YES WE H/CK

GROUPE ADP

GROUPE ADP

Programme de Bug Bounty Public

ÉTUDE DE CAS

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

DANIEL DIEZ, RESPONSABLE DU PÔLE DIGITAL FACTORY DU DOMAINE SI DIGITAL, GROUPE ADP :

L'équipe RSSI du Groupe ADP est à l'initiative de ce projet. Pour ma part, je n'avais pas de connaissance préalable sur le bug bounty, mais j'ai très rapidement vu l'intérêt et la force de cette solution. Je n'ai pas eu de doute ni d'appréhension particulière et aujourd'hui, je n'y vois que des bénéfices. Les vulnérabilités que les chercheurs nous remontent ne sont pas cachées : ce sont des vulnérabilités que nos cabinets d'audit et nous-mêmes ne voyons pas forcément et qui sont donc potentiellement exploitables par des personnes malveillantes.

ERIC VAUTIER, RSSI, GROUPE ADP :

En matière de cybersécurité, tout est question d'anticipation : il faut conserver un coup d'avance sur les hackers. Cela implique de considérer avec attention les innovations du marché et dans le domaine du Web, si on fait de la protection à l'ancienne, alors on est forcément en retard. Un bon moyen pour combler ce retard est donc de travailler directement avec des chercheurs en sécurité qui emploient les méthodes des hackers.

DANIEL DIEZ, RESPONSABLE DU PÔLE DIGITAL FACTORY DU DOMAINE SI DIGITAL, GROUPE ADP :

Nous avons commencé à travailler sur le bug bounty en nous demandant si nous arriverions à l'adapter à notre mode de fonctionnement. Aujourd'hui, c'est devenu l'un des piliers dans notre stratégie de sécurité web.

Bien entendu, il faut faire attention dans la définition des règles du programme : bien cadrer les tests pour que les chercheurs ne se dispersent pas. Trouver les bonnes limites et le descriptif du programme sont, à ce titre, très importants. On a commencé avec un périmètre restreint, qu'on élargit depuis, au fur et à mesure.

"Un bon moyen pour combler ce retard est donc de travailler directement avec des chercheurs en sécurité qui emploient les méthodes des hackers.

QUELLES SONT LES VALEURS AJOUTÉES DU BUG BOUNTY FACE AUX SOLUTIONS TRADITIONNELLES DE CYBERSÉCURITÉ (PENTEST) ?

DANIEL DIEZ, RESPONSABLE DU PÔLE DIGITAL FACTORY DU DOMAINE SI DIGITAL, GROUPE ADP :

Le test en continu. C'est le point fort du bug bounty. Le pentest, on le fait à un instant T – pas à chaque mise en production mineure. Alors qu'avec le bug bounty, les chercheurs travaillent en permanence, sont attentifs à chaque nouveauté et peuvent ainsi détecter si les changements apportés créent des vulnérabilités.

ERIC VAUTIER, RSSI, GROUPE ADP :

Dans un monde idéal, nous devrions tester systématiquement toutes les mises à jour de notre site web. Cela reviendrait à faire un audit de pentest chaque semaine, voire plus... Le bug bounty permet justement cette vérification continue.

DANIEL DIEZ, RESPONSABLE DU PÔLE DIGITAL FACTORY DU DOMAINE SI DIGITAL, GROUPE ADP :

J'ai reçu des rapports que je n'avais jamais eus précédemment avec nos pentests – des rapports plus poussés, notamment sur la cinématique de navigation sur le site. Les auditeurs n'ont pas forcément cette orientation d'esprit et un pentest a une durée limitée, alors que les chercheurs prennent le temps nécessaire pour aller aussi loin que possible. Au fur et à mesure, ils deviennent de plus en plus familiers avec notre périmètre, ce qui leur permet de travailler en profondeur.

ERIC VAUTIER, RSSI, GROUPE ADP :

Le bug bounty permet de faire remonter des vulnérabilités applicatives, plus fonctionnelles, et pas seulement techniques : c'est là un point différentiant avec le pentest. L'angle est complètement différent – le pentest repose souvent sur des outils automatiques alors que le bug bounty les complémente avec une approche plus humaine.

DANIEL DIEZ, RESPONSABLE DU PÔLE DIGITAL FACTORY DU DOMAINE SI DIGITAL, GROUPE ADP :

Ce qui est intéressant, ce sont toutes les interactions avec les chercheurs. Ces derniers nous aident à comprendre les vulnérabilités qu'ils ont trouvées, et comment les corriger efficacement. Cette démarche permet de capitaliser sur l'expertise.

Le bug bounty demande un investissement et du temps : il faut être disponible pour comprendre ce que les chercheurs ont tenté de faire, pour échanger avec eux... Mais grâce à eux, nous nous posons de nouvelles questions : par exemple, comment un hacker ferait-il pour contourner nos mesures de protection ?

GROUPE ADP

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

DANIEL DIEZ, RESPONSABLE DU PÔLE DIGITAL FACTORY DU DOMAINE SI DIGITAL, GROUPE ADP :

L'un ne va pas sans l'autre : tout d'abord, on ne teste pas forcément les mêmes choses. Ensuite, on ne peut pas partir à l'aventure sans avoir un minimum de certitudes préalables.

Le bug bounty s'inscrit dans une suite logique de maturité où il faut capitaliser sur un socle minimum avant de lancer son programme. Cependant, aujourd'hui et sur le périmètre actuel, nous n'avons plus besoin de faire de tests d'intrusion car le bug bounty se suffit à lui-même. Quand on démarre, il faut simplement mettre la barre au bon niveau, et cela devient ensuite quelque chose de récurrent.

