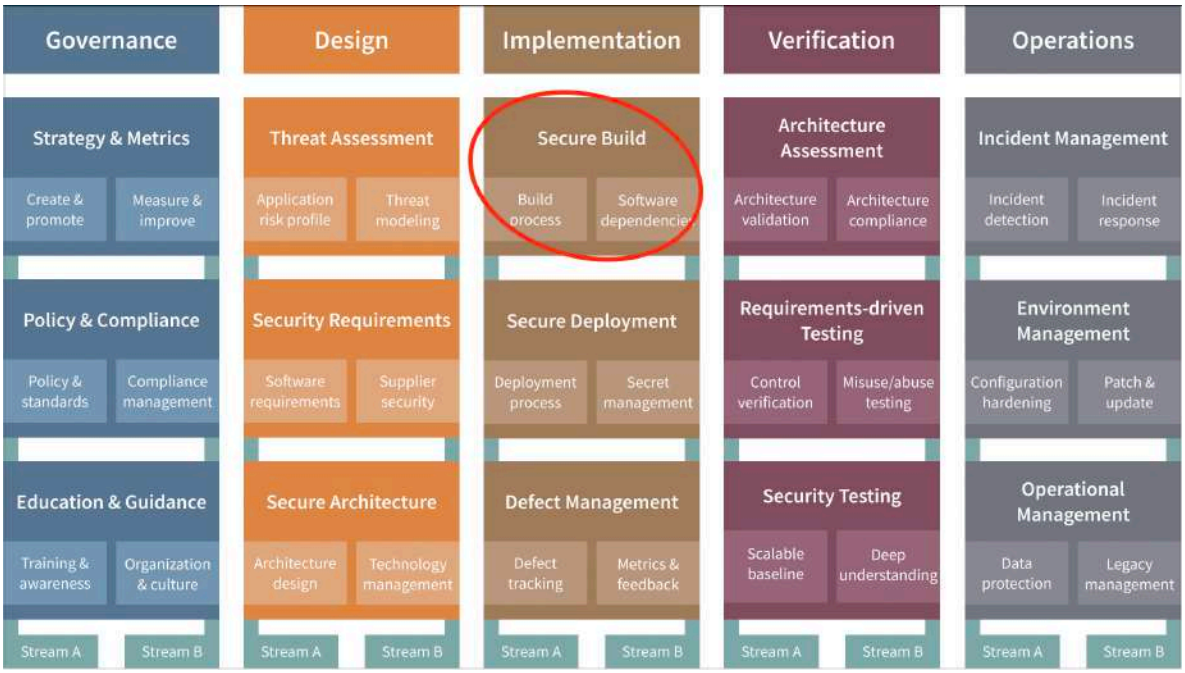
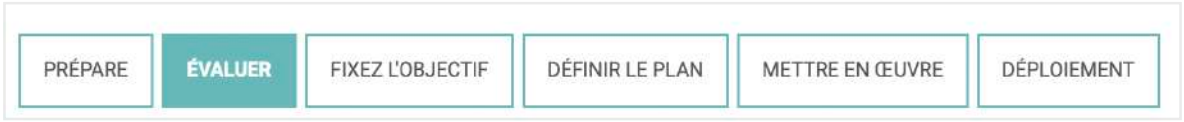
Owasp SAMM

Le framework Owasp SAMM identifie 5 fonctions dites métier. Chaque fonction contient 3 pratiques, elles-mêmes décomposées en 2 sous catégories appellées « volet ».

Sur les 15 pratiques, nous allons nous concentrer sur une seule histoire de préciser la démarche.



Mise en place



Structuration du questionnaire d'évaluation

Il expose **UNE question** par niveau de maturité pour un volet d'une pratique sécuritaire. Soit 1 x 3 X 2 X 15 = 90 questions

Implémentation > Construction sécurisée

La pratique « Secure Build » (SB) souligne l'importance de construire des logiciels de manière **standardisée et reproductible**, et de le faire en utilisant des composants sécurisés, y compris des dépendances logicielles tierces.

Niveau de maturité	Description	Processus de construction	Dépendances logicielles
1	Le processus de construction est reproductible et cohérent.	Créez une définition formelle du processus de construction afin qu'il devienne cohérent et reproductible.	Créez des notices avec la nomenclature de vos applications et analysez-les de manière opportuniste.
2	Le processus de construction est optimisé et entièrement intégré au flux de travail.	Automatisez votre pipeline de construction et sécurisez l'outillage utilisé. Ajoutez des contrôles de sécurité dans le pipeline de construction.	Évaluez les dépendances utilisées et assurez-vous d'une réaction rapide aux situations présentant un risque pour vos applications.
3	Le processus de construction aide à empêcher les défauts connus d'entrer dans l'environnement de production.	Définissez des contrôles de sécurité obligatoires dans le processus de construction et assurez-vous que les artefacts non conformes échouent.	Analysez les dépendances utilisées pour les problèmes de sécurité d'une manière comparable à votre propre code.

