LEADER EUROPÉEN ASSURANCE

Programme de Bug Bounty privé

ÉTUDE DE CAS

POUVEZ-VOUS VOUS PRÉSENTER RAPIDEMENT ?

Je suis le RSSI Groupe d'un des premiers groupes d'assurance européens. Mon équipe souhaitait notamment mettre en place un « bouclier cyber » vis à vis du groupe et de l'ensemble de ses filiales, en proposant différents services sécurité à nos filiales et notament le Bug Bounty.

QU'EST-CE QUI VOUS A DÉCIDÉ À LANCER UN PROGRAMME DE BUG BOUNTY ?

J'ai découvert ce modèle en discutant avec plusieurs RSSI de grandes institutions françaises. La recommandation d'institutions financières majeures aussi exigeantes en termes de sécurité a évidemment compté dans ma décision. On a d'abord fait quelques essais qui se sont avérés concluants et avons progressivement ouvert plusieurs programmes de Bug Bounty. C'est une approche différente et il est nécessaire de s'y accoutumer.

YES WE H/CK

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

D'abord l'assurance d'une surveillance en continu, et pas seulement ponctuelle, comme c'est le cas avec les tests d'intrusion classiques.

Si je fais un pentest de deux semaines chaque année, cela implique que nous restons « sans protection » pendant les 50 autres semaines, ce qui n'est plus concevable aujourd'hui.

À ce titre, les tests automatisés peuvent être aussi très utiles, mais moins pointus.

Maintenant, avec le Bug Bounty, j'ai des chercheurs qui travaillent en permanence sur mes périmètres.

Cette continuité des tests est primordiale, surtout lorsqu'on a des livraisons fréquentes dans un contexte de développement de plus en plus agile.

Le Bug Bounty nous permet aussi d'être plus flexible : je peux faire tester des environnements encore en développement, en phase de recette, avant la mise en production, selon le rythme de chaque projet. Ce qui est difficile à faire dans le cadre de pentests habituels.

La plateforme YesWeHack nous permet d'ajuster nos règles de chaque programme, et notamment la grille de primes, selon la phase du projet.

Je parlerais également de réactivité et disponibilité. Il est de plus en plus difficile, voire parfois impossible de trouver de bons pentesteurs au moment où l'on a le plus besoin d'eux, c'est-à-dire lorsqu'on fait une nouvelle mise en production.

> **« Avec le Bug Bounty, on appuie sur un bouton et ça démarre, on peut lancer des tests à tout moment, et obtenir la confirmation de remédiation très rapidement.**

Avec le Bug Bounty, on appuie sur un bouton et ça démarre, on peut lancer des tests à tout moment, et obtenir la confirmation de remédiation très rapidement.

Enfin, une valeur ajoutée supplémentaire réside dans la variété des vulnérabilités remontées.

On voit des scénarios plus intéressants, ou par exemple des chercheurs ont trouvé des « bouts » de vulnérabilités dont la combinaison rendait possible des attaques inédites. Ce sont des vulnérabilités que l'on ne traitait pas jusque-là, qui ne nous étaient pas remontées et que l'on a pu corriger en profondeur.

Avec le Bug Bounty, on se met vraiment dans la tête d'un hacker plus que dans la vulnérabilité froide trouvée d'un résultat d'audit.

LE BUG BOUNTY SIGNE-T-IL LA MORT DU PENTEST, OU EST-CE COMPLÉMENTAIRE ?

Pour moi, c'est complémentaire. Mais la réalité est qu'au vu du nombre de tests que l'on doit réaliser, la disponibilité des cabinets d'audits n'est pas suffisante...

D'où le caractère indispensable du Bug Bounty. De plus, les audits de pentest, outre les points mentionnés avant, présentent des limites : il faut les programmer à l'avance, prévoir une date de lancement et une date de fin, assurer la gestion de projet, etc.

Cette synchronisation est un vrai casse-tête, surtout avec des développements agiles. Si jamais une livraison a deux jours de retard sur un périmètre, les pentesteurs ne sont plus disponibles, ce qui pose un véritable problème d'intendance.

Ce que j'aime beaucoup aussi dans le Bug Bounty, c'est le contre-audit. Dans les audits traditionnels de pentest, il n'y a presque jamais de contre-audit. Suite à un pentest, un développeur de mon équipe peut me dire « j'ai corrigé le bug », mais je n'ai généralement que sa promesse.

Le Bug Bounty me permet de déléguer ce contrôle au chercheur, qui est parfaitement objectif. Ça me permet de corriger une vulnérabilité et valider la correction dans la foulée, contrairement à un contre-audit traditionnel, que je devrais lancer une fois que toutes mes vulnérabilités ont été traitées.

Maintenant, lorsqu'une vulnérabilité grave ou critique est découverte, je sais qu'elle est corrigée rapidement, et que je vais pouvoir dormir tranquille. (Rires)

YES WE HACK

AVEZ-VOUS PU OBSERVER DES CHANGEMENTS DANS VOS ÉQUIPES DEPUIS QUE VOUS ÊTES EN PROGRAMME DE BUG BOUNTY ?

Il y a plus d'échanges, c'est sûr, mais le point majeur que j'observe, c'est l'accélération de la cadence de correction : nos développeurs corrigent beaucoup plus rapidement. Le fait de répondre aux chercheurs, de les rémunérer, de clôturer les rapports, etc. engage les développeurs à réagir rapidement et entraîne un raccourcissement très net des délais de correction.

ET EN TERMES D'AGILITÉ ?

Comme évoqué plus tôt, nous avons mis en place des programmes dédiés aux environnements de test, avant leur mise en production. On détecte et corrige donc les vulnérabilités de plus en plus en amont des projets, ce qui permet 1. de former nos développeurs « à la volée » et 2. d'accélérer nos livraisons – puisqu'il y a beaucoup moins de corrections à faire en phase de recette et en production.

Nous gagnons donc en réactivité, à la fois dans l'intérêt des développeurs et des métiers.

PROCHAINES ÉTAPES ?

La première étape a consisté à élargir progressivement les périmètres du groupe. Et sur ces périmètres, de passer progressivement de boîte noire à boîte grise.

La deuxième étape, dans laquelle nous nous trouvons actuellement, est de mettre à disposition le service à nos filiales, en leur proposant quelque chose de nouveau et d'avant-gardiste, leur permettant de renouveler leur vision de la cybersécurité et des audits.

À PROPOS DE

YES WE HACK

Créé en 2013, YesWeHack est la première plateforme de Bug Bounty et de VDP en Europe.

Notre plateforme connecte plus de 23 000 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 milliers 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