

GitHub Advanced Security

De l'open source au DevOps, les entreprises recherchent de nouveaux moyens d'accélérer la livraison de logiciels, tout en s'appuyant sur les outils de sécurité traditionnels. GitHub Advanced Security aide les équipes à créer plus rapidement un code plus sûr grâce au moteur d'analyse de code sémantique le plus avancé au monde.

Une approche communautaire en matière de sécurité

Plus de 1 700 requêtes prêtes à l'emploi

Intégrez les meilleurs chercheurs en sécurité à votre équipe à l'aide de requêtes d'experts du secteur et de chercheurs de GitHub.

Partage des meilleures pratiques en matière de sécurité

Améliorez la sécurité à l'échelle de votre entreprise grâce à des requêtes codifiées, exécutables et partageables dont tout le monde peut apprendre et utiliser.

Sécurisez vos workflows depuis une branche jusqu'à la production



Exécutez des requêtes prêtes à l'emploi ou personnalisées

Des chercheurs en sécurité et des développeurs de requêtes de code utilisant un langage appelé CodeQL. Les équipes peuvent exécuter ces requêtes CodeQL personnalisées ou prêtes à l'emploi sur des bases de code afin de détecter des vulnérabilités de sécurité à grande échelle.



Examinez les alertes de sécurité avec des correctifs étape par étape

Lorsqu'une vulnérabilité est détectée, une alerte de sécurité apparaît directement dans la pull request du développeur, accompagnée d'une documentation étape par étape et des correctifs proposés par des experts en sécurité.



Trouvez et corrigez pour de bon les bugs de sécurité

Les requêtes QL mises à jour sont écrites et ajoutées à GitHub Advanced Security chaque fois qu'une nouvelle vulnérabilité de sécurité est identifiée. Ainsi, la même vulnérabilité ne peut se produire deux fois.



Améliorez et mettez à jour vos requêtes au fur et à mesure

Avec chaque déploiement, les développeurs internes et les équipes de sécurité peuvent continuer à modifier les requêtes pour les adapter à votre code, éviter les faux positifs et identifier de nouveaux problèmes de sécurité.

Des outils puissants pour protéger le code et les clients



Le code comme données

Traitez le code comme des données en identifiant les vulnérabilités dont vous êtes à la recherche, au lieu des correctifs que vous ne recherchez pas.



Une sécurité évolutive

Analysez rapidement le code et identifiez même les patterns sémantiques les plus complexes dans votre base de code.



Moins de faux positifs

Faites en sorte que les équipes de sécurité et de développement se concentrent sur les vulnérabilités qui comptent le plus pour votre entreprise.



Des requêtes orientées objet

Exécutez des requêtes sémantiques sur le contrôle personnalisé, l'analyse du data flow et le suivi des défauts en seulement quelques heures, et non pas en plusieurs semaines.



« Nous utilisons GitHub Advanced Security pour bâtir une expertise qui est ensuite partagée à l'échelle de l'entreprise, ce qui nous permet de travailler en équipe et de faire progresser notre produit tous ensemble »

Gregory Burns

Directeur du développement logiciel chez BlackLine

Sécurité de bout en bout :

Pour en savoir plus sur GitHub et la sécurité des logiciels, rendez-vous sur github.com/features/security

Besoin d'aide ?

Adressez-vous à notre équipe de vente :
sales@github.com
github.com/enterprise