yousign

ÉTUDE DE CAS

PROGRAMME PRIVÉ BUG BOUNTY

LEADER EUROPÉEN DE LA SIGNATURE ÉLECTRONIQUE

Novembre 2019

YES WE HACK

YOUSIGN

Qu'est-ce qui vous a décidé à vous lancer dans cette solution encore nouvelle et disruptive qu'est le Bug Bounty ?

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 selon vous les valeurs ajoutées du Bug Bounty aux solutions traditionnelles de cybersécurité (pentest) ?

La diversité des points de vue et des compétences. Chaque hunter à 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, leur classement, etc.
Mais 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.

CONTINUIÉTÉ

ARGUMENT DE VENTE

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 de 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...**

Le Bug Bounty, c'est la fin du Pentest ? Ou ça reste complémentaire ?

Pour Yousign, ça reste complémentaire. 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 fort d'un point de vue marketing et commercial pour nous, en tant qu'acteur de confiance : c'est clairement un argument de poids vis-à-vis de nos moyens et grands comptes. On le mentionne systématiquement dans nos réponses aux appels d'offres. Aujourd'hui c'est vu par le marché comme un gage de qualité.

YOUSIGN

Quelles différences entre les résultants du Pentest VS Bug Bounty ?

J'ai eu des 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 la réelle 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.

Avez-vous pu observer des changements sur vos équipes depuis que vous êtes en Bug Bounty ?

Clairement. Au début, je gérais seul les programmes, puis j'ai assez rapidement mobilisé les équipes devs afin qu'ils répondent aux hunters, corrigent les bugs, etc.
La majorité des rapports concernaient la partie applicative, c'est donc eux qui ont pris le sujet en main : ils se sont confrontés à la réalité, si j'ose dire. **Et leurs interactions avec les hunters a 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, gardant l'aspect sécurité en tête. **D'une certaine façon, ils ne livrent pas seulement pour les clients, mais aussi pour les hunters (rires).**

MONTÉE EN COMPÉTENCES DES ÉQUIPES

La prochaine étape ?

La prochaine étape c'est d'utiliser encore plus le Bug Bounty. En plus des 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 agile, et d'inclure complètement le Bug Bounty dans notre démarche de développement et d'intégration continue. Et puis à terme, peut-être passerons-nous à un programme public.

Kevin Dubourg
Bug Bounty Program Manager

yousign