YES WE HACK

OUTSCALE

OUTSCALE

Programme de Bug Bounty Public

ÉTUDE DE CAS

POURQUOI AVEZ-VOUS DÉCIDÉ DE LANCER UN PROGRAMME DE BUG BOUNTY ?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE :

Nous sommes certifiés ISO 27001 depuis 2014 et sommes ainsi obligés de faire de la recherche de vulnérabilités via des pentests. Au début, les pentests étaient utiles, mais plus le temps passait, moins les résultats étaient intéressants. On a rapidement constaté que sur la durée limitée d'un audit (2 à 3 semaines), un pentesteur n'avait pas le temps de trouver des vulnérabilités élaborées. Au mieux, il avait des intuitions mais ensuite, il nous fallait travailler dessus.

Nous avons vu aussi que le bug bounty marchait bien aux Etats-Unis depuis quelques années, où de grands noms utilisaient cette approche.

Nous avons d'abord hésité entre le red team et le bug bounty, avec des chercheurs venant de différents horizons pour tester nos périmètres et découvrir de nouvelles vulnérabilités.

Si on s'était lancé dans le red team, nous aurions eu le même problème qu'avec le pentest classique, évoqué juste avant. Nous avons donc choisi de lancer un bug bounty, en nous disant que si les pentesteurs ne trouvaient plus rien, cela ne voulait pas dire qu'il n'y avait pas d'autres problèmes.

On a commencé avec un programme privé, avec une quinzaine de hunters, car nous n'étions pas « sûrs » de nos applications. De belles vulnérabilités ont été remontées. Nous avons progressivement élargi le nombre de hunters invités, avant de faire passer deux périmètres en public : notre service d'infrastructure, et notre portail client.

POUVEZ-VOUS NOUS DÉCRIRE L'ÉVOLUTION ET LE DÉROULEMENT DE VOTRE PROGRAMME ?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE :

Ça a été assez rapide – un an environ. Lors de notre passage en public, nous n'avons pas assisté à un pic brutal de vulnérabilités : on a commencé avec une grille de primes très raisonnable, que l'on a augmentée progressivement, pour relancer régulièrement l'activité des hunters sur notre programme, afin d'atteindre notre « vitesse de croisière » actuelle.

LA NOTION DE SOUVERAINETÉ A-T-ELLE PESÉ DANS VOTRE DÉCISION DE TRAVAILLER AVEC YESWEHACK ?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE :

Oui, clairement. Quand nous avons envisagé le bug bounty, nous visions en parallèle des qualifications ANSSI et HDS, et il nous a donc paru plus opportun de travailler avec un acteur français, nous apportant de solides garanties sur le traitement de nos données.

TRAVAILLER AVEC UNE PLATEFORME SOUVERAINE EST-IL AUSSI UN ATOUT POUR VOUS, DANS LA FAÇON DONT VOUS ABORDEZ VOTRE MARCHÉ ?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE :

Oui, le principe de souveraineté est très important pour nos clients français et européens, qui comptent des organismes publics, parapublics, ou encore des OIV, naturellement sensibles à ces questions de souveraineté et de maîtrise de leurs données, dans le cadre de la fourniture de services cloud. Nous adjoindre à une plateforme souveraine comme YesWeHack assure à nos clients que l'ensemble de la chaîne de traitement des vulnérabilités est pleinement maitrisé.

De manière plus large, le bug bounty est un avantage concurrentiel pour Outscale, tout simplement parce qu'il garantit une sécurité résolument active : là où nous faisions des pentests semestriels et des scans périodiques, nous recherchons désormais les vulnérabilités en continu. Et dès qu'un hunter remonte une vulnérabilité, on est capable de l'intégrer automatiquement dans notre cycle de correction. Nos clients sont rassurés de savoir que nous n'attendons pas les mises à jour des éditeurs pour corriger nos vulnérabilités. Par ailleurs, nous sommes aussi capables de détecter et corriger les vulnérabilités sur nos produits développés en interne.

SELON VOUS, QUELLES SONT LES VALEURS AJOUTÉES DU BUG BOUNTY ?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE :

D'abord, les hunters n'ont pas de contraintes temporelles, et peuvent prendre le temps nécessaire pour détecter des vulnérabilités très sophistiquées, développer un exploit, proposer une remédiation et rédiger un rapport détaillé. Alors qu'un pentest se traduit souvent par quelques scans et deux ou trois CVE, sans réelles preuves d'exploitation.

