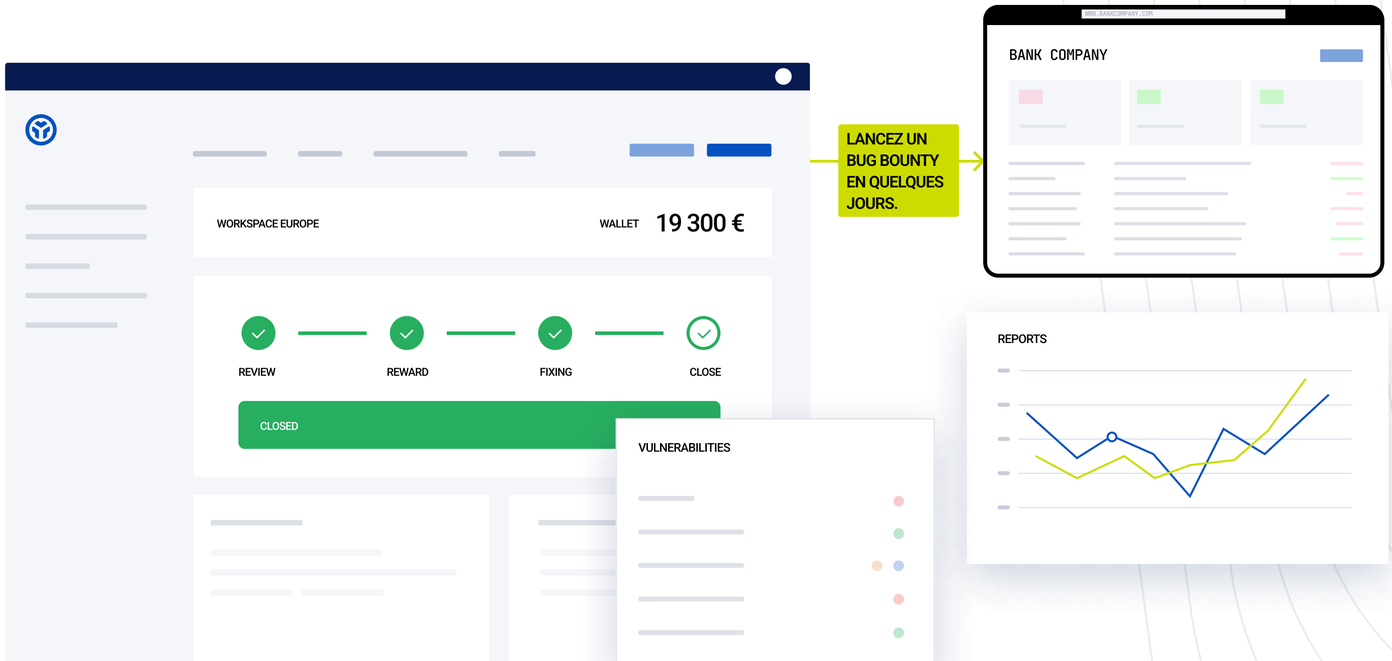
Bug Bounty privé

UN TEST DE SÉCURITÉ OFFENSIF ET CONTINU PAR UNE COMMUNAUTÉ DE CHERCHEURS EN SÉCURITÉ CHEVRONNÉS.

Évaluez la sécurité de vos actifs en continu et identifiez **les vulnérabilités critiques restées dans l'ombre.** Récompensez, corrigez et re-testez avec agilité avant qu'elles ne soient exploitées.

- **Accédez à une communauté privée de plus de 800 chercheurs en sécurité, spécialisés dans différents types d'actifs.**
- **Rémunérez uniquement les vulnérabilités approuvées.**
- **Assurez la découverte continue des vulnérabilités critiques, recevez des rapports incluant les preuves de concept (POC) et des conseils de remédiation, et communiquez directement avec les experts en sécurité.**

Notre plateforme de Sécurité Offensive permet une gestion des vulnérabilités simplifiée de bout en bout et un accès à des services taillés pour vos besoins.



La Yogosha Strike Force

800+ CHERCHEURS EN SÉCURITÉ. TRIÉS SUR LE VOLET ET HAUTEMENT QUALIFIÉS

Yogosha sélectionne uniquement les chercheurs les plus talentueux. Seuls 20% des candidats sont acceptés, après avoir réussi un examen technique et pédagogique. Leur identité et leurs antécédents sont également vérifiés.

