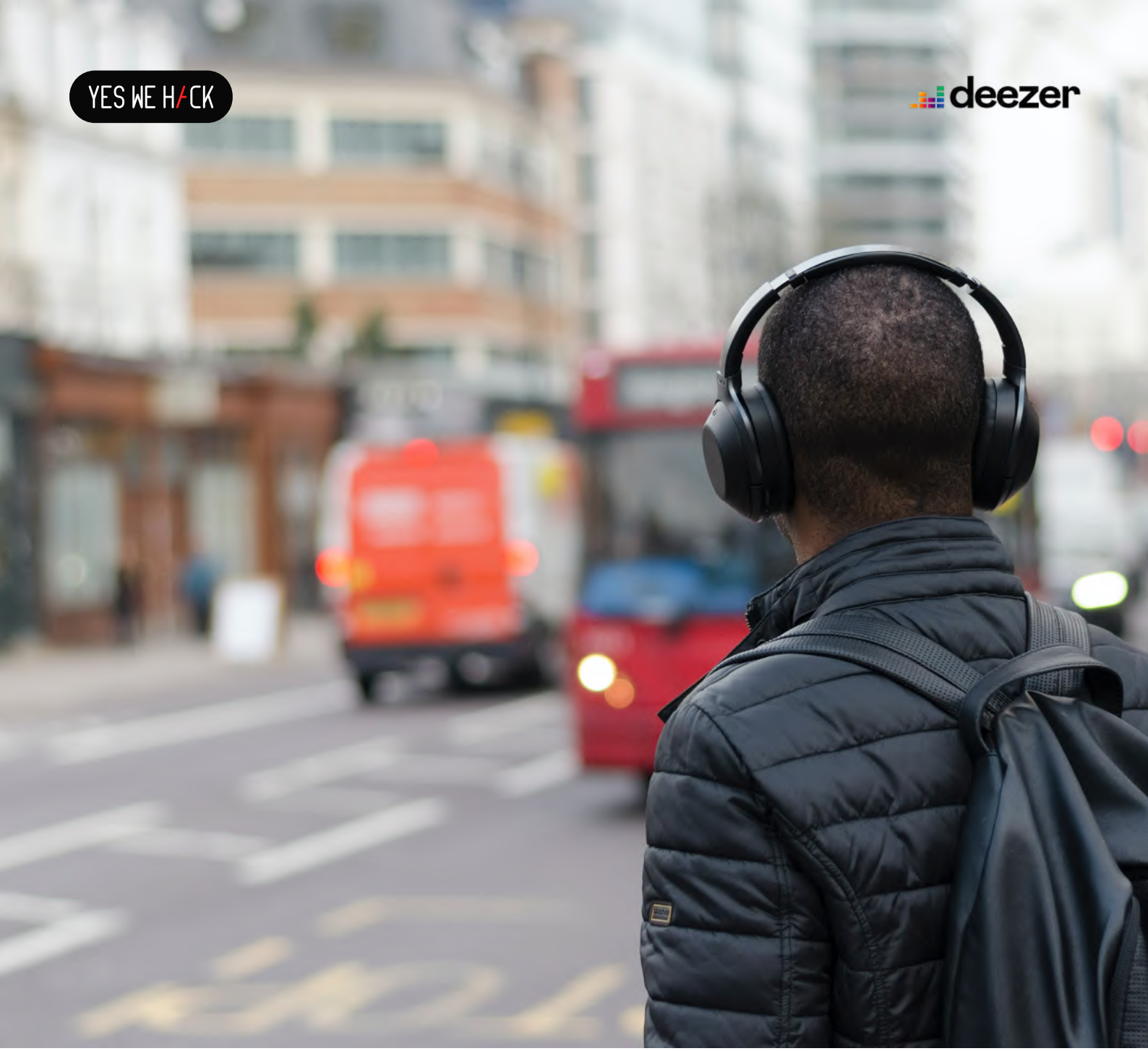

YES WE HACK
deezer
DEEZER
Programa público de Bug Bounty
ESTUDIO DE CASO



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

ROMAIN LODS, JEFE DE INGENIERÍA DE DEEZER:

Unos dos años antes de lanzar nuestro programa de Bug Bounty, habíamos empezado ya a hacer auditorías de seguridad a nivel interno sobre nuestro código, algo que nunca antes se había hecho en Deezer.

Dichas pruebas nos permitieron dar el primer paso y corregir importantes vulnerabilidades. Posteriormente, por las circunstancias, nos decidimos por el Bug Bounty y YesWeHack.

La facilidad de uso de la plataforma consiguió convencernos de lo interesante de poner en marcha un programa.

A SU JUICIO, ¿QUÉ VENTAJAS TIENE EL BUG BOUNTY FRENTE A SOLUCIONES TRADICIONALES COMO EL PENTEST?

ROMAIN LODS, JEFE DE INGENIERÍA DE DEEZER:

Habitualmente se lleva a cabo una auditoría anual sobre varios de nuestros servicios, con una duración de una a tres semanas. Se trata de un planteamiento costoso, que se centra cada vez en algunos servicios concretos y, tras varios años, deja de mostrar resultados interesantes.

