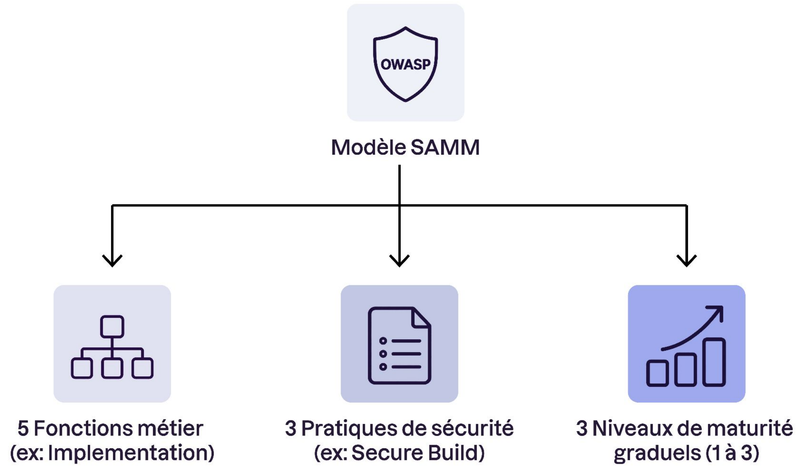
Fiche récap : Sécurisez votre chaîne de développement logiciel avec l'OWASP

Cybersécurité

1. Intégrer la sécurité à chaque phase du cycle de développement avec un S-SDLC
2. Évaluer la maturité AppSec avec OWASP SAMM et construire une feuille de route progressive
3. Définir des exigences de sécurité vérifiables et contractualisables avec OWASP ASVS
4. Orchestrer les contrôles DevSecOps et sécuriser les pipelines CI/CD
5. Pérenniser le programme AppSec par la formation, les Security Champions et l'amélioration continue



Bonnes pratiques

- ✅ Intégrer les principes Security-by-Design et Security-by-Default dès la conception
- ✅ Protéger les branches principales et imposer les revues de code avant fusion
- ✅ Automatiser les scans de secrets, SAST et SCA dans les pipelines CI/CD
- ✅ Générer un SBOM standardisé à chaque build pour tracer les composants logiciels
- ✅ Adapter les Security Gates à la criticité et au niveau d'assurance ASVS visé
- ✅ Centraliser et prioriser les vulnérabilités avec une approche ASPM
- ✅ Isoler les environnements de build et signer les artefacts pour garantir leur provenance
- ✅ Responsabiliser les développeurs et animer un réseau de Security Champions

Erreurs classiques

- ❌ Traiter la sécurité uniquement en fin de cycle de développement
- ❌ Inventer un framework de sécurité au lieu de s'appuyer sur des standards éprouvés
- ❌ Viser systématiquement le niveau maximal de maturité SAMM sans considérer les risques
- ❌ Se contenter de questionnaires déclaratifs pour évaluer la sécurité des fournisseurs
- ❌ Déployer des outils complexes avant de maîtriser les contrôles DevSecOps fondamentaux
- ❌ Désactiver les contrôles de sécurité CI/CD sous la pression des délais de livraison
- ❌ Mettre en production du code généré par IA sans validation et compréhension humaines
- ❌ Faire du Security Champion l'unique responsable de la sécurité de son équipe

Définitions

S-SDLC
cycle de développement intégrant exigences, analyses et contrôles de sécurité à chaque phase du logiciel.

OWASP SAMM
framework permettant d'évaluer la maturité AppSec et de construire une feuille de route d'amélioration.

OWASP ASVS
standard d'exigences de sécurité applicative précises et vérifiables selon plusieurs niveaux d'assurance.

OWASP WSTG
guide méthodologique décrivant comment tester concrètement la sécurité des applications web.

SBOM
nomenclature logicielle recensant les composants et dépendances intégrés dans un logiciel.

ASPM
approche centralisant et contextualisant les données de sécurité pour prioriser les vulnérabilités critiques.

Security Gate
critère de sécurité automatisé pouvant bloquer une fusion ou un déploiement lorsqu'un risque interdit est détecté.