YES WE H/CK

OVHcloud

OVHCLOUD

Programme de Bug Bounty Public

ÉTUDE DE CAS

POURQUOI AVEZ-VOUS DÉCIDÉ DE LANCER UN BUG BOUNTY ?

JULIEN LEVRARD, RESPONSABLE CONFORMITÉ & SÉCURITÉ, OVHCLOUD :

Historiquement, la sécurité fait partie de l'ADN d'OVHcloud. Elle est inhérente à notre métier de fournisseur d'infrastructures, sur l'ensemble des services que nous proposons. Le haut niveau de sécurité de nos infrastructures doit être une exigence constante, et pour nos clients un moteur de confiance. Il repose sur des mesures de protection physiques et logiques et des activités de contrôle, scans, tests d'intrusion interne et externes, revues de code, de configuration, etc. Certaines de ces mesures sont assurées en continu par nos équipes, d'autres reposent sur une collaboration avec des tiers de confiance.

Nous avons lancé un programme de bug bounty avec YesWeHack il y a plusieurs années pour ajouter une couche de sécurité à nos systèmes déjà en place. Nous retrouvons des valeurs communes entre nos entreprises, évoluons dans le même écosystème, et partageons la même passion et le même ancrage européen. C'est en partie pour ces raisons que nous avons débuté avec cette plateforme - nous avons été l'un des premiers clients en programme public chez YesWeHack, et avons lancé notre programme lors d'un Live Bug Bounty à la Nuit du Hack.

LE BUG BOUNTY RENFORCE-T-IL LA CONFIANCE ACCORDÉE PAR VOS CLIENTS ?

JULIEN LEVRARD, RESPONSABLE CONFORMITÉ & SÉCURITÉ, OVHCLOUD :

Clairement, oui. OVHcloud travaille avec différentes typologies de clients. Certains opèrent eux-mêmes leurs infrastructures, et sont très sensibles à une communication technique. Notre communication repose ainsi sur la transparence et la rigueur de l'information. D'autres clients sont eux davantage vigilants quant à notre capacité à faire intervenir des tiers de confiance, comme des auditeurs de certifications ou des prestataires externes. Le bug bounty est donc un élément de confiance supplémentaire pour certains de nos clients, qui exigent plus que les moyens conventionnels de sécurité.

YesWeHack travaille avec des grandes entreprises françaises sensibles et « souveraines » telles que des OIV, et nous nous positionnons nous-même sur ce marché. Faire du bug bounty avec YesWeHack est un des éléments de cet écosystème de confiance et devient un « must have » pour des organisations telles que la nôtre. Et c'est aussi une question d'image vis-à-vis de la communauté des chercheurs, qui est partie prenante de cet écosystème : à travers YesWeHack, nous pouvons interagir avec des personnes qui ne sont pas forcément accessibles par d'autres canaux.

> **Le bug bounty nous met en relation avec des experts possédant des expertises complémentaires à celles de nos équipes, sur toute la diversité des technologies que nous exploitons.**

QU'EST-CE QUE VOUS APPORTE LE BUG BOUNTY PAR RAPPORT AUX DISPOSITIFS CITÉS PLUS TÔT (AUDITS, SCANS, TESTS D'INTRUSION, ETC.) ?

JULIEN LEVRARD, RESPONSABLE CONFORMITÉ & SÉCURITÉ, OVHCLOUD :