> **“ Cependant, aujourd'hui et sur le périmètre actuel, nous n'avons plus besoin de faire de tests d'intrusion car le bug bounty se suffit à lui-même.**

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

DANIEL DIEZ, RESPONSABLE DU PÔLE DIGITAL FACTORY DU DOMAINE SI DIGITAL, GROUPE ADP :

Comme tout le monde, nous avons des outils de gestion des sources, des builds, de suivi de nos projets et d'analyse des performances. Nous utilisons aussi ces outils pour référencer et tracer chaque nouveau rapport de vulnérabilité issu du programme de bug bounty, et nous vérifions à chaque sprint ce que nous pouvons embarquer, permettant ainsi un traitement au fil de l'eau.

POURQUOI ÊTES-VOUS PASSÉ EN MODE PUBLIC ? QU'EST-CE QUE CELA A CHANGÉ DANS VOTRE APPROCHE DU BUG BOUNTY ?

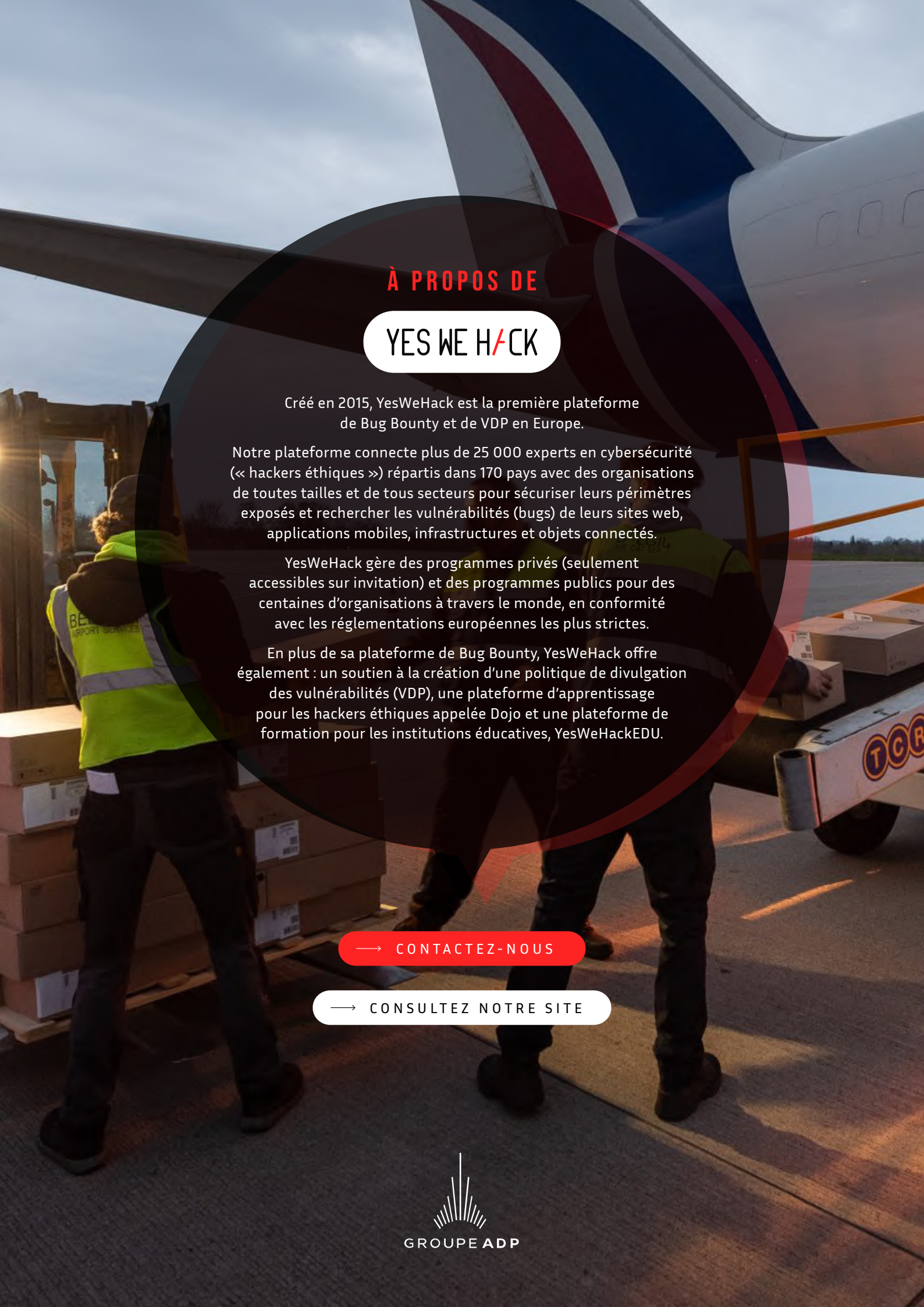
ERIC VAUTIER, RSSI, GROUPE ADP :

Le principal intérêt est de maximiser notre couverture du risque en démultipliant les tests potentiels. Ce faisant, nous disposons d'un canal unique de remontée des vulnérabilités de notre site web.

LA SUITE ?

ERIC VAUTIER, RSSI, GROUPE ADP :

Nous allons ouvrir de nouveaux périmètres, sur d'autres sujets, et auprès d'autres entités métiers, avec le même modèle : tests en mode privé d'abord, puis passage en mode 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

GROUPE ADP