OPENSAMM

Sources :

Qu'est-ce que l'OpenSAMM ?	https://owaspsamm.org/guidance/quick-start-guide/ https://www.opensamm.org https://owaspsamm.org/about/
Les 5 fonctions commerciales	https://drive.google.com/file/d/1cI3Qzfrly_X89z7StLWI5p_Jfqs0-OZv/view?pli=1
Comment évaluer le niveau de maturité en termes de sécurité logicielle ?	https://owaspsamm.org/about/
Premier document	https://docs.google.com/spreadsheets/d/1jmLVltRhuG19AX5cLUcWH1Qox2Uic17rD29gMVG5zDE/view#gid=1716553355
Deuxième document	https://www.aymericlagier.com/2017/09/27/cybersecurite-opensamm-modele-de-maturite-developpement-dapplications-securisees/
Troisième document	https://docs.google.com/spreadsheets/d/1jmLVltRhuG19AX5cLUcWH1Qox2Uic17rD29gMVG5zDE/view#gid=1716553355
Comment mettre en place OpenSAMM ?	https://www.aymericlagier.com/2017/09/27/cybersecurite-opensamm-modele-de-maturite-developpement-dapplications-securisees/ https://owaspsamm.org/guidance/quick-start-guide/

1) Qu'est-ce que l'OpenSAMM ?

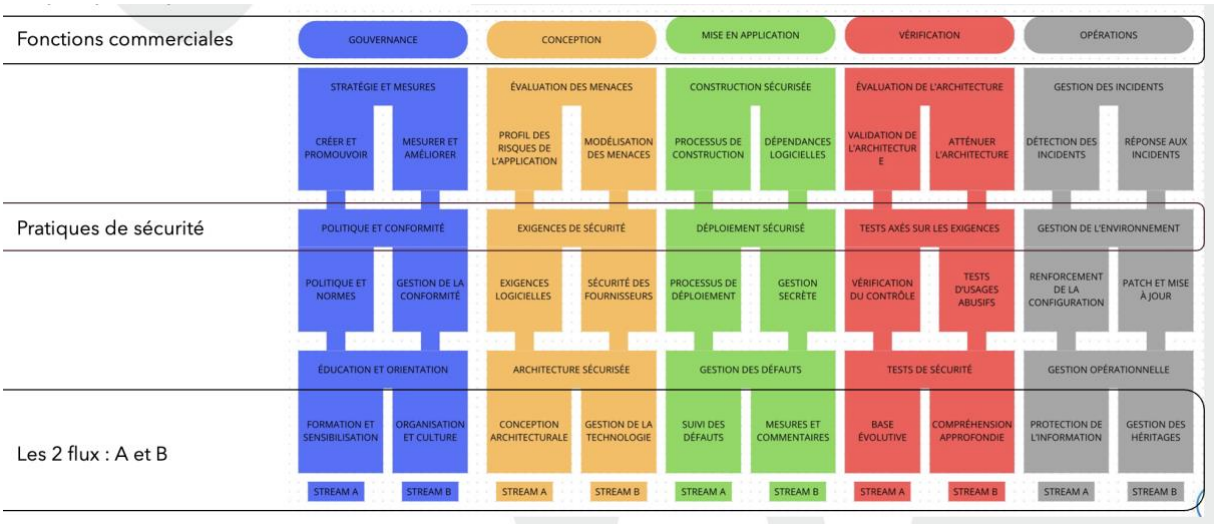
L'OpenSAMM (Software Assurance Maturity Model) est un projet ouvert de l'OWASP (Open Web Application Security Project) qui aide les organisations à évaluer, à formuler et à mettre en œuvre une stratégie de sécurité logicielle. Il est disponible gratuitement et il peut être utilisé par les petites, moyennes et grandes organisations utilisant n'importe quel style de développement.
La communauté SAMM de l'OWASP est alimentée par des bénévoles compétents en matière de sécurité provenant d'entreprises et d'organisations éducatives. Elle travaille à la création d'articles, de méthodologies, de documentations, d'outils et de technologies librement disponibles.