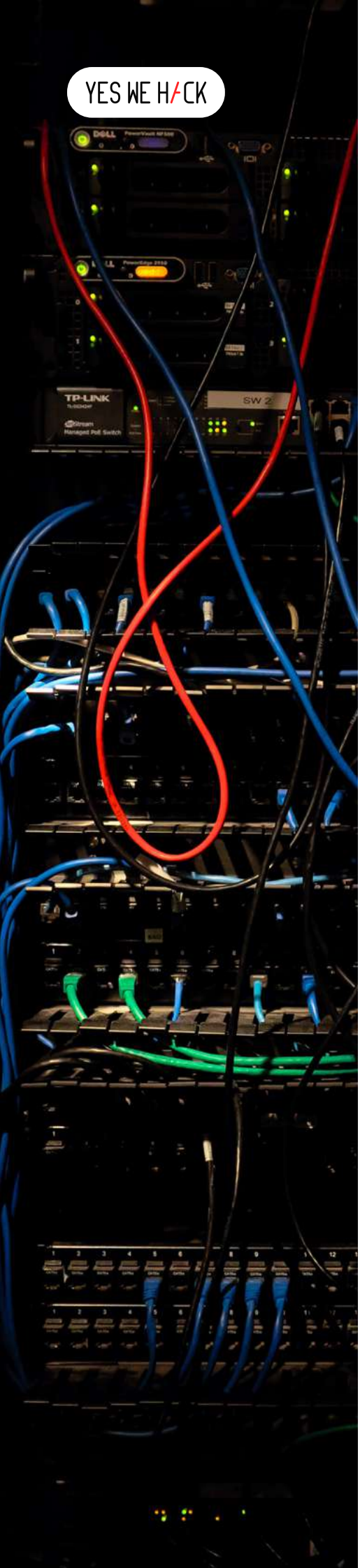
Le bug bounty nous met en relation avec des experts possédant des expertises complémentaires à celles de nos équipes, sur toute la diversité des technologies que nous exploitons. Cela inclut OpenStack, Kubernetes, des outils de Machine Learning, d'IA, etc. Il est impossible de trouver une équipe de pentesteurs disposant de compétences avancées sur l'intégralité de ces technologies.

YesWeHack nous donne facilement accès à des experts de ces différentes technologies qui se disent : « *Je suis un expert de Kubernetes, je vais donc regarder tous les programmes de bug bounty sur lesquels il y a des offres Kubernetes pour creuser le sujet.* » Cela complète donc efficacement notre démarche sécurité en apportant un regard complémentaire à celui de nos équipes.

Un autre point très important, c'est que le bug bounty apporte un cadre formel pour les remontées de vulnérabilités, et nous permet de fournir un point d'entrée juridiquement sécurisé aux hunters. Même si ce n'est pas le seul canal pour remonter des vulnérabilités chez OVHcloud, nous recommandons aux personnes qui « trouvent » des vulnérabilités de passer par notre programme. Cela nous permet d'avoir un flux entrant unique et un processus associé pour la gestion des remontées de vulnérabilités. C'est donc un élément structurant de notre CVD (Coordinated Vulnerability Disclosure).

Enfin, au-delà des avantages du bug bounty comme modèle, je souhaiterais mettre en avant la plateforme YesWeHack qui est très pratique, avec une interface utilisateur fluide et agréable. L'équipe OVHcloud qui gère le programme de bug bounty me fait d'excellents retours sur la gestion du workflow ainsi que sur le traitement des rapports et des interactions avec les chercheurs.

Les API permettent d'intégrer toutes les informations utiles à nos propres outils et tableaux de bord, de façon automatisée, et également de suivre notre budget primes et l'activité de chaque programme. D'un coup d'œil, nous pouvons connaître l'état de nos programmes, et présentons des indicateurs à notre management : le bug bounty s'intègre totalement à notre stratégie et au pilotage de notre sécurité globale.



OVHcloud

COMMENT LE BUG BOUNTY S'INTÈGRE DANS VOTRE DÉMARCHE AGILE ?

JULIEN LEVRARD, RESPONSABLE CONFORMITÉ & SÉCURITÉ, OVHCLOUD :

C'est notre équipe de pentesteurs qui pilote notre bug bounty : deux managers sont en charge du programme ainsi que de l'animation de la communauté des hunters. Ils font ensuite le lien avec les différentes équipes concernées par les vulnérabilités, afin qu'on les intègre dans nos systèmes de gestion et qu'on s'assure de leur correction.

