YES WE HACK

OUTSCALE

OUTSCALE

Programa Público de *Bug Bounty*

ESTUDIO DE CASO

¿QUÉ LES LLEVÓ A PONER EN MARCHA UN PROGRAMA DE *BUG BOUNTY*?

EDOUARD CAMOIN, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, 3DS OUTSCALE:

Tenemos la certificación ISO 27001 desde 2014 y estamos obligados a utilizar test de penetración para buscar vulnerabilidades. Al principio, los test de penetración resultaron útiles. Sin embargo, con el tiempo, generaron menos resultados interesantes. Rápidamente nos dimos cuenta de que, debido a la limitada duración de una auditoría (de 2 a 3 semanas), el probador de penetración no tenía tiempo para identificar vulnerabilidades más graves. En el mejor de los casos, tenía corazonadas, pero había que trabajarlas.

También vimos que, durante varios años, el *bug bounty* había funcionado bien en Estados Unidos.

Sondeamos las opciones del *red team* y del *bug bounty*, con investigadores de diversos orígenes para hacer pruebas en nuestras áreas de aplicación y descubrir nuevas vulnerabilidades.

Si hubiéramos optado por el *red team*, nos habríamos encontrado con el mismo problema que tuvimos con los test de penetración clásicos que señalé antes. Así que optamos por lanzar el *bug bounty* considerando que, aunque los probadores de penetración ya no encontraban nada, eso no significaba que no hubiera otros problemas.

Empezamos con un programa privado colaborando con unos 15 *hunters* porque no estábamos "seguros" del funcionamiento de nuestras aplicaciones. Los *hunters* identificaron algunas vulnerabilidades importantes. Poco a poco fuimos invitando a más *hunters* antes de abrirlo al público con dos áreas de aplicación: nuestro servicio de infraestructura y nuestro portal para clientes.

¿PUEDE DESCRIBIR LA EVOLUCIÓN Y EL DESARROLLO DE SU PROGRAMA?

EDOUARD CAMOIN, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, 3DS OUTSCALE:

La implantación del programa fue razonablemente rápida: un año. Cuando lo hicimos público, no experimentamos un repunte brusco de vulnerabilidades: empezamos con una parrilla de bonificaciones muy razonables, que fuimos incrementando gradualmente para reactivar la actividad de los *hunters* en nuestro programa hasta alcanzar nuestra actual "velocidad de crucero".

¿INFLUYÓ LA SOBERANÍA EN SU DECISIÓN DE TRABAJAR CON YESWEHACK?

EDOUARD CAMOIN, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, 3DS OUTSCALE:

Sí, desde luego. Cuando nos planteamos el *bug bounty*, nuestro objetivo era tanto la calificación SecNumCloud de ANSSI como la certificación HDS. Por ello, nos pareció más oportuno trabajar con un socio también francés, que nos diera garantías sólidas sobre la gestión de nuestros datos.

¿TRABAJAR CON UNA PLATAFORMA SOBERANA SUPONE ALGUNA VENTAJA A LA HORA DE ABORDAR EL MERCADO?

EDOUARD CAMOIN, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, 3DS OUTSCALE:

Sí, el concepto de soberanía es esencial para nuestros clientes franceses y europeos. Entre ellas se encuentran organizaciones públicas y parapúblicas junto con organizaciones de importancia estratégica (OIV, Operadores de Importancia Vital), que son sensibles a las cuestiones de soberanía y control de sus datos. En el contexto del suministro de servicios en la nube, la asociación con una plataforma soberana como YesWeHack garantiza a nuestros clientes que la cadena de procesamiento de vulnerabilidades de extremo a extremo está controlada de forma eficaz.

En un sentido más amplio, el *bug bounty* ofrece a Outscale una ventaja competitiva porque garantiza una seguridad activa: donde antes realizábamos test de penetración bianuales y escaneos periódicos, ahora buscamos vulnerabilidades continuamente. En el momento en que un *hunter* señala una vulnerabilidad, podemos incluirla en nuestro ciclo de corrección automáticamente. Nuestros clientes están tranquilos, ya que saben que no esperamos las actualizaciones de los proveedores para corregir nuestras vulnerabilidades. Además, somos capaces de detectar y corregir las vulnerabilidades de los productos que desarrollamos internamente.

¿CUÁL ES EL VERDADERO VALOR DEL *BUG BOUNTY*?

EDOUARD CAMOIN, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, 3DS OUTSCALE:

En primer lugar, los *hunters* no tienen limitaciones de tiempo. Pueden tomarse el tiempo necesario para detectar vulnerabilidades sofisticadas, desarrollar un *exploit*, sugerir soluciones y redactar un informe detallado. En cambio, los test de penetración suelen dar como resultado unos pocos escaneos y dos o tres vulnerabilidades estándar (CVE), sin ninguna prueba concreta de *exploit*.

La diversidad de la comunidad es otra ventaja: Se puede intercambiar con *hunters* especializados, por ejemplo, en interfaz de usuario (UI) o en servicios de aplicaciones. Cada *hunter* ofrece cosas diferentes y complicadas que un auditor "no especializado" nunca podría encontrar. A veces, uno diría que hay que estar loco para darse cuenta de esas cosas

Tengo acceso a un montón de experiencia. Y encuentran cosas que nadie encontraría.