Leur mission est d'aider les organisations à évaluer leur niveau actuel de maturité en matière de sécurité logicielle et à fournir des recommandations pour progresser vers des niveaux de maturité supérieurs.
L'organisation détermine le niveau de maturité cible pour chaque pratique de sécurité qui convient le mieux à ses besoins.

SAMM fournit des ressources qui aident à évaluer l'existence d'une organisation pratique de sécurité logicielle. Cela permet de comprendre le niveau de maturité actuel en matière de sécurité des logiciels et d'identifier les forces et faiblesses. Par exemple, l'OWASP met à disposition un tableau pour évaluer le niveau de maturité actuel de l'organisation.
Ensuite, il aide à construire un programme de sécurité logicielle équilibré dans des itérations bien définies. SAMM suggère une approche bien définie pour construire progressivement un programme complet et équilibré. L'OWASP propose un document avec des étapes concrètes pour aider l'organisation à démarrer.
Il aide à démontrer des améliorations concrètes à un programme d'assurance de la sécurité en utilisant une roadmap pour améliorer un ou plusieurs points de sécurité.
Enfin, il aide à définir et mesurer les activités liées à la sécurité au sein d'une organisation. L'OWASP propose un plan avec des fonctions commerciales et des pratiques de sécurité à suivre.

SAMM est basé sur environ 15 pratiques de sécurité regroupées en 5 fonctions commerciales (gouvernement, conception, mise en application, vérification, opérations). Une fonction commerciale est une catégorie d'activités que toute organisation impliquée dans le développement de logiciels doit accomplir.

Ensuite, chaque fonction commerciale est répartie en trois pratiques de sécurité, ce sont des domaines d'activités liées à la sécurité.
Les pratiques de sécurité sont divisées en deux flux.
Pour chaque pratique de sécurité, SAMM définit trois niveaux de maturité. Ils sont différents pour chaque pratique. Les activités à un niveau de maturité inférieur sont généralement plus faciles à exécuter et nécessitent moins de formalisation que celles à un niveau de maturité plus élevé.



La gouvernance se concentre sur l'établissement d'une direction stratégique pour la sécurité des logiciels au sein de l'organisation. Elle implique la création de politiques, de responsabilités et de mécanismes de prise de décision pour garantir que la sécurité des logiciels est une priorité au niveau de la direction.
L'objectif est d'intégrer la sécurité des logiciels dans la culture organisationnelle.

La conception se concentre sur la manière dont la sécurité est intégrée dans le processus de développement de logiciels dès le début. Elle implique la définition d'exigences de sécurité, la sélection d'architectures et de technologies sécurisées, ainsi que la formation des développeurs à la conception sécurisée.
L'objectif est de réduire les vulnérabilités dès la phase de conception, ce qui permet de réaliser des économies à long terme.

La mise en application concerne la manière dont les pratiques de sécurité sont appliquées tout au long du cycle de développement de logiciels. Cela inclut l'utilisation de techniques de codage sécurisé, la gestion des vulnérabilités, les tests de sécurité et la validation des exigences de sécurité.
L'objectif est de s'assurer que les logiciels sont développés de manière sécurisée et conforme aux politiques de sécurité établies.

La fonction de vérification consiste à évaluer et à vérifier régulièrement la sécurité des logiciels, tant au niveau de code source que de l'architecture. Elle inclut des audits de sécurité, des tests de pénétration, des analyses de vulnérabilités, et d'autres méthodes d'inspection.
L'objectif est de s'assurer que les logiciels restent sécurisés face à l'évolution des menaces et des technologies.

La fonction d'opération se concentre sur la gestion de la sécurité des logiciels une fois qu'ils sont en production. Cela inclut la surveillance des systèmes, la gestion des correctifs, la gestion des incidents de sécurité et la réponse aux incidents.
L'objectif est de garantir la continuité de la sécurité tout au long du cycle de vie des logiciels, en minimisant les risques opérationnels.

