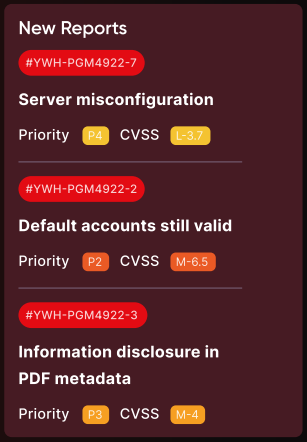
YesWeHack

POLITIQUE DE DIVULGATION DE VULNÉRABILITÉS

Un canal sécurisé et simplifié pour signaler les vulnérabilités qui ont un impact sur votre organisation



PERMETTEZ AUX CHERCHEURS DE SIGNALER LES VULNÉRABILITÉS QU'ILS DÉCOUVRENT

Les surfaces d'attaque ne cessent de croître et les organisations doivent permettre aux chercheurs de bonne foi de les informer des vulnérabilités potentielles qu'ils peuvent découvrir dans leurs actifs numériques. Il incombe aux équipes cyber de fournir un dispositif sûr et simple pour faciliter ce processus.

YesWeHack offre un cadre technique et juridique, clair et sécurisé pour recevoir les vulnérabilités potentielles de vos actifs en ligne, vous permettant de prendre rapidement les mesures appropriées.

Une politique de divulgation de vulnérabilités, ou VDP, est préconisée par des organismes de réglementation tels que le NIST, l'ENISA et la CISA, et prescrite par les normes ISO 29147 et ISO 30111.

IDENTIFIEZ VOS VULNÉRABILITÉS AVANT LES CYBERCRIMINELS

AFFICHEZ VOTRE ENGAGEMENT EN MATIÈRE DE SÉCURITÉ

FACILITEZ LA COMMUNICATION ET ÉLIMINEZ LE « BRUIT »

FONCTIONNALITÉS DU PRODUIT

- FORMULAIRE DE SOUMISSION PERSONNALISÉ
- CANAL CHIFFRÉ DE BOUT EN BOUT
- SERVICE DE TRIAGE EXPERT
- GESTION UNIFIÉE DES VULNÉRABILITÉS

VDP VS. BUG BOUNTY

	POLITIQUE DE DIVULGATION DE VULNÉRABILITÉS (VDP)	PROGRAMME DE BUG BOUNTY
QUOI ?	C'est un dispositif sécurisé, public et passif permettant à quiconque de signaler légalement les vulnérabilités découvertes de façon fortuite au sein des actifs d'une organisation.	C'est une invitation proactive adressée à des hackers éthiques afin qu'ils testent des actifs numériques spécifiques, avec des récompenses financières pour des vulnérabilités pré-définies.
POURQUOI ?	Pour permettre aux chercheurs de bonne foi de signaler les vulnérabilités potentielles sur tout actif numérique exposé de l'organisation, avant que des acteurs malveillants ne les découvrent.	Pour augmenter les capacités de test de sécurité et couvrir plus d'actifs, plus rapidement et de manière plus exhaustive qu'avec d'autres méthodes de tests.
COMMENT ?	En fournissant des instructions claires pour signaler de manière responsable les vulnérabilités, et un canal sécurisé pour transmettre tous les détails pertinents.	En détaillant les règles du programme, les actifs présents ou exclus du périmètre, les vulnérabilités admissibles, une grille de récompenses et toutes les exigences utiles en matière de tests autorisés.
QUI ?	Tout le monde – des professionnels de la cybersécurité qui signalent des vulnérabilités techniques, aux simples utilisateurs qui remarquent que des informations sensibles sont visibles sur une page web publique.	Uniquement des chercheurs inscrits et vérifiés. Les programmes privés sont destinés à des chasseurs sélectionnés et invités.
RÉCOMPENSES ?	Non. Il ne doit pas y avoir d'incitation ou d'attente de récompenses financières pour le signalement de vulnérabilités via une VDP.	Oui. La grille de récompenses est établie avant le lancement et est clairement communiquée aux chasseurs dans les détails du programme.

« LA MISE EN PLACE D'UNE POLITIQUE DE DIVULGATION DES VULNÉRABILITÉS NOUS A FOURNI UN CANAL DE COMMUNICATION CRUCIAL ET TRÈS EFFICACE AVEC LE MONDE EXTÉRIEUR. »

Ingénieur En Cybersécurité, Leader Européen De La Vente Au Détail d'Électronique Grand Public

« Notre VDP est principalement utilisée pour l'image de marque : avec cet outil en place, nous montrons que la sécurité est considérée comme une priorité par l'entreprise. »

RSSI Adjoint, Groupe Français De Luxe

« Nous constatons un intérêt croissant de la part de nos clients envers les dispositifs que nous déployons. Désormais, ils s'interrogent sur la mise en place éventuelle d'une Politique de Divulgation de Vulnérabilités (VDP) ou d'un programme de Bug Bounty au sein de notre entreprise. »

Jean Yves Le Breton, Product Security Manager

YesWeHack se conforme à des exigences strictes en matière de sécurité, de traçabilité financière et de respect de la vie privée. Les services de YesWeHack sont certifiés ISO 27001, ISO 27017 et accrédités CREST. L'infrastructure de YesWeHack s'appuie sur un hébergement privé basé en UE, conforme au RGPD et répondant aux normes les plus strictes : ISO 27001, ISO 27017, ISO 27018, ISO 27701 et SOC II Type 2. La plateforme YesWeHack est également soumise en permanence à un programme public de Bug Bounty.