Une fois que les vulnérabilités sont remontées à travers la plateforme, on les intègre dans nos processus : nous avons toute une mécanique organisationnelle que l'on appelle système de management de la sécurité, dans le cadre de la certification ISO 27001. Cela inclut des processus, des rôles et des responsabilités qui sont documentés et permettent de s'assurer que chaque vulnérabilité, incident ou menace potentielle est traité et suivi dans la durée par nos équipes, et fait l'objet d'un plan d'action précis, dont l'application est vérifiée (selon la sensibilité du produit concerné, et du niveau d'exigence associé). Grâce à l'API YesWeHack, nous avons facilement intégré les rapports de bug bounty à ce process : tout est géré par des tickets, consultables dans nos tableaux de bord, et accessibles par nos auditeurs externes au besoin.

> **Nous sommes dans une relation où l'on discute ouvertement des constats, sur la manière d'analyser une vulnérabilité. On a des échanges ultra productifs qu'on ne peut avoir par aucun autre moyen.**

VOUS ÊTES EN PROGRAMME PUBLIC, COMMENT SE PASSENT LES ÉCHANGES AVEC LA COMMUNAUTÉ ?

JULIEN LEVRARD, RESPONSABLE CONFORMITÉ & SÉCURITÉ, OVHCLOUD :

Gérer un programme de bug bounty, c'est un véritable engagement envers l'ensemble des parties prenantes investies pour un internet plus sûr. Nous avons donc la responsabilité de nous montrer rigoureux et transparents dans le traitement et la résolution des vulnérabilités qui nous sont remontées. Ce qui facilite les choses, c'est que la plateforme cadre et facilite à la fois les relations entre clients et chercheurs, avec des échanges très riches et très directs. Nous sommes dans une relation où l'on discute ouvertement des constats, sur la manière d'analyser une vulnérabilité. On a des échanges ultra productifs qu'on ne peut avoir par aucun autre moyen.

LES PROCHAINES ÉTAPES ?

JULIEN LEVRARD, RESPONSABLE CONFORMITÉ & SÉCURITÉ, OVHCLOUD :

On travaille sur les tickets générés par les rapports de vulnérabilités pour les intégrer de façon standard à notre modèle de gestion globale des risques. L'objectif est de pouvoir uniformiser notre gestion des risques quelle que soit la source d'information – incident avéré ou remontée de vulnérabilités. Il s'agit donc d'exploiter toutes les possibilités de l'API pour automatiser encore un peu plus le traitement des rapports.

Nous avons aussi identifié certains chercheurs particulièrement performants sur notre programme public, avec qui on entretient d'excellentes relations ou qui ont des compétences bien précises, pour les inviter sur des programmes dédiés à des produits spécifiques. Cela se fera sans doute cette année.

À PROPOS DE

YES WE HACK

Créée en 2015, YesWeHack est une plateforme mondiale de Bug Bounty et de VDP.

Notre plateforme connecte des dizaines de milliers d'experts en cybersécurité (« hackers éthiques ») répartis dans 170 pays avec des organisations de toutes tailles et de tous secteurs pour sécuriser leurs périmètres exposés et rechercher les vulnérabilités (bugs) de leurs sites web, applications mobiles, infrastructures et objets connectés.

YesWeHack gère des programmes privés (seulement accessibles sur invitation) et des programmes publics pour des centaines d'organisations à travers le monde, en conformité avec les réglementations européennes les plus strictes.

En plus de sa plateforme de Bug Bounty, YesWeHack offre également : un soutien à la création d'une politique de divulgation des vulnérabilités (VDP), une plateforme d'apprentissage pour les hackers éthiques appelée Dojo et une plateforme de formation pour les institutions éducatives, YesWeHackEDU.

⟶ CONTACTEZ-NOUS

⟶ CONSULTEZ NOTRE SITE

OVHcloud