YES WE HACK

ENSEIGNE DE LUXE INTERNATIONALE

Programme de Bug Bounty privé

ÉTUDE DE CAS

CONTEXTE

- Croissance rapide des revenus provenant du e-commerce
- Augmentation des cyberattaques au cours des neuf derniers mois

UNE ORGANISATION AGILE

- Cadre de travail agile
- Plateforme DevSecOps
- Une équipe Cyber SOC en 24/7

CHALLENGES

- Aligner la sécurité avec un développement agile et des mises en production bimensuelles
- Les audits, même lorsqu'ils durent un mois, ne sont jamais assez approfondis.
- Soumissions «anarchiques» de vulnérabilités par le biais de divers canaux.

SOLUTIONS

- Programme de Bug Bounty privé avec YesWeHack
- Déploiement d'une Vulnerability Disclosure Policy (VDP)

Notre client, une entreprise mondiale de produits de luxe, a été confronté à un défi commun à de nombreux RSSI dans le monde.

L'équipe sécurité était confrontée à une augmentation massive des cyberattaques (plus d'un million au cours des neuf derniers mois), principalement du fait de sa numérisation accélérée : plus d'un milliard de pages Web, une migration vers le cloud, l'ouverture des systèmes d'information et une utilisation croissante des API, le tout soutenu par un développement agile, avec des intégrations continues.

Cette transformation numérique exigeait une adaptation et évolution correspondante du volet sécuritaire. Notre client a pris conscience de la nécessité d'une approche moderne et efficace, mieux adaptée à ses nouveaux défis. Avec de nouvelles mises en production chaque quinzaine, ce nouveau modèle devait être agile, innovant et efficient.

L'heure était au changement et au progrès. Après avoir consulté différentes plateformes, cette enseigne de luxe de renommée mondiale a choisi YesWeHack pour l'aider à mettre en œuvre une stratégie de sécurité crowdsourcée et à lancer ses programmes de Bug Bounty.

Voici leur histoire : Comment ils ont défini et exécuter leur stratégie de sécurité crowdsourcée, comment ils ont fait évoluer leur programme, et ce qu'ils prévoient de mettre en place dans un avenir proche.

ÉTAPES ET PROGRESSION

1 DÉFINITION DES PROGRAMMES

Notre client a commencé par lancer deux programmes privés de Bug Bounty : l'un consacré à la Chine et à l'Asie-Pacifique, qui disposent d'infrastructures dédiées, et l'autre au « reste du monde ». Son périmètre comprenait une douzaine d'URL, principalement les sites e-commerce, et quelques API back-end.

En termes de budget et de récompenses, notre client a débuté avec un budget de récompenses de 15 000€ et des primes allant de 100 à 1000€.

« Contrairement à ce que les prestataires américains vous diront, il est possible de commencer un programme de Bug Bounty avec un petit budget. » RSSI adjoint, enseigne de luxe internationale.

⟶ CONSEIL DU CLIENT

Profitez de l'expertise et des conseils de YesWeHack pour déterminer votre périmètre et votre grille de récompenses.

2 CHOIX DES CHERCHEURS

Pour ses périmètres en Chine, notre client avait besoin de chercheurs locaux capables de lire le mandarin. Ces chercheurs devaient également connaître les pratiques de la région, en raison de la nature spécifique des applications, de l'approche particulière en matière de commerce et d'achat, et des outils différents de ceux utilisés en Europe et aux États-Unis.

YesWeHack a invité ? sélectionné pour le client une équipe de chercheurs qui correspondait à ces attentes.

⟶ CONSEIL DU CLIENT

Demandez à YesWeHack de vous aider à sélectionner votre première équipe de chercheurs.

3 LANCEMENT DES PROGRAMMES

Le premier rapport est arrivé dans les 30 minutes suivant l'ouverture du programme. Après seulement quatre heures, plus de huit rapports avaient été soumis, dont une vulnérabilité critique et deux vulnérabilités de gravité élevée.

⟶ CONSEIL DU CLIENT

1. *Ne lancez pas votre programme de Bug Bounty en début de soirée si vous voulez dormir la nuit !*

2. *Soyez un minimum réactif. Si vous voulez que les chercheurs s'impliquent et restent actifs sur votre programme, vous devez leur répondre rapidement. Notre objectif est que les rapports des chercheurs soient traités dans les trois jours.*

4 INTÉGRATION EN DOUCEUR

Pour s'assurer que les rapports de vulnérabilité soient partagés rapidement et de manière sécurisée entre les chercheurs et les équipes de développement, notre client utilise le connecteur JIRA fourni par YesWeHack. De cette façon, les tickets peuvent être envoyés directement aux équipes, facilitant ainsi la remédiation des vulnérabilités.

5 DEUX MOIS APRÈS LE LANCEMENT

Deux mois après le lancement du programme, environ 30 rapports avaient été soumis et 60% avaient été corrigés. Ce premier aperçu du modèle du Bug Bounty a permis à notre client de se rendre compte de l'ampleur des failles dans son infrastructure – notamment en Chine. ***« Nous avions réalisé de nombreux pentests sur notre infrastructure chinoise. Mais ils n'ont jamais remonté les vulnérabilités critiques comme celles mises en évidence par notre programme de Bug Bounty. »*** RSSI adjoint, enseigne de luxe internationale.

LA MONTÉE EN PUISSANCE

Une fois le modèle du Bug Bounty bien pris en main, l'équipe sécurité a décidé d'étendre son périmètre, d'augmenter les récompenses et d'inviter de nouveaux chercheurs.

Chez YesWeHack, nous conseillons toujours à nos clients de démarrer petit à petit et de procéder par étapes. Cette première phase est essentielle pour bien appréhender le fonctionnement du modèle, pour comprendre les chercheurs, leur raisonnement, leur manière de travailler, mais aussi pour apprendre à gérer les soumissions sans se laisser déborder.

LES PROCHAINES ÉTAPES

En tant que marque de luxe de renommée mondiale, notre client reçoit régulièrement des rapports « sauvages », par le biais de divers canaux de communication tels que le centre de service, les emails et les réseaux sociaux. Il est donc difficile de tout centraliser, de les transmettre aux bonnes personnes et de les traiter avec la rigueur nécessaire.

Pour gérer au mieux ces remontées, notre client a également mis en place une politique de divulgation des vulnérabilités (VDP) avec l'aide de YesWeHack. Cette VDP leur permet de :

- Centraliser les demandes, en s'assurant qu'elles sont transmises à la bonne entité en interne.
- Réduire le « bruit » (les soumissions non pertinentes) : en effet, les soumissions doivent être rédigées par les chercheurs à travers un formulaire en ligne dédié et détaillé.
- Standardiser le format des rapports reçus via la VDP et le programme de Bug Bounty – en rationalisant/simplifiant les processus internes et en permettant une automatisation à l'échelle.

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 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