Mi equipo está familiarizado con diferentes enfoques, gracias a conversaciones con gente que tiene diferentes enfoques de la gestión de la vulnerabilidad. A veces tenemos que explicar que un hallazgo no es una vulnerabilidad, sino una mala práctica por su parte o cosas por el estilo.

Por último, pero no menos importante, con el tiempo se crea un vínculo con los *hunters* individuales. Si un investigador descubre vulnerabilidades importantes y quiere probar cosas más complejas, entonces le damos los recursos o el acceso para hacer cosas más emocionantes. Este enfoque profundo y de colaboración es imposible de alcanzar con los típicos probadores de penetración, constantemente abrumados y atrapados en plazos cortos.

"Tengo acceso a un montón de experiencia. Y encuentran cosas que nadie encontraría.

¿SUPONE EL *BUG BOUNTY* EL FINAL DE LOS *PENTEST* O ES ALGO COMPLEMENTARIO?

EDOUARD CAMOIN, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, 3DS OUTSCALE:

En mi opinión, son dos enfoques completamente distintos. Utilizo los test de penetración por lo que valen como certificados y para cumplir con normas específicas: me permiten satisfacer a clientes que requieren dichas certificaciones. Por su parte, el *bug bounty* responde a la necesidad de una seguridad más operativa y de centrarse en todo lo que los test de penetración y los escaneos clásicos no son capaces de detectar.

¿HA OBSERVADO ALGÚN CAMBIO EN SUS EQUIPOS DESDE QUE OUTSCALE COMENZÓ A UTILIZAR EL *BUG BOUNTY*?

EDOUARD CAMOIN, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, 3DS OUTSCALE:

En el Centro de Operaciones de Seguridad (SOC en inglés), gestionamos los programas existentes, los bonos y las relaciones con los *hunters*, la creación de nuevos programas y cualquier cambio en los ámbitos. Los informes del *bug bounty* llegan al equipo del SOC, que luego evalúa cada vulnerabilidad.

En el 90 % de los casos, se trata de vulnerabilidades no críticas que se valoran rápidamente. Si hay alguna duda, la discutimos internamente. Si la vulnerabilidad es especialmente interesante, la persona encargada de gestionarla la presenta al equipo. A continuación, hablamos de su posible impacto, de las soluciones que podemos utilizar, de las recomendaciones del *hunter* y de cómo podemos asegurarnos de que no se repita. Estos intercambios aumentan las habilidades de todo el equipo.

> **“ El *bug bounty* responde a la necesidad de una seguridad más operativa y de centrarse en todo lo que los test de penetración y los escaneos clásicos no son capaces de detectar.**

¿HAN CONSEGUIDO TAMBIÉN QUE SUS EQUIPOS COLABOREN MÁS ESTRECHAMENTE?

EDOUARD CAMOIN, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, 3DS OUTSCALE:

Sí, porque estimula la curiosidad: la gente se motiva y quiere comprender. Resulta siempre más concreto mostrar una vulnerabilidad real que ocurrido en la plataforma.

¿Y SUS EQUIPOS Y LA ORGANIZACIÓN SE HAN VUELTO MÁS ÁGILES?

EDOUARD CAMOIN, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, 3DS OUTSCALE:

Trabajamos en integración continua, y el *bug bounty* se presta a nuestros métodos ágiles.

Cuando recibimos un informe de vulnerabilidad, sopesamos las métricas de evaluación de vulnerabilidades (CVSS) y, en función de esa puntuación, determinamos el plazo de reparación. El informe se envía directamente a los equipos correspondientes para su corrección. Lo mismo ocurre con las dependencias utilizadas en el código; se envían a I+D para su análisis y la actualización de versiones. En todos los casos, el *bug bounty* es un punto de entrada como cualquier otro, y como tal, las vulnerabilidades se gestionan a través de tarjetas.