Ensuite, il y a aussi la diversité de la communauté : je peux échanger avec des hunters spécialisés en UI, d'autre en application services, etc. Chacun d'eux me rapporte des choses différentes, complexes, qu'un auditeur « généraliste » ne pourrait trouver. Parfois, je me dis qu'il faut être fou pour trouver des choses comme ça ! J'ai vraiment un panel d'expertises très riche à disposition. Ils trouvent des choses que personne d'autre ne trouverait. Et ils prennent le temps de les mettre en valeur.

> **« J'ai vraiment un panel d'expertises très riche à disposition. Ils trouvent des choses que personne d'autre ne trouverait.**

Il y aussi du bruit, beaucoup de gens s'essaient au bug bounty et ne sont pas pertinents dans leur approche. Cela permet à mes équipes de se familiariser, de discuter avec les chercheurs de différentes approches en matière de gestion des vulnérabilités. Il faut parfois expliquer que ce qu'ils ont trouvé n'est pas une vulnérabilité, mais une mauvaise utilisation qu'ils ont eue de leur côté.

Et enfin, il y a une proximité qui se crée avec certains hunters dans la durée. Si tel chercheur a trouvé de belles vulnérabilités, et qu'il veut tester des choses un peu plus complexes, on va lui mettre à disposition des ressources ou des accès spécifiques pour qu'il puisse faire des choses plus intéressantes. Cette approche collaborative, ce travail en profondeur sont impossibles à mettre en œuvre avec des pentesteurs qui sont toujours débordés et pris par leurs contraintes de livraison.

EST-CE QUE LE BUG BOUNTY SIGNE LA MORT DU PENTEST, OU LES DEUX APPROCHES RESTENT COMPLÉMENTAIRES ?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE :

De mon point de vue, ce sont deux approches totalement différentes : j'utilise le pentest pour sa valeur certifiante, de mise en conformité avec certains standards. Les audits me permettent de répondre aux clients exigeant ces certifications.

Le bug bounty répond à un besoin de sécurité plus opérationnel et permet de me focaliser sur toutes les choses que les pentests et les scans classiques ne me permettent pas de détecter.

AVEZ-VOUS VU PU OBSERVER DES CHANGEMENTS AU SEIN DE VOS ÉQUIPES DEPUIS QUE VOUS ÊTES EN BUG BOUNTY ?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE :

Le responsable du SOC s'occupe de la gestion des programmes en cours, des primes, des relations avec les hunters, de la création de nouveaux programmes et des évolutions des périmètres. Les rapports de bug bounty arrivent à mon équipe SOC (Security Operations Center) qui qualifie chaque vulnérabilité.

Dans 90 % des cas, ce sont des vulnérabilités qui ne sont pas critiques et rapidement qualifiées. S'il y a un doute, nous en discutons en interne. Si la vulnérabilité est particulièrement intéressante, je la présente à l'équipe et on discute ensemble de son impact potentiel, des solutions à prévoir, des recommandations du hunter et de la façon de s'assurer qu'elle ne réapparaisse pas. Ces échanges font monter en compétence l'ensemble de l'équipe.

> **“ Le bug bounty répond à un besoin de sécurité plus opérationnel et permet de me focaliser sur toutes les choses que les pentests et les scans classiques ne me permettent pas de détecter.**

EST-CE QUE CELA PRODUIT ÉGALEMENT UN RAPPROCHEMENT ENTRE VOS ÉQUIPES ?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE :

Oui, car ça stimule la curiosité, les gens sont intéressés et veulent comprendre, c'est plutôt une bonne chose. C'est toujours plus concret de montrer une vraie vulnérabilité qui a vraiment eu lieu sur la plateforme.

ET EN TERMES D'AGILITÉ ?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE :

Nous travaillons en intégration continue, et le bug bounty s'est naturellement intégré à nos méthodes agiles.

Lorsque nous recevons un rapport de vulnérabilité, nous qualifions le score CVSS, et selon ce score nous fixons le délai de remédiation. Ensuite, le rapport est directement transmis aux équipes concernées pour correction. Il en va de même pour les dépendances utilisées dans le code ; elles sont transmises à la R&D pour analyse et montée de version. Dans tous les cas, le bug bounty est un point d'entrée comme un autre, et à ce titre les vulnérabilités sont gérées au travers de tickets.