- **Spécialisés dans la recherche des vulnérabilités les plus critiques en simulant les attaques sophistiquées des pirates informatiques.**
- **Experts dans de multiples types d'actifs**

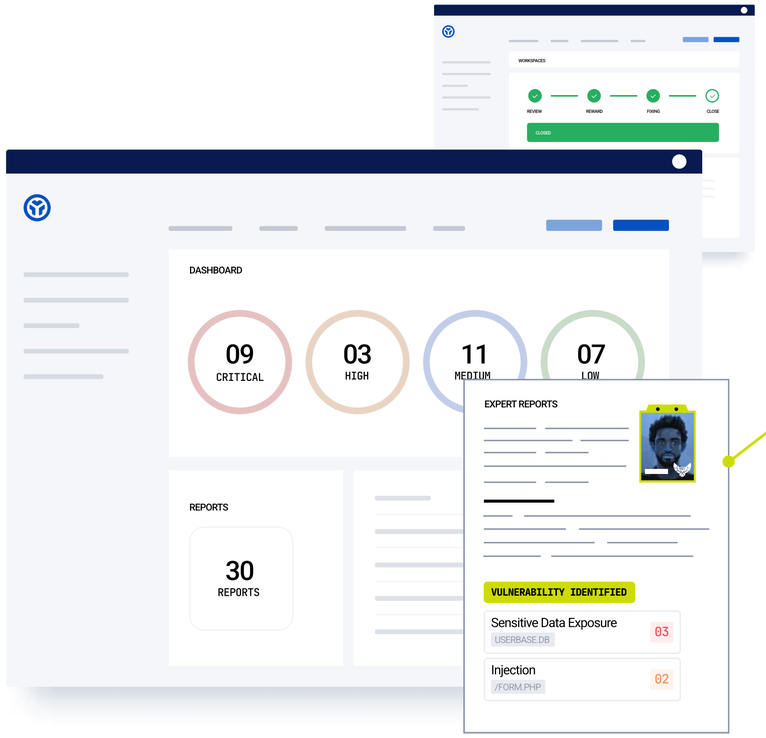
  `Web` `Applications Mobiles` `IOT` `Cloud` `Réseaux` `APIs` `Infrastructure`
- **Détiennent des certifications telles que**

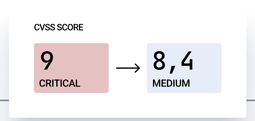
  `OSCP` `OSEP` `OSWE` `OSEE` `GXPN` `GCPN` `eWPTXv2` `PNPT` `CISSP`

Avant que les acteurs malveillants ne le fassent

IDENTIFIEZ LES VULNÉRABILITÉS CRITIQUES QUE VOUS IGNOREZ ENCORE

Les chercheurs en sécurité examinent vos actifs manuellement en utilisant toute une série d'outils, de tactiques et de procédures pour déceler les vulnérabilités critiques. Les vulnérabilités découvertes sont documentées avec leur score CVSS, des preuves de concept (POC) et des conseils de remédiation, et signalées en direct sur une plateforme centralisée de gestion des vulnérabilités, le VOC™.





Votre succès, notre priorité

DES CONSEILS D'EXPERTS POUR DE MEILLEURS RÉSULTATS

Notre équipe dédiée vous accompagne tout au long de votre parcours de sécurité offensive avec des conseils éclairés pour des résultats optimaux – des premières consultations aux réunions d'étape avec des recommandations ad hoc pour une bonne gestion du programme et une remédiation accélérée.

Rémunérez uniquement les vulnérabilités validées

UN SYSTÈME DE RÉCOMPENSE CLAIR POUR LES CHERCHEURS EN SÉCURITÉ

Approvisionnez et contrôlez facilement votre cagnotte, et déclenchez les paiements en toute simplicité lorsqu'une vulnérabilité est acceptée. Tirez parti des options de paiement et de recharge automatiques pour poursuivre le programme sans effort.

Menez la danse

CONTRÔLEZ LES OPÉRATIONS GRÂCE À DES DONNÉES EN TEMPS RÉEL

La plateforme Yogosha permet de centraliser tous les programmes de bug bounty et les rapports de vulnérabilité.

Des données en temps réel comme les types de vulnérabilités et les scores de sévérité permettent d'avoir une vision claire de l'exposition aux risques de vos actifs. Le système de “workspace" permet de comprendre et comparer le profil de risque de votre organisation à travers plusieurs entités et départements.

Des workflows efficients pour des bug bounty efficaces

LE DÉROULEMENT DU BUG BOUNTY PAR YOGOSHA

Les bug bounty courent sur vos actifs sans discontinuer. Afin de vous garantir les meilleurs résultats possibles, nos experts en cybersécurité et notre équipe Customer Success vous accompagnent tout au long de votre parcours de Sécurité Offensive.

