PRODUCT SHEET

UBIKA VIRTUAL PATCHING

Évitez les correctifs de panique. Bénéficiez des solutions efficaces de patching virtuel d'UBIKA et des capacités de test des experts de YesWeHack.

La prolifération des applications et des mots de passe correspondants constitue un défi pour les services informatiques des entreprises. Il leur est devenu difficile de protéger les données de l'entreprise et de répondre aux demandes de réinitialisation des mots de passe. Il est indispensable d'identifier les utilisateurs, mais il n'est pas pratique pour eux de se souvenir d'un trop grand nombre de mots de passe. Les utilisateurs passent trop de temps à se connecter à des applications individuelles. Les correctifs virtuels réduisent considérablement le temps pendant lequel les données sensibles sont exposées à des attaques potentielles et aident les équipes informatiques à réagir rapidement et efficacement aux failles de sécurité.

Les technologies UBIKA WAAP et la plateforme de bug bounty de YesWeHack se complètent parfaitement car le client peut nous envoyer une demande de correctif basée sur le rapport de vulnérabilité du chasseur de sécurité.

360 fois plus rapide pour corriger une vulnérabilité avant la mise en production

Avec les méthodes traditionnelles, il faut en moyenne 30 jours (43 200 minutes) pour corriger une vulnérabilité. Grâce à nos capacités de correction virtuelle, vous pouvez créer une règle personnalisée, la tester et la déployer en production en environ 2 heures (120 minutes).

Comment cela fonctionne-t-il ?

1. Nous analysons la vulnérabilité
Lorsqu'ils sont informés du rapport du chasseur, nos experts en sécurité accèdent au ticket et analysent la vulnérabilité.

2. Création d'un correctif virtuel
Si notre produit n'est pas équipé pour protéger, l'expert crée un patch virtuel avec un minimum de faux positifs et de faux négatifs.

3. Test et mise en œuvre du correctif
Une fois que le correctif est prêt, il est appliqué à notre produit. Le client importe le fichier de correctifs virtuels. Une fois activée, l'attaque est bloquée.

Le patching virtuel d'UBIKA

Pour les attaques majeures (comme l'injection de commande, l'injection SQL, le cross-site scripting, le path traversal, etc.) nous avons des moteurs de sécurité standards et avancés intégrés dans UBIKA WAAP Gateway (sur site), UBIKA WAAP Cloud (version cloud public d'UBIKA WAAP Gateway), UBIKA Cloud Protector une véritable version SaaS WAAP. Pour les vulnérabilités restantes, nous analysons la menace et fournissons un correctif virtuel. Notre patch virtuel est basé sur une nouvelle alternative au pen testing - « on demand crowd testing » - grâce à une plateforme et une communauté de chercheurs vérifiés de YesWeHack, vous permettant d'élever l'efficacité, l'agilité et le ROI de vos audits de sécurité.

Vos avantages en un coup d'œil
Les correctifs virtuels réduisent l'impact global du risque sur l'entreprise. Les avantages sont les suivants :

- Des performances plus rapides grâce à la neutralisation des menaces de sécurité.
- Sécurité renforcée pour vos applications web grâce à une protection instantanée.
- Finies les pertes de revenus et de productivité dues à l'indisponibilité des applications.

YesWeHack #1 plateforme européenne de bug bounty

YesWeHack est une plateforme mondiale de Bug Bounty et de VDP. YesWeHack offre aux entreprises une approche innovante de la cybersécurité grâce au Bug Bounty (paiement par vulnérabilité découverte). Elle met en relation plus de 25 000 experts en cybersécurité (hackers éthiques) à travers 170 pays avec des organisations pour sécuriser leurs périmètres exposés et signaler les vulnérabilités de leurs sites web, applications mobiles, infrastructures et appareils connectés.

Vos avantages en un coup d'œil

- Ne payez que pour les résultats et optimisez votre budget de sécurité.
- Renforcer la transparence et améliorer la responsabilité au sein des équipes.
- Réduire les frais généraux et utiliser efficacement les ressources.
- Faciliter les affaires en favorisant l'agilité et en améliorant les délais de mise sur le marché.
- Vérifiez la réalité avec les programmes publics de primes aux bugs.

Patch virtuel d'UBIKA

- Instaurez la confiance grâce à des tests à la demande.
- Accédez facilement à des experts dans diverses technologies, ce qui permet de diversifier la base de connaissances en matière de tests.
- Renforcez votre posture de cybersécurité avec des correctifs virtuels en utilisant UBIKA WAAP Gateway, UBIKA WAAP Cloud ou UBIKA Cloud Protector.
- Réduire le coût, le temps et l'effort de sécurisation des applications.