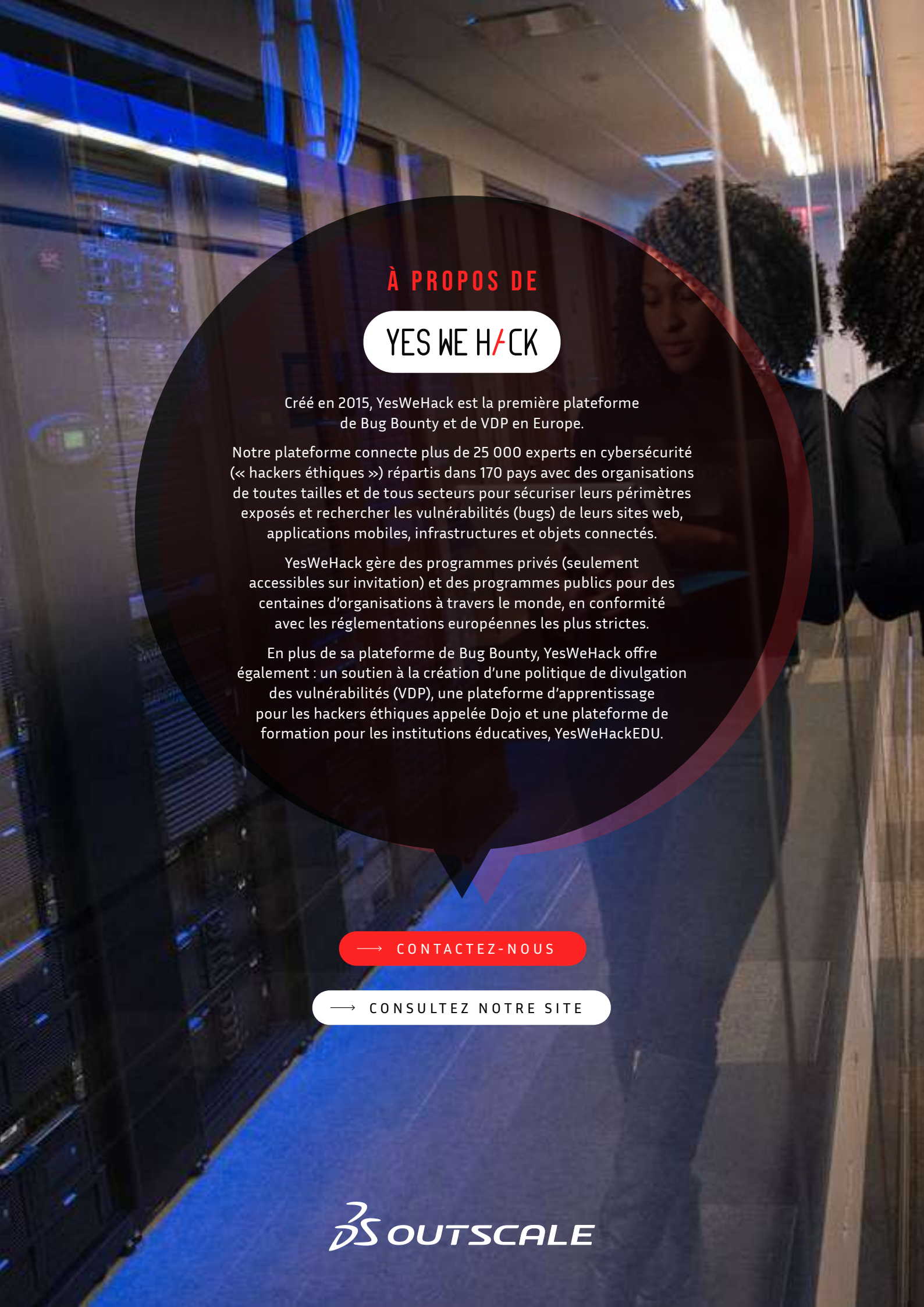
Nous ajustons le traitement selon l'urgence : si une correction rapide est nécessaire, nous livrons un correctif immédiatement, qui sera réintégré à la prochaine version. Dans ce cas, nous créons (ou modifions) une user story en incluant ces nouveaux éléments, qui serviront de base pour les développements.

QUELLE EST LA PROCHAINE ÉTAPE ?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE :

On va essayer d'élargir nos périmètres dans les programmes. Et pour encourager les hunters à « entrer » dans notre produit en profondeur (au-delà du frontal web) nous allons monter la grille de primes.

J'aimerais aussi leur donner des accès à nos plateformes privées pour pouvoir faire des tests un peu plus costauds. Nous avons déjà essayé une fois, et cela a donné des résultats très intéressants, avec des scénarios d'extraction des données en dur sur nos plateformes de tests. Cela nécessite cependant de fournir des périmètres de tests spécifiques aux hunters, ce qui prend du temps.



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

3DS OUTSCALE