01 Réunion de lancement

VOUS PRÉPARER AU SUCCÈS

- Définition du périmètre du Bug Bounty
- Onboarding et formation sur la plateforme
- Mise en place de réunions d'étape

02 Tests offensifs

DÉTECTEZ LES VULNÉRABILITÉS CRITIQUES

Un groupe présélectionné d'une trentaine de chercheurs au moins signale les vulnérabilités en direct sur la plateforme.

03 Traitement

TRIAGE

Validez en quelques clics les rapports de vulnérabilité ou sollicitez nos services de triage.

04 Paiement au résultat

RÉCOMPENSEZ LE CHERCHEUR EN SÉCURITÉ

Rémunérez le chercheur en toute simplicité selon la criticité de la vulnérabilité.

05 Remédiation

CORRIGEZ LES VULNÉRABILITÉS

Tirez parti des rapports détaillés et des preuves de concept, et communiquez directement avec les experts en sécurité.

06 Vérification

TESTEZ LA ROBUSTESSE DES CORRECTIONS

Contactez directement nos chercheurs et demandez un test de contrôle de la remédiation que vous avez implémenté en un seul clic.

07 Activité du programme

STIMULEZ LES CHERCHEURS

Pour assurer la découverte continue de nouvelles vulnérabilités, recrutez davantage de chercheurs, élargissez votre périmètre de test ou augmentez les récompenses.

La gestion des vulnérabilités simplifiée et sécurisée

LE VOC™ VULNERABILITY OPERATIONS CENTER

La plateforme Yogosha vous permet de rationaliser vos tests de sécurité offensifs et de gérer vos vulnérabilités de bout en bout. Voici pourquoi :

- **Un lancement simple des tests de sécurité**
  Organisez un test en quelques clics.
- **Un accès direct à des experts en sécurité**
  Constituez votre équipe de chercheurs en vous appuyant sur notre communauté, la Yogosha Strike Force, ou sur la vôtre.
- **Un environnement de test contrôlé** ÉLÉMENT DIFFÉRENCIANT
  Tirez profit du VPN Yogosha et mettez les chercheurs sur liste blanche pour leur donner un accès exclusif à vos actifs. Mettez les tests en pause à tout moment.
- **Une plateforme robuste et sécurisée**
  Notre plateforme SaaS est hébergée chez 3DS Outscale, certifié SecNumCloud. Nous sécurisons continuellement nos actifs à travers un pipeline DevSecOps, les directives OWASP et un programme de bug bounty / VDP continu. Par ailleurs, la certification ISO 27001 est en cours.
- **Des options d'intégration flexibles**
  Utilisez notre API, nos webhooks et nos connecteurs pour vous connecter à vos outils de ticketing et de remédiation.
- **Une attribution facile des rôles**
  Attribuez des rôles et permissions, et distribuez les tickets de remédiation à votre équipe de sécurité/développement.
- **Une gestion des vulnérabilités rationalisée de bout en bout** ÉLÉMENT DIFFÉRENCIANT
  Gérez les vulnérabilités critiques avec précision selon différents statuts : de la détection au triage, en passant par les conseils de remédiation et les re-tests.
- **Des rapports de vulnérabilité détaillés**
  Les rapports incluent le nom du chercheur en sécurité, le score CVSS, la preuve de concept (POC) avec des images ou des vidéos et des conseils de remédiation.
- **Une communication directe avec les chercheurs en sécurité**
  Gardez le contact avec les experts en sécurité et informez-les des mises à jour de votre programme de tests de sécurité. Pour chaque rapport soumis, communiquez directement avec le chercheur pour lui poser des questions ou lui faire part de vos commentaires.
- **Une vision précise et en temps réel de votre exposition au risque**
  Contrôlez l'évolution de l'exposition au risque de tous vos actifs afin de savoir où et quand agir.
- **Une comparaison des profils de risque**
  Utilisez le système de “workspace" pour comprendre et comparer le profil de risque de votre organisation à travers plusieurs entités et départements.
- **De multiples solutions d'hébergement** ÉLÉMENT DIFFÉRENCIANT
  Choisissez notre modèle SaaS ou auto-hébergez la plateforme sur un cloud public/privé ou on-premise pour rester maître de vos données.

PRESENTATION

VOIR LA DEMO

Get Offensive

Bénéficiez des conseils d'un expert

Contactez nous à contact@yogosha.com

DEPUIS 2015

800+ chercheurs en sécurité chevronnés

Des tests de sécurité lancés **en quelques jours**

Une gestion des vulnérabilités rationalisée **de bout en bout**

PARIS • LONDRES • DUBAI

Avec la confiance de plus de 300 clients dans 12 pays

FINANCE & ASSURANCE

SECTEUR PUBLIC & INDUSTRIE

RETAIL & ECOMMERCE

EDITEURS & DIGITAL FACTORIES