2) Comment évaluer le niveau de maturité en termes de sécurité logicielle ?

Le modèle SAMM est structuré selon 4 points. Cela passe par l'évaluation de la position actuelle de l'organisation en matière de sécurité logicielle, la définition de l'objectif de l'organisation, la définition d'une feuille de route de mise en œuvre pour y arriver et des conseils sur la façon de mettre en œuvre des activités particulières.

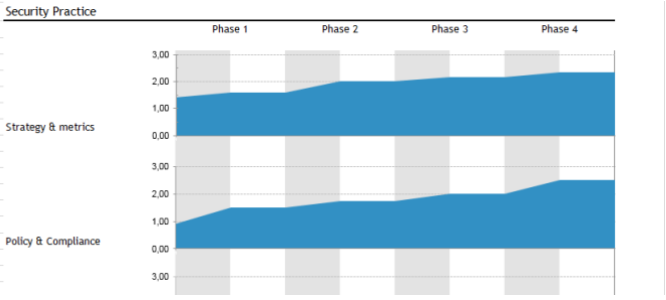
L'OWASP fournit un document dans lequel l'organisation peut évaluer son niveau de maturité en termes de sécurité logicielle.
Le questionnaire est organisé en plusieurs parties, on retrouve dans l'image ci-dessous : la fonction commerciale « gouvernance », la pratique de sécurité « strategy & metrics », le flux « create and promote » et les trois niveaux de maturité (level 1, 2 et 3) avec une question à se poser pour chaque niveau.

Il est calculé en fonction d'un barème (0 ; 0,25 ; 0,5 ; 1) lié aux réponses aux questions de chaque niveau de maturité.

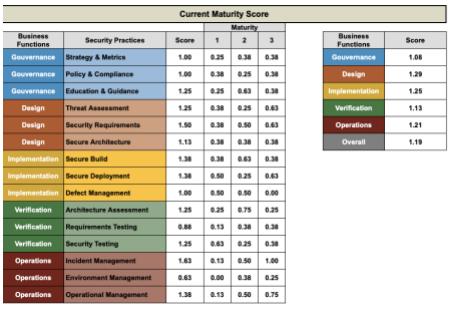
Gouvernance								
Stream	Level	Strategy & Metrics		Answer			Interview Notes	Rating
Create and Promote	1	Do you understand the enterprise-wide risk appetite for your applications ? You capture the risk appetite of your organization's executive leadership The organization's leadership vet and approve the set of risks You identify the main business and technical threats to your assets and data You document risks and store them in an accessible location	N	No	0	0.250		1.00
	2	Do you have a strategic plan for application security and use it to make decisions? The plan reflects the organization's business priorities and risk appetite The plan includes measurable milestones and a budget The plan is consistent with the organization's business drivers and risks The plan lays out a roadmap for strategic and tactical initiatives You have buy-in from stakeholders, including development teams	O	Yes, we review it annually	0.25	0.375		
	3	Do you regularly review and update the Strategic Plan for Application Security? You review and update the plan in response to significant changes in the business environment, the organization, or its risk appetite Plan update steps include reviewing the plan with all the stakeholders and updating the business drivers and strategies You adjust the plan and roadmap based on lessons learned from completed roadmap activities You publish progress information on roadmap activities, making sure they are available to all stakeholders	P	Yes, we review it at regular times	0.5	0.375		

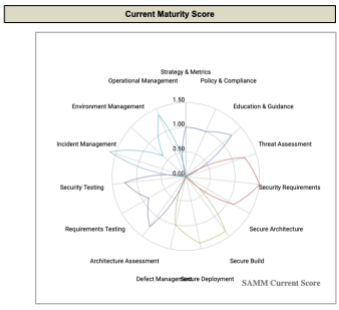
Ensuite, on trouve une roadmap pour améliorer les scores en fonction des réponses données dans le tableau et propose d'améliorer un ou plusieurs points.
On retrouve les pratiques de sécurité avec quatre phases qui correspondent aux quatre premières étapes pour mettre en place OpenSAMM : préparer, évaluer, fixer la cible, définir le plan.
Le « current gap » pour voir l'écart actuel et un graphique pour voir l'évolution du score par phase.

