrar esa vulnerabilidad. Eso sí, en ningún caso Bug Bounty va a reemplazar las auditorías tradicionales, ya que una organización debe haber auditado los activos como paso previo a este tipo de programas. Algún cliente también nos ha preguntado si reemplaza a un Red Team, y tampoco. Mientras que el Red Team pretende acceder y tratar de moverse por la organización, el objetivo de estos programas se centra, principalmente, en la superficie de ataque expuesta.

– ¿Cómo está en España el mercado de Bug Bounty? En EE.UU. hasta la Fuerza Aérea y las agencias federales han apostado por ello…

– Aún hay cierto desconocimiento, pero nos ha alegrado encontrar mucho interés y son varias las organizaciones que no tenían presupuesto para Bug Bounty y, tras presentarles nuestra propuesta, la han tenido en cuenta para el siguiente ejercicio. Estamos comenzando con algunos pilotos en modalidad privada.

– ¿Qué sectores aún son ajenos a este concepto?

– Los de aviación o la navegación marítima son todavía algo ajenos a estos conceptos y pensábamos que la Administración Pública también… Sin embargo, nos hemos dado cuenta, recientemente, que está mostrando muchísimo interés en el modelo, también en España.

– A tenor de la apuesta de EE.UU. (y CISA) por el Bug Bounty, obligando a implantarlo en sus agencias federales, ¿se está realizando la apuesta adecuada en nuestro país?

– Tanto el ejemplo estadounidense como las propias brechas de ciberseguridad, de las que todos hemos sido conocedores –y que no solo han sufrido las administraciones públicas–, han empujado a los responsables de seguridad, a tomar medidas y a analizar todas las soluciones existentes, entre ellas la de Bug Bounty, sobre todo por la efectividad que tiene. En España nos encontramos en una fase muy inicial. Sin embargo, estamos convencidos de que cada vez veremos más iniciativas como la que ha realizado recientemente la Generalitat catalana. Creo que actualmente las administraciones no tienen un enfoque completamente definido, pero son conscientes de las ventajas que ofrece este nuevo modelo y ya están trabajando en ello. Nosotros estaremos encantados de poder ayudar a la Administración en este sentido.

– De los diferentes entornos de TIC –nube, seguridad web, redes, *host*, aplicaciones, etc.–, ¿en cuál va a focalizarse primero Epic Bounties? ¿Y en qué sectores?

– Principalmente pondríamos el foco en API, Aplicaciones Web, Móvil y Cloud. Actualmente

no estamos diferenciando sectores, sino grado de exposición. Pensamos que podemos ayudar mucho más a un cliente que cuenta con múltiples webs, APIs, aplicaciones móviles que a uno que apenas tiene la web corporativa. Existen organizaciones con mucha estructura interna, pero ese no es nuestro foco.

– ¿Qué estrategia comercial van a adoptar para crecer de forma continuada y escalada entre clientes corporativos y MSSP…?

– Nuestra estrategia de cara al mercado actual consiste en priorizar el sector corporativo y a las grandes *startups*, en ambos casos en España y Latinoamérica. También nos centraremos en la Administración. Pretendemos canalizar la mayoría de los clientes corporativos a través de los MSSP, si bien algunos nos han transmitido que prefieren trabajar directamente con nosotros. En este momento estamos en contacto con el 50% de los más importantes del mercado español, comenzando a cerrar nuestras colaboraciones. Por eso, de momento, no podemos dar nombres…

– Recientemente se ha incorporado al proyecto Jaime Andrés Restrepo, (fundador de la comunidad DragonJAR), todo un referente iberoamericano. ¿Qué estrategia de internacionalización tienen previsto acometer?

– Hemos comenzado a trabajar en España, que es nuestro primer mercado, y Latam simultáneamente. Ya estamos hablando con algunas de las organizaciones más grandes de España y Latinoamérica, así como con *startups* tecnológicas de gran volumen. Gracias a los MSSPs, podemos empezar a trabajar fuera de España, de manera muy rápida, y con ayuda de Jaime (referente en Bug Bounty) y la comunidad DragonJAR, podemos acceder a todo el talento de Latam. Eso sí, no queremos quedarnos como la plataforma hispana de Bug Bounty. Tras los primeros años queremos competir en el mercado global, colaborando con los principales MSSP de cada región, comenzando probablemente por Asia y, sobre todo, por Singapur.

– ¿Cómo atraerán a los mejores investigadores y qué exigen? ¿Cómo se da confianza a los clientes de su calidad?