Aide à l'évaluation > Volet « Processus de construction »

Réponses possibles:

- Non => 0
- Oui quelques applications => 0,25
- Oui au moins la moitié des applications => 0,5
- Oui pour la plupart voire toutes les applications => 1

NIVEAU 1 - Votre processus de construction complet est-il formellement décrit ?

- *Vous avez suffisamment d'informations pour recréer les processus de construction*
- *Votre documentation de construction à jour*
- *Votre documentation de construction est stockée dans un emplacement accessible*
- *Les sommes de contrôle d'artefact produites sont créées lors de la construction pour prendre en charge une vérification ultérieure*
- *Vous durcissez les outils qui sont utilisés dans le processus de construction*

NIVEAU 2 - Le processus de construction est-il entièrement automatisé ?

- *Le processus de construction lui-même ne nécessite aucune interaction humaine*
- *Vos outils de construction sont renforcés conformément aux meilleures pratiques et aux conseils du fournisseur*
- *Vous cryptez les secrets requis par les outils de construction et contrôlez l'accès selon le principe du moindre privilège*

NIVEAU 3 - Appliquez-vous des contrôles de sécurité automatisés dans vos processus de génération ?

- *Les builds échouent si l'application ne respecte pas une ligne de base de sécurité prédéfinie*
- *Vous avez une gravité maximale acceptée pour les vulnérabilités*
- *Vous enregistrez les avertissements et les pannes dans un système centralisé*
- *Vous sélectionnez et configurez des outils pour évaluer chaque application par rapport à ses exigences de sécurité au moins une fois par an*

Calcule d’une note

Pour **chaque question**, on enregistre la note correspondant à la réponse. A la fin des 3 questions du volet, nous obtenons un score entre 0 et 3. Sachant que l’on a 2 volets dans une pratique, ce score pèsera pour moitié dans le score global de la pratique.
Exemple: si j’ai « 2 » sur le volet « Processus de construction » et 1 sur le volet « Dépendances logicielles », cela fera une note de 2/2 + 1/2, soit 1,5.

On reconduit ces questions sur toutes les pratiques pour obtenir un niveau de maturité sur chaque pratique

Challenger l’évaluation du volet « Processus de construction »

- Comment matérialiser / exprimer la **Stack de dev** ainsi que **le parc informatique** VM, poste enrollé « standardisé » ?
- Préciser le curseur de la réponse dite idéale. La réponse ne laisse transparaître qu’une notion de quantité, et non de qualité.

Exemple

NIVEAU 2 - Le processus de construction est-il entièrement automatisé ?

Oui en hors production mais une phase de recette est à réaliser à la main ainsi qu’une planification de mise en prod.

- Une maturité de 3 sur une pratique ne retranscrit pas la dimension qualitative du logiciel produit, elle traduit une certaine maturité « organisationnelle » dans la production logiciel.

Autrement dit, la dimension qualitative est absente du framework car elle est à part. L’identification des règles qualité (seuils de qualité, https de bout en bout, …) sont à challenger indépendamment d’owasp SAMM.

Exemple : Mes builds sont automatiques de mon commit à la production, et tout est tracé. Il est toujours possible que je pousse une vulnérabilité en production. Il s’agirait d’un défaut dans ma « gestion qualité logiciel ».

- Owasp SAMM expose des questions qui peuvent ne pas être applicables.

Exemple: La sécurité doit absolument valider tous les livrables manuellement et la barrière qualité est exclusivement manuelle (équipe dédiée).

Par conséquent, **il faut nuancer les scores à l’échelle de votre organisation**.

Avis

Selon moi, OWASP SAMM est un excellent point de départ pour appréhender la sécurité logiciel dans votre organisation. Ce cadre va de paire avec des chantiers de qualité logiciel.
Il convient de préciser que ce framework ne va pas vous apporter de clefs sur les règles qualitatives à mettre en place pour atteindre une maturité optimale.
D’autre part, un plafond de verre peut être présent dans une organisation et il me paraît intéressant de le faire apparaître afin de mieux mesurer les améliorations au cours des itérations.

OWAP SAMM va vous apporter sur votre organisation

1. Une vision global des pratiques à mettre en place pour implémenter de la sécurité
2. Des pratiques dites « idéales »
3. Une démarche d'amélioration continue

En revanche, il ne va pas vous apporter :

1. Des règles qualitatives à mettre en place
2. Une cartographie complète des activités liées de près ou de loin à la sécurité
3. Des outils ou des implémentations à favoriser (ex : outils self-hosted ou cloud pour le CI/CD)

🧠 En somme, OWASP SAMM permet uniquement de mettre en place des pratiques liées à la sécurité logicielle. En revanche, ce framework ne va pas vous apporter de solutions techniques, ni des indicateurs, des outils où des implémentations précises.