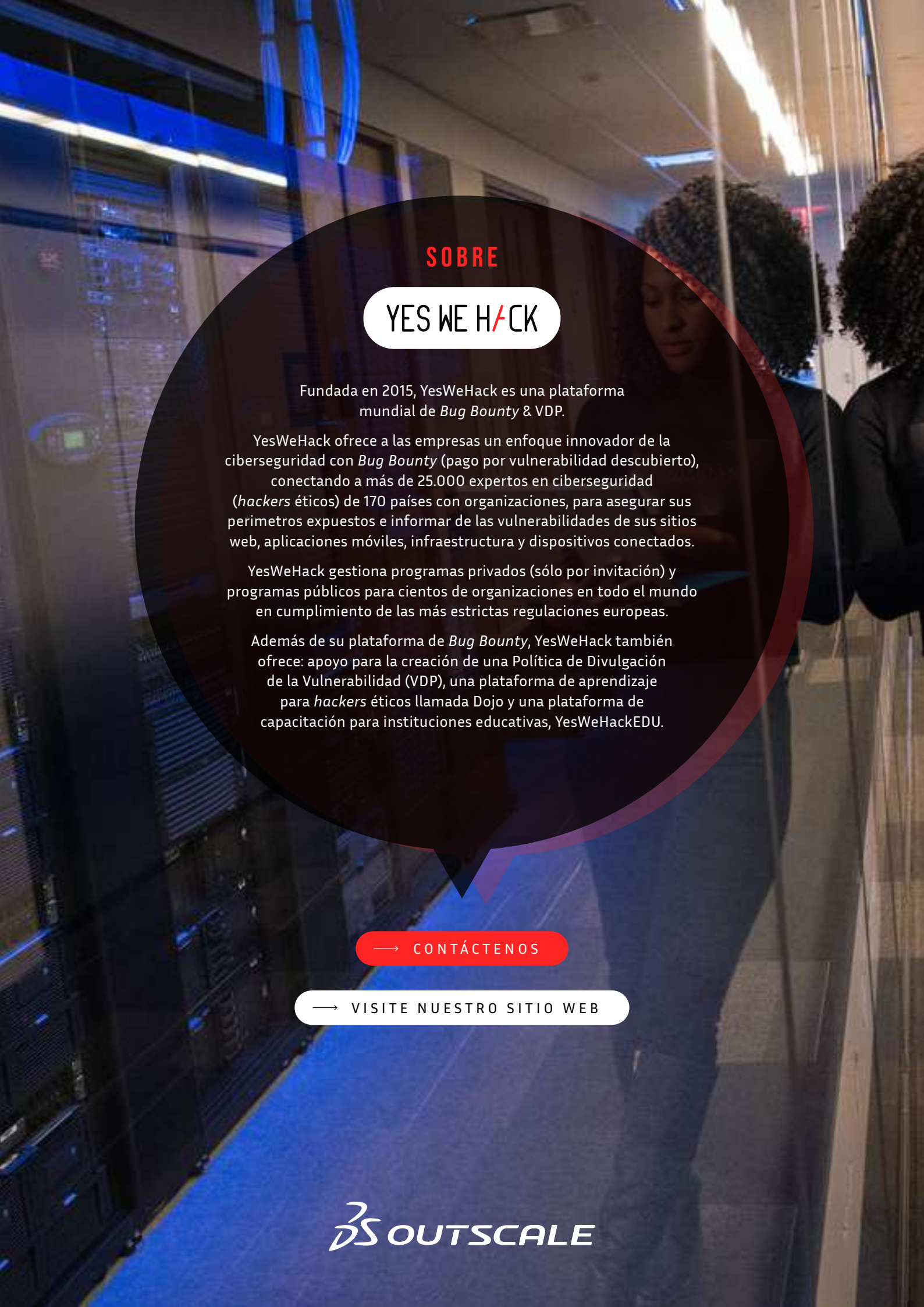
Adaptamos el tratamiento en función de la urgencia: si se requiere una corrección rápida, entregamos un parche inmediatamente, que se reincorpora en la siguiente versión. En este caso, creamos (o modificamos) una historia de usuario utilizando estos nuevos elementos, que servirán de base para los desarrollos.

¿CUÁLES SERÁN LOS SIGUIENTES PASOS?

EDOUARD CAMOIN, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, 3DS OUTSCALE:

Ampliaremos nuestro alcance en los programas. También animaremos a los *hunters* a "profundizar" en nuestro producto, más allá del desarrollo de una interfaz basada en la web. Y aumentaremos la parrilla de bonificaciones.

También me gustaría darles acceso a nuestras plataformas privadas para que puedan realizar pruebas más estrictas. Ya lo hemos probado una vez, y obtuvimos resultados muy interesantes, con escenarios de extracción de datos codificados en nuestras plataformas de prueba. Sin embargo, esto implica dar a los *hunters* áreas de aplicación del test específicas, algo que lleva mucho tiempo.



SOBRE

YES WE HACK

Fundada en 2015, YesWeHack es una plataforma mundial de *Bug Bounty* & VDP.

YesWeHack ofrece a las empresas un enfoque innovador de la ciberseguridad con *Bug Bounty* (pago por vulnerabilidad descubierto), conectando a más de 25.000 expertos en ciberseguridad (*hackers* éticos) de 170 países con organizaciones, para asegurar sus perimetros expuestos e informar de las vulnerabilidades de sus sitios web, aplicaciones móviles, infraestructura y dispositivos conectados.

YesWeHack gestiona programas privados (sólo por invitación) y programas públicos para cientos de organizaciones en todo el mundo en cumplimiento de las más estrictas regulaciones europeas.

Además de su plataforma de *Bug Bounty*, YesWeHack también ofrece: apoyo para la creación de una Política de Divulgación de la Vulnerabilidad (VDP), una plataforma de aprendizaje para *hackers* éticos llamada Dojo y una plataforma de capacitación para instituciones educativas, YesWeHackEDU.

⟶ CONTÁCTENOS

⟶ VISITE NUESTRO SITIO WEB

3DS OUTSCALE