– Para nosotros es crucial estar en contacto con la Comunidad concernida y tener gran conocimiento del sector, por eso pensamos en Jaime Restrepo como un socio estratégico. Por un lado, nos abre las puertas de DragonJAR, una comunidad de más de 400.000 expertos de lengua hispana. Por otro lado, aporta el conocimiento del sector, ya que es un *hunter* reconocido que ha colaborado con organizaciones como Harvard University, Netflix, Sony, Visa, Mastercard, AT&T, IBM, Redbull, Yahoo!, General Motors y Alibaba, entre otras.

Antes de abrir nuestro primer programa público, el de nuestra propia plataforma, ya teníamos a cientos de *hunters* –incluso de habla no hispana– a la espera de poder registrarse. Para nosotros el mejor especialista es el que no solo es capaz de encontrar vulnerabilidades complejas o de idea feliz, sino que es capaz de explicar bien los detalles y es colaborativo: estas características son evaluadas por los clientes, quienes otorgarán puntos a los *hunters* y valen como referencia a otras empresas para conocer la calidad de trabajo de cada uno de los investigadores de la plataforma. Independientemente de eso, estamos trabajando en crear CTF (*Capture The Flag*), que permitan obtener puntos extra válidos en nuestra plataforma y así encontrar talento emergente.

– Aún hay muchas empresas escépticas y desconfiadas por plantearse pagar por trabajos que impliquen que externos puedan 'entrar' en sus sistemas…

– Las organizaciones más grandes están recibiendo ataques, por parte de cibercriminales, que tratan de encontrar información para venderla o explotarla. Como ejemplo, podemos encontrar en la Dark Web un mercado negro de acceso remoto a diversas corporaciones y entidades. En el momento en el que se abre un programa de Bug Bounty y un *hunter* reporta una vulnerabilidad y esta es corregida, deja de tener valor en el mercado negro. No tiene sentido que los atacantes reales puedan seguir localizando vulnerabilidades sin permiso y tratar de limitar el acceso a investigadores que quieren ayudarnos. Eso sí, siempre de forma legal.

– ¿Cómo se evita que los investigadores que participan en estos programas incurran en actuaciones poco éticas?

En el momento en el que un *hunter* se registra en nuestra plataforma, acepta determinadas condiciones y códigos éticos. Además, cada investigador registrado pasa por un proceso de *Know Your Customer* (KYC), para identificarlo con DNI o Pasaporte. Nuestra plataforma cuenta con un sistema de clasificación que otorga o elimina puntos a los *hunters* por su destreza y comportamiento en los diferentes programas. Los que acrediten más puntos podrán ser invitados a los mejores programas privados, en los que las empresas eligen a los investigadores que quieren que participen en función de su perfil. Por eso, en ellos, de manera opcional, realizamos un proceso de *screening* o '*background check*' con un análisis exhaustivo de los participantes.

– El objetivo de Epic Bounties para 2021…

– Este año nuestro reto es evangelizar acerca del uso de Bug Bounty y ayudar a las organizaciones a dar sus primeros pasos con programas privados. Para 2022 nos gustaría comenzar a innovar con nuevas funcionalidades que no ofrecen actualmente plataformas similares. Por ejemplo, estamos dando los primeros pasos para desarrollar una 'plataforma de conocimiento cero' que permita la comunicación directa entre *hunter* y empresa, no teniendo nosotros acceso a ello. Así que ofrece la máxima confidencialidad y seguridad.

– ¿Acudirán a rondas de financiación?

– Actualmente hemos recibido 330.000 euros de inversión como capital semilla y ya estamos empezando a trabajar en la siguiente ronda.

– Para concluir, brinde un consejo para los investigadores que quieran vivir de los programas de Epic Bounties…

– Los *hunters* que más dinero ganan no están especializados en fallos de 'día cero', muy complicados de encontrar, sino en vulnerabilidades concretas. Para dar con ellas se hacen sus propias herramientas, las aplican a programas públicos y, muchos, llegan a ganar entre 20.000 y 30.000 euros al mes. Los mejores, además, son seleccionados para programas privados. Pero esto no va a durar siempre. Vamos a un entorno donde será, cada vez, más complejo dar con vulnerabilidades, aunque también se pagarán mejor. ■

"Si el impacto de una vulnerabilidad puede tener un coste de varios millones, y la recompensa es de miles de euros, el Retorno de la inversión en Seguridad de la Información (ROSI) va a ser mucho mayor que el de una auditoría, que no garantiza encontrar esa vulnerabilidad"