El Bug Bounty nos permite obtener informes todo el año sobre diversas áreas y detectar errores rápidamente tras su aparición.

En cuanto al ROI (retorno de la inversión), el Bug Bounty resulta también muy atractivo, al decidir nosotros mismos la recompensa que se asigna a cada vulnerabilidad.

El Bug Bounty nos garantiza asimismo una diversidad de competencias de los investigadores. En cambio, los auditores están altamente especializados y se les orienta hacia lo que deseamos que se compruebe. Con el Bug Bounty, nos han sorprendido mucho ciertas observaciones de investigadores que nos han transmitido los resultados de hipótesis bastante originales, nunca vistas con anterioridad.

En fin, aprecio la calidad de los informes de errores que nos llegan a través de YesWeHack: se nota que los investigadores tratan realmente de ofrecer una prueba de concepto (POC) funcional, reproducible, que podemos fácilmente volver a testar internamente.

> **“El Bug Bounty nos permite obtener informes todo el año sobre diversas áreas y detectar errores rápidamente tras su aparición.**

Los informes de nuestras auditorías habituales son bastante precisos en general, pero esta precisión también se aprecia en el ámbito del Bug Bounty, ya que los investigadores son competentes y saben lo que hacen. Es un verdadero placer recibir sus informes ilustrados con pantallazos y vídeos, que facilitan mucho su comprensión, su verificación y su comunicación a los equipos correspondientes.

Asimismo se facilitan los intercambios de información con los investigadores a través de la plataforma cuando se necesitan precisar ciertos datos.

deezer

¿LOS HACKERS LES AYUDAN PARA ANALIZAR Y CORREGIR LOS BUGS RECIBIDOS?

ROMAIN LODS, JEFE DE INGENIERÍA DE DEEZER:

Efectivamente, pueden ayudarnos en la fase de reproducción de fallos. En ciertos casos los empleamos incluso para verificar que la vulnerabilidad se ha corregido.

Sin embargo, esto no deja de ser algo puntual, ya que contamos con un gran equipo interno de desarrolladores que se ocupan de la gestión de estas incidencias.

PARA USTED, ¿EL BUG BOUNTY SIGNIFICA EL FIN DEL PENTEST O ES COMPLEMENTARIO?

ROMAIN LODS, JEFE DE INGENIERÍA DE DEEZER:

A mi juicio, sigue siendo absolutamente complementario. El Bug Bounty es una herramienta que va más allá de la auditoría.

Como decía hace un momento, el pentest, tal y como se utiliza hasta ahora, se centra en los nuevos servicios o en las áreas en las que se sabe de antemano que hay problemas.

deezer

¿HA PERCIBIDO CAMBIOS DENTRO DE SUS EQUIPOS DESDE QUE LANZARON EL BUG BOUNTY?

ROMAIN LODS, JEFE DE INGENIERÍA DE DEEZER:

Es evidente que hay una creciente concienciación con respecto a la seguridad. Hemos puesto en marcha grandes proyectos para reforzar la seguridad como consecuencia de los reportes de nuestro programa de Bug Bounty.

La visión ha evolucionado y las cosas han cambiado respecto a la ciberseguridad, siendo el Bug Bounty uno de los impulsores de este cambio.

En cuanto al proceso, los informes son recopilados, seleccionados y validados. Posteriormente, sobre la base de los elementos de cada informe validado, se crea un ticket interno y se le asigna al equipo encargado para su tratamiento con un grado de prioridad determinado.

¿CONSIDERA A BUG BOUNTY COMO UN INSTRUMENTO FIABLE DE CARA AL MERCADO?

ROMAIN LODS, JEFE DE INGENIERÍA DE DEEZER:

Bajo mi punto de vista, sí. Por medio de un programa de Bug Bounty público, demostramos y ponemos de manifiesto nuestra preocupación por la seguridad y la transparencia. Se asume también el hecho de exponerse a los ataques, por supuesto “controlados”, y de tener en cuenta los comentarios críticos de la comunidad.

En Deezer, contamos con un equipo dedicado a la lucha contra el fraude, ya que a los artistas y los sellos discográficos se les remunera según la audiencia de las pistas. De este modo, para garantizar sus ingresos, debemos protegerlos contra cualquier abuso en la plataforma. Por lo tanto, esta cuestión es crucial en nuestra estrategia de seguridad y dentro del alcance del Bug Bounty.

> **“Por medio de un programa de Bug Bounty público, demostramos y ponemos de manifiesto nuestra preocupación por la seguridad y la transparencia.**

YES WE HACK

¿CUÁL SERÁ EL SIGUIENTE PASO?

ROMAIN LODS, JEFE DE INGENIERÍA DE DEEZER:

Por ahora, seguimos con nuestra estrategia actual, reactivando de manera regular el programa cuando la actividad disminuye.

