
YES WE H/CK
OVHcloud
OVHCLOUD
Programa Público de *Bug Bounty*
ESTUDIO DE CASO

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

JULIEN LEVRARD, DIRECTOR DE OPERACIONES DE SEGURIDAD, OVHCLOUD:

La seguridad siempre ha formado parte del ADN de OVHcloud. Es algo inherente a nuestro negocio como proveedor de infraestructuras y a todos los servicios que ofrecemos. La seguridad de nuestras infraestructuras es un objetivo permanente y sirve para generar confianza en nuestros clientes. Esa seguridad se basa en salvaguardas físicas y lógicas y en actividades de supervisión, escaneos, pruebas de penetración internas y externas, revisiones de código y configuración, y otras medidas de seguridad. Algunas de estas salvaguardas son gestionadas de forma ininterrumpida por nuestros equipos, mientras que otras dependen de la colaboración con terceros de confianza.

Hace varios años realizamos un *bug bounty* para OVH con YesWeHack a fin de añadir una capa de seguridad a nuestros sistemas existentes. Nuestras empresas comparten los mismos valores fundamentales y evolucionan en el mismo ecosistema; compartimos la misma pasión y las mismas raíces europeas. En parte por estas razones comenzamos con esta plataforma: participamos en el Primer programa público de YesWeHack y pusimos en marcha nuestro programa durante un *bug bounty* en vivo en la parisina *Nuit du Hack*.

¿EL *BUG BOUNTY* REFUERZA LA CONFIANZA DE LOS CLIENTES?

JULIEN LEVRARD, DIRECTOR DE OPERACIONES DE SEGURIDAD, OVHCLOUD:

Sí, desde luego. OVHcloud trabaja con diferentes tipos de clientes. Algunos de ellos gestionan ellos mismos su infraestructura y son muy receptivos a las comunicaciones técnicas. Por ello, nuestra comunicación se basa en la transparencia y la fiabilidad. Otros clientes son más conscientes de nuestra capacidad para incorporar a terceros de confianza, como auditores de certificación o proveedores de servicios externos. El *bug bounty* ofrecen un grado de confianza adicional para algunos de nuestros clientes que exigen más que las medidas de seguridad tradicionales.

YesWeHack trabaja con grandes organizaciones estratégicas como los OVI (Operadores de Importancia Vital) y también actuamos en ese mercado. El *bug bounty* de YesWeHack forma parte de este ecosistema de confianza y se está convirtiendo en algo imprescindible para organizaciones como la nuestra. También es una cuestión de reputación entre la comunidad de *hunters*, que son parte interesada en este mundillo: a través de YesWeHack, podemos interactuar con personas que no siempre están disponibles a través de otros canales.

> **El *bug bounty* nos pone en contacto con expertos con conocimientos que complementan a nuestros equipos en todo el espectro de tecnologías que utilizamos.**

¿QUÉ OFRECE EL *BUG BOUNTY* EN LOS SERVICIOS QUE HA SEÑALADO: AUDITORÍAS, ESCANEOS, PRUEBAS DE PENETRACIÓN...?

JULIEN LEVRARD, DIRECTOR DE OPERACIONES DE SEGURIDAD, OVHCLOUD:

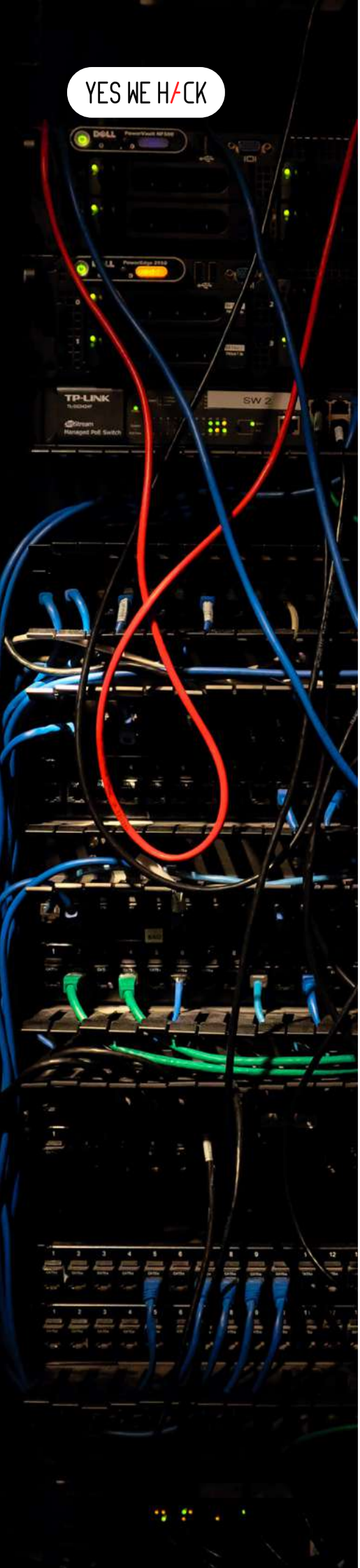
El *bug bounty* nos pone en contacto con expertos con conocimientos que complementan a nuestros equipos en todo el espectro de tecnologías que utilizamos. Esto incluye OpenStack, Kubernetes, herramientas de aprendizaje automático e IA. Es imposible encontrar un equipo de probadores de penetración con conocimientos avanzados en todas estas tecnologías.

