Politique de push & validation sécurité

Équipe Sécurité, AOUDIA Lilia, vérifié par LESTIENNE Jules

Version 1.0

1 Objectif

Ce document a pour but d'expliquer à **toutes les entités/équipes** la manière de pousser du code lorsqu'une **validation sécurité** est nécessaire. L'idée est de :

— laisser les développeurs pousser librement,
— être notifiés proprement,
— tracer ce qui a été audité,
— produire une documentation de sécurité à chaque validation.

Ce document complète le CR "Processus (axé sécurité)".

2 Principe général

1) Les développeurs peuvent **pusher normalement** sur leur dépôt/branche.
2) **Dès qu'un block de code est finit**, le commit doit être **signalé à la sécurité** (infra, authentification, chiffrement, réseau, droits, données, secrets...)
3) La sécurité **ne vérifie que la sécurité**, pas le fonctionnel.

3 Ce que doivent faire les autres entités

3.1 Au moment du push

1) Vous poussez normalement.
2) Le commit qui doit être contrôlé est **tagué** :
   — `<sécurité>` **obligatoire**,
   — obligatoirement, variante par pôle : `<sécurité>-<nom_du_pole>` pour qu'on s'y retrouve.

3.2 Ping obligatoire sur Discord

Après le push, l'équipe qui a poussé doit **obligatoirement** nous prévenir sur le channel dédié Discord en envoyant :

— l'**ID du commit** (hash),
— le **dépôt** concerné,
— un **contexte très court** (ex. : "ajout route API + token", "modif Docker + droits").

Important : *pas de ping = pas de démarrage du délai.* Le délai commence uniquement à partir du ping Discord.

3.3 Documentation obligatoire côté équipe

Pour **chaque** commit tagué `<sécurité>`, **l'équipe qui pousse doit produire sa propre documentation**, même courte. Sans cette doc, la sécurité ne garantit pas de comprendre le contexte ni de faire une analyse complète.

La documentation minimale doit contenir :

a) **Qu'est ce que le code fait** (lien avec les US, quel est le besoin ?, 2 à 5 lignes),

b) **Où est le code concerné** (fichiers/dossiers impactés),

c) **Comment le code fonctionne techniquement** (techno, algo, protocoles...),

d) **Les informations sensibles** (auth, droits, données, infra, secrets...).

Sans cette doc, la sécurité peut :
— demander des précisions (et donc rallonger le cycle dans les 72h),
— ou ne valider que **partiellement** en notant "contexte insuffisant" dans sa doc.

4 Ce que fait l'équipe Sécurité

4.1 Point de départ du délai

Le délai de traitement démarre **uniquement** quand :
a) le commit est tagué `<sécurité>`, **et**
b) nous avons reçu le **ping Discord avec l'ID du commit**, **et**
c) le lien/éléments de **doc de l'équipe** sont fournis.

4.2 Délai

L'équipe Sécurité dispose de **72 heures maximum** (3 jours) après le ping pour analyser et répondre.

4.3 Analyse de risque

La sécurité réalise une **analyse de risque** (format "fiche d'analyse de risque") comprenant au minimum :
— éléments modifiés,
— risques introduits,
— risques **acceptés** (si le temps manque),
— niveau de sécurité visé/atteint (critique, moyen, faible).
Si le niveau demandé est trop élevé par rapport au temps ou au contexte, la sécurité **diminue explicitement le niveau** et le **documente**.

4.4 Validation et re-tag

Une fois l'analyse faite, la sécurité :
1) **re-tag le commit** avec `<sécurité validée>`.
2) **pousse / dépose la documentation de sécurité** (analyse de risque, remarques, risques acceptés) dans l'espace prévu (repo doc, dossier sécu, etc.) afin d'assurer la traçabilité.

5 Traçabilité

Chaque commit passé en sécurité doit pouvoir être relié à :
a) son **ID de commit**,
b) le **ping Discord**,

c) la **doc de l'équipe** (fournie au moment du ping),
d) la **fiche d'analyse de risque** de la sécurité,
e) le **tag final** `<sécurité validée>`.

6 Cas particuliers

6.1 Manque de temps côté dev

Les équipes peuvent tout de même pusher. Dans ce cas :
— la sécurité documente les risques non traités,
— l'équipe pourra faire une seconde passe sécurité plus tard.

7 Récapitulatif

1. Je push.
2. Je tag le commit : `<sécurité>`.
3. **Je fais ma doc courte** (ce qui est fait, où, impact, partie sensible).
4. Je ping la sécu sur Discord avec l'ID du commit + **lien/éléments de doc**.
5. La sécu a **78h max** pour analyser.
6. La sécu fait une **analyse de risque** et documente.
7. La sécu re-tag : `<sécurité validée>` et pousse sa doc.