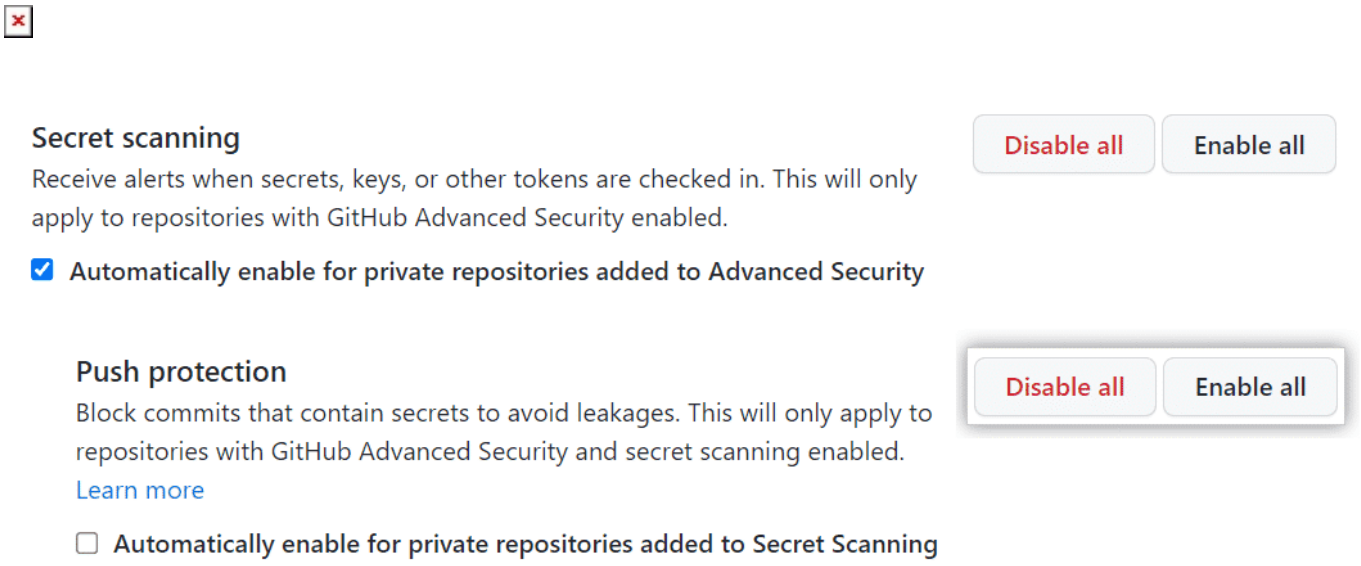
GitHub : « shift left » sur la détection automatique des secrets

Tendance « shift left » sur GitHub. La détection automatique des secrets peut désormais se faire au moment des *pushs*. Et non plus seulement par après.

Sur tous les dépôts publics, cette fonctionnalité est incluse. Pour l'utiliser sur des dépôts privés, il faut disposer de la licence Advanced Security. Celle-ci est disponible en complément à GitHub Enterprise Cloud et Enterprise Server (version 3.0 et ultérieures).



Socle de la démarche : un programme à destination des fournisseurs de services. Ces derniers peuvent transmettre à GitHub des patterns permettant de repérer les secrets qu'ils émettent.

Lorsque le système de détection pense avoir repéré un secret sur un dépôt public, il avertit l'émetteur. Qui peut ensuite décider de prendre contact avec l'utilisateur. La licence Advanced Security, en plus d'élargir le périmètre aux dépôts privés, allonge la liste des secrets pris en charge. Avec, par exemple, les jetons d'accès à GitLab, les clés API Grafana, les clés de licence New Relic ou les *tokens* des *bots* Telegram.

La détection au niveau des *pushs* gère pour le moment nettement moins de secrets que celle au niveau des dépôts. Manquent notamment à l'appel les *tokens* d'Adobe, de HashiCorp (Terraform et Vault), de Twilio ou encore une partie des secrets Azure (clés de comptes Azure Storage, certificats Azure Service Management…).

Il faut dire que cette analyse en amont est plus critique : par défaut, elle bloque la livraison du code problématique. Pour contourner ce blocage, trois solutions : marquer comme « à traiter plus tard », signaler qu'il s'agit d'un test ou déclarer un faux positif. La première option génère une alerte ouverte qui adresse régulièrement des notifications au contributeur et aux admins du dépôt concerné. Les deux autres engendrent une alerte (sans notifications) dans l'onglet « Sécurité » du dépôt.

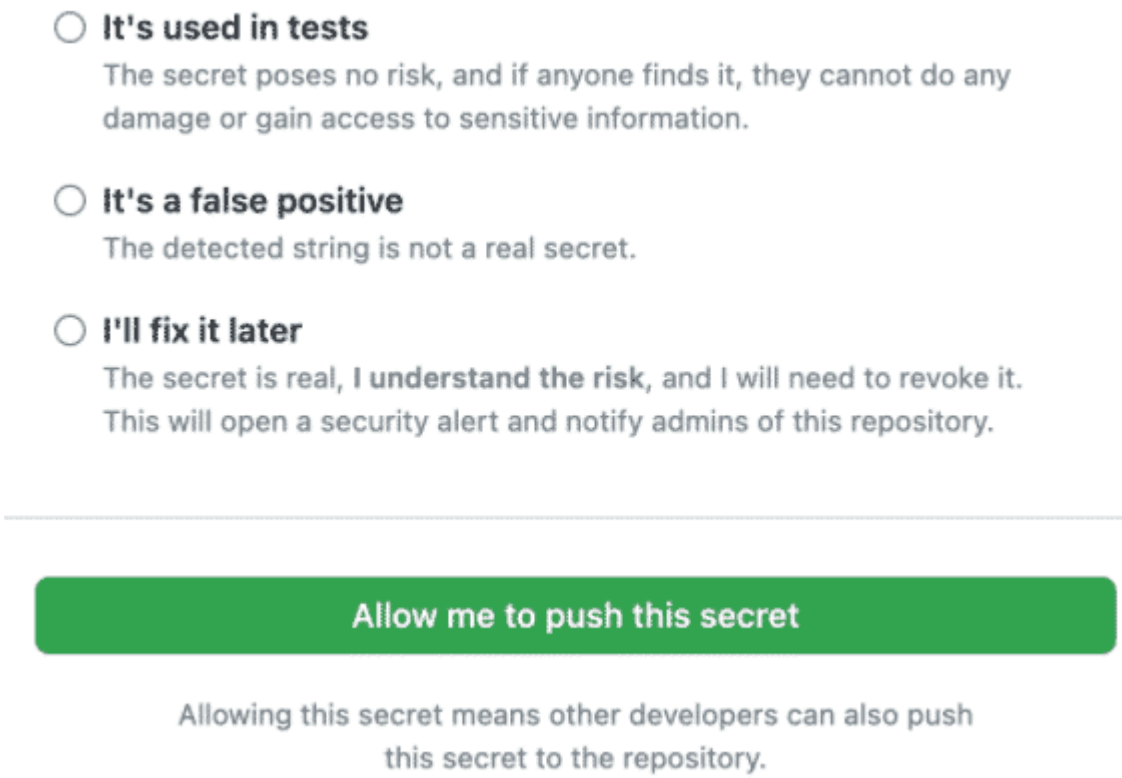


Illustration principale © bygermina – Shutterstock