YES WE HACK

yousign

YOUSIGN

Programme de Bug Bounty Privé

ÉTUDE DE CAS

POURQUOI AVEZ-VOUS OPTÉ POUR LE BUG BOUNTY ?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN :

Il existe un certain nombre de plateformes, notamment américaines. Nous voulions certaines garanties sur les hunters participant à nos programmes, et il nous a semblé que YesWeHack apportait ces garanties et la confiance nécessaire pour lancer un programme de bug bounty.

QUELLES SONT LES VALEURS AJOUTÉES DU BUG BOUNTY FACE AUX SOLUTIONS TRADITIONNELLES DE CYBERSÉCURITÉ, COMME LES PENTESTS ?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN :

La diversité des points de vue et des compétences. Chaque hunter a sa propre approche, sa façon de faire, qui rend chaque attaque si unique. Cela change du pentest et permet d'aller beaucoup plus loin. Avec le bug bounty, on a un peu quitté le monde classique du pentest, pour se retrouver avec 10, 20 ou 30 points de vue différents, qui vont réellement « challenger » nos équipes et nos services.

Ce qui est intéressant, c'est que les hunters ne sont pas forcément tous « professionnels de la cybersécurité ». Tout l'écosystème est représenté sur la plateforme, et nous pouvons sélectionner les profils selon leur nationalité, leurs compétences et leur classement sur la plateforme.

Cependant, la plus grosse valeur ajoutée du bug bounty, c'est la continuité, la récurrence, l'« annualisation » des tests : dès qu'on met en production une nouvelle version, on l'intègre au programme en cours et on obtient un retour immédiat sur la sécurité de cette évolution. On n'a plus besoin d'attendre le prochain pentest, un an plus tard, pour connaître la sécurité de notre mise à jour. La démarche est intégrée au cycle de vie des projets.

La production évolue tous les jours, les bugs évoluent en même temps. Les failles n'apparaissent pas une fois par an mais bien tous les jours, et le bug bounty nous permet de les détecter à temps. C'est une sorte de contrôle permanent de nos services, et c'est très rassurant pour tout le monde. D'un point de vue budgétaire, il serait également impossible de faire un test d'intrusion à chaque livraison alors que cela serait nécessaire.

Et puis il y a le ROI : Yousign conduit un pentest par an. C'est un budget quand même conséquent, par rapport à un programme de bug bounty. C'est assez incroyable, quand on y pense : on est sur des montants quasiment identiques, mais le bug bounty couvre une année alors qu'un audit dure une semaine seulement.

yousign

LE BUG BOUNTY SIGNE-T-IL LA MORT DU PENTEST ? OU LES DEUX APPROCHES RESTENT COMPLÉMENTAIRES ?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN :

Pour Yousign, les deux restent complémentaires. Ça peut signifier la mort du pentest dans certains contextes, mais pas dans le nôtre : en tant qu'acteur de confiance, nous sommes contraints à des audits réglementaires réguliers. Dans un contexte réglementaire moins contraignant, je me poserais sans doute la question de ne faire que du bug bounty.

Le bug bounty reste toutefois un argument de poids d'un point de vue marketing et commercial : c'est clairement un élément différentiant vis-à-vis de nos grands comptes. On le mentionne systématiquement dans nos réponses aux appels d'offres, puisque c'est perçu par le marché comme un gage de qualité.

QUELLES DIFFÉRENCES ENTRE LES RÉSULTATS D'UN PENTEST VS CEUX DU BUG BOUNTY ?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN :

J'ai eu quelques remontées communes, mais on a clairement eu beaucoup plus de remontées via le bug bounty que par le pentest. Et après avoir réalisé un pentest sur un périmètre donné, le bug bounty remonte toujours des vulnérabilités supplémentaires.

Un des problèmes du pentest, c'est que les résultats dépendent surtout de l'expertise du pentesteur. Notre dernier pentest a apporté des choses pertinentes, mais quand on compare ses résultats avec ceux du programme de bug bounty qu'on a lancé par la suite, ce n'est pas comparable.

> **« Après avoir réalisé un pentest sur un périmètre donné, le bug bounty remonte toujours des vulnérabilités supplémentaires.**

AVEZ-VOUS OBSERVÉ DES CHANGEMENTS PARMI VOS ÉQUIPES DEPUIS QUE VOUS ÊTES EN BUG BOUNTY ?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN :

Tout à fait. Au début, je gérais seul les programmes, puis j'ai assez rapidement mobilisé les équipes devs afin qu'ils répondent aux hunters et corrigent les bugs. La majorité des rapports concernait la partie applicative, c'est donc eux qui ont pris le sujet en main et se sont confrontés à la réalité, si j'ose dire.

De plus, leurs interactions avec les hunters ont rapidement eu un impact positif sur leur façon de livrer et de travailler : non seulement ils intègrent mieux la sécurité dans leur développement, mais ils « pensent » autrement, en gardant l'aspect sécurité en tête. D'une certaine façon, ils ne livrent pas seulement pour les clients, mais aussi pour les hunters !

LA PROCHAINE ÉTAPE ?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN :

La prochaine étape, c'est d'utiliser encore plus le bug bounty. Outre les programmes actuels sur nos environnements de production et de « staging », nous souhaitons automatiser la création de programmes dans notre workflow d'intégration et de livraison continue (CI/CD) afin de compléter notre panoplie de tests tant unitaires que fonctionnels. Cela nous permettra d'être encore plus agiles, et d'inclure complètement le bug bounty dans notre démarche de développement et d'intégration continue.

Et puis à terme, nous passerons peut-être à un programme public.

À PROPOS DE

YES WE HACK

Créé en 2015, YesWeHack est la première plateforme de Bug Bounty et de VDP en Europe.

Notre plateforme connecte plus de 25 000 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

yousign