YesWeHack nos permite acceder fácilmente a expertos en estas diversas tecnologías que comentan cosas como: "*Soy experto en Kubernetes. Voy a echarles un vistazo a estos programas de* bug bounty *que tienen ofertas de Kubernetes y voy a meterme a fondo.*" Así se completa eficazmente nuestro enfoque de seguridad, al aportar una perspectiva que complementa la de nuestros equipos.

El *bug bounty* también ofrecen un marco formal para la notificación de vulnerabilidades. Nos permite ofrecer un punto de entrada legalmente seguro para los *hunters*. Aunque no es el único canal de OVHcloud para informar sobre vulnerabilidades, recomendamos a cualquiera que "encuentre" vulnerabilidades que utilice nuestro programa. De este modo, disponemos de una sola entrada y un proceso vinculado para gestionar los informes de vulnerabilidad. Por lo tanto, es una parte definitoria de nuestra divulgación coordinada de vulnerabilidades (CVD).

Aparte de las ventajas del *bug bounty* como modelo, destacaría la plataforma de YesWeHack, que tiene una interfaz de usuario muy intuitiva. Los comentarios acerca de la gestión del flujo de trabajo, el procesamiento de los informes y las interacciones con los *hunters* que nos llegan desde el equipo de OVHcloud encargado del programa de *bug bounty* son excelentes.

Con las API logramos integrar información útil en nuestras propias herramientas y cuadros de mando de forma automática. También podemos hacer un seguimiento de nuestro presupuesto de bonificaciones y de la actividad de cada programa. De un vistazo, calibramos el estado de nuestros programas y podemos informar rápidamente a la dirección acerca de los indicadores. El *bug bounty* está totalmente integrado en nuestra estrategia global de seguridad.



OVHcloud

¿QUÉ PAPEL DESEMPEÑA EL *BUG BOUNTY* EN SU METODOLOGÍA DE DESARROLLO ÁGIL?

JULIEN LEVRARD, DIRECTOR DE OPERACIONES DE SEGURIDAD, OVHCLOUD:

Nuestro equipo de probadores de penetración supervisa nuestro *bug bounty* por errores: tenemos dos directores a cargo del programa que además lideran la comunidad de *hunters*. A continuación, trabajan con los distintos equipos afectados por las vulnerabilidades para que podamos integrarlas en nuestros sistemas de gestión y garantizar su corrección.

Una vez que se comunican las vulnerabilidades a través de la plataforma, las integramos en nuestros procesos: tenemos toda una estructura organizativa que denominamos sistemas de gestión de la seguridad, dentro del marco de certificación ISO 27001. Los procesos documentados, las funciones y las responsabilidades garantizan que cada vulnerabilidad, incidente o amenaza potencial sea procesada y supervisada en el tiempo por nuestros equipos. También forma parte de un plan de acción detallado cuya aplicación se verifica en función de la sensibilidad del producto en cuestión y del nivel de exigencia asociado. Gracias a las API de YesWeHack, podemos integrar fácilmente los informes de *bug bounty* en este proceso. Todo se gestiona mediante tarjetas que se pueden ver en nuestros tableros y a las que pueden acceder nuestros auditores externos.

> **Hemos entablado una relación en la que se comentan de manera abierta las conclusiones acerca de cómo analizar cada vulnerabilidad. No hay otra forma de tener una comunicación tan productiva.**

ESTÁ EN UN PROGRAMA PÚBLICO, ¿CÓMO SON SUS INTERCAMBIOS CON LA COMUNIDAD?

JULIEN LEVRARD, DIRECTOR DE OPERACIONES DE SEGURIDAD, OVHCLOUD:

Gestionar un *bug bounty* es un compromiso real con todas las partes interesadas en lograr que Internet sea más segura. Tenemos la responsabilidad de ser rigurosos y transparentes en la gestión y resolución de las vulnerabilidades notificadas. Esto se vuelve más sencillo por el hecho de que la plataforma proporciona un marco que facilita las relaciones entre clientes y *hunters*, con una comunicación muy rica y muy directa. Hemos entablado una relación en la que se comentan de manera abierta las conclusiones acerca de cómo analizar cada vulnerabilidad. No hay otra forma de tener una comunicación tan productiva.

¿CUÁLES SERÁN LOS SIGUIENTES PASOS?

JULIEN LEVRARD, DIRECTOR DE OPERACIONES DE SEGURIDAD, OVHCLOUD:

Estamos trabajando para estandarizar la integración de las tarjetas que se generan en los informes de vulnerabilidad en nuestro modelo global de gestión de riesgos. El objetivo es unificar nuestra gestión de riesgos con independencia de la fuente de información, ya sea un incidente probado o un informe de vulnerabilidad. Se trata de aprovechar todo el potencial de las API para automatizar aún más los informes.

También hemos identificado a ciertos *hunters* que son especialmente competentes en nuestro programa público, otros con los que tenemos excelentes relaciones o que tienen habilidades muy específicas. Tenemos previsto invitar a estos expertos a programas dedicados a productos específicos. Es probable que lo hagamos este año.

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 decenas de miles de 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

OVHcloud