En términos generales, el número de comunicaciones de vulnerabilidades depende a menudo de la visibilidad en la actualidad de Deezer y cuando hacemos campañas de comunicación, los investigadores muestran más interés por nuestro programa.

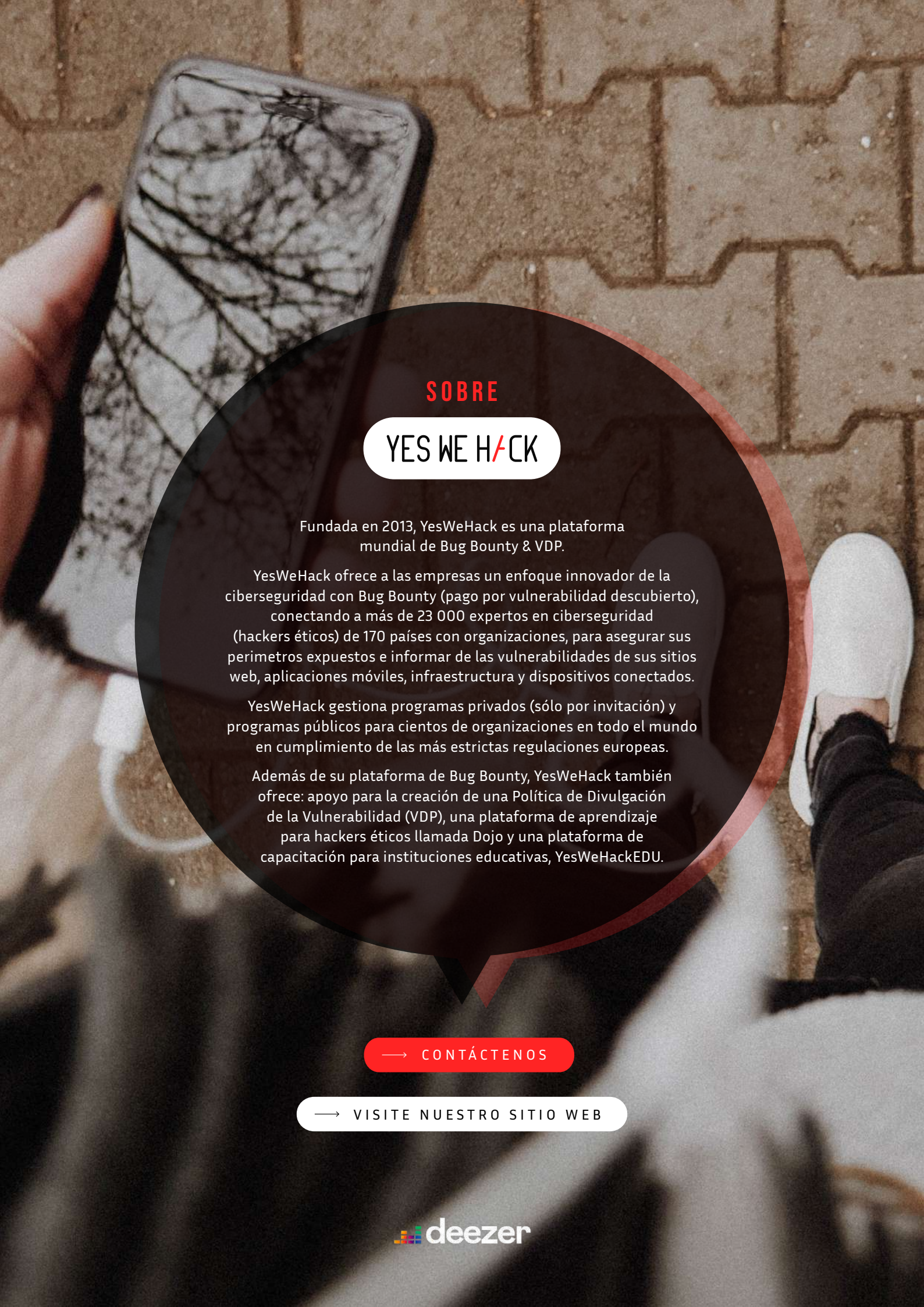
Más adelante, consideraremos un aumento de las recompensas para animar a los investigadores a encontrar fallos más complejos.

¿DARÍA ALGÚN CONSEJO A LOS CISO O A LAS STARTUPS QUE ESTÁN PENSANDO EN LANZARSE AL BUG BOUNTY?

ROMAIN LODS, JEFE DE INGENIERÍA DE DEEZER:

Como regla general, es mejor conocer los fallos de seguridad cuando se pone en marcha un proyecto que esperar a que haya demasiadas cosas que gestionar una vez hecha una (mala) elección de arquitecturas.

Cuando veo lo que ha detectado nuestro programa de Bug Bounty, pienso que hubiera sido preferible haber tenido en cuenta estos elementos desde el principio. Por lo tanto, aconsejaría no esperar demasiado para implementar herramientas como el Bug Bounty, para minimizar así la dependencia de los sistemas heredados, más difíciles de proteger.



SOBRE

YES WE H/CK

Fundada en 2013, 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 23 000 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

deezer