

# 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 pushes](#). 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).



## Secret scanning

Receive alerts when secrets, keys, or other tokens are checked in. This will only apply to repositories with GitHub Advanced Security enabled.

Disable all

Enable all

Automatically enable for private repositories added to Advanced Security

## Push protection

Block commits that contain secrets to avoid leakages. This will only apply to repositories with GitHub Advanced Security and secret scanning enabled.

[Learn more](#)

Disable all

Enable all

Automatically enable for private repositories added to Secret Scanning

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 *pushes* 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.

**It's used in tests**

The secret poses no risk, and if anyone finds it, they cannot do any damage or gain access to sensitive information.

**It's a false positive**

The detected string is not a real secret.

**I'll fix it later**

The secret is real, I understand the risk, and I will need to revoke it. This will open a security alert and notify admins of this repository.

---

**Allow me to push this secret**

Allowing this secret means other developers can also push this secret to the repository.

*Illustration principale © bygermina – Shutterstock*