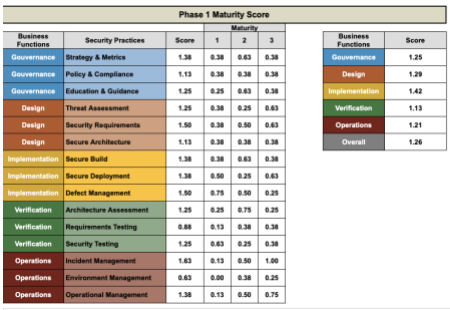
Source Data	As-Is				To-Be	
Security Practices/Phase	Start	Phase 1	Phase 2	Phase 3	Phase 4	Current GAP
Strategy & metrics	1,42	1,58	2,00	2,17	2,33	0,92
Policy & Compliance	0,90	1,50	1,75	2,00	2,50	1,60
Education & Guidance	1,05	1,20	1,45	1,70	2,20	1,15
Threat Assessment	1,10	1,20	1,35	1,92	1,92	0,82
Security Requirements	1,55	1,70	1,70	1,95	1,95	0,40
Secure Architecture	1,45	1,45	1,70	1,70	1,70	0,25
Design Analysis	1,85	1,85	1,85	2,00	2,00	0,15
Implementation Review	1,05	1,20	1,35	1,60	2,25	1,20
Security Testing	1,12	1,12	1,12	1,27	1,52	0,40
Issue Management	1,93	1,93	2,08	2,08	2,33	0,40
Environment Hardening	1,70	1,70	1,70	1,85	1,85	0,15
Operational Enablement	0,95	1,05	1,20	1,45	1,60	0,65
SAMM velocity:		1,42	1,77	2,43	2,47	8,08
		18%	22%	30%	31%	66%

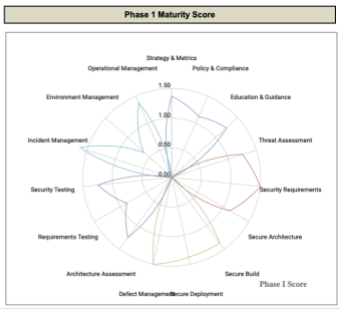


Il y a aussi une feuille qui présente les statistiques sur la situation actuelle (par niveau de maturité, avec un graphique, par fonctions commerciales).









3) Comment mettre en place OpenSAMM ?

Il faut suivre différentes étapes pour mettre en place OpenSAMM.
Pour chaque étape, on a un objectif à atteindre et plusieurs activités à mener pour atteindre l'objectif. Il y a aussi des ressources pour s'aider et les meilleures pratiques à mettre en place pour réussir.

La première étape est la préparation, l'objectif est d'assurer un bon démarrage du projet. Ensuite, les activités à mettre en place sont de définir la portée, identifier les parties prenantes et communiquer sur les initiatives.

La seconde étape est l'évaluation, l'objectif est d'identifier et comprendre la maturité de la portée choisie dans chacune des 15 pratiques de sécurité logicielle. Pour les activités, il faut évaluer les pratiques actuelles et déterminer le niveau de maturité.

La troisième étape est de fixer la cible, l'objectif est de définir le niveau cible dans chaque sous-domaine. Il faut définir la cible et estimer l'impact global.

La quatrième étape est de définir le plan, l'objectif est de développer ou mettre à jour le plan pour faire passer l'organisation au niveau supérieur. Les activités à mettre en place sont de déterminer le calendrier des changements et d'élaborer ou mettre à jour le plan de la feuille de route.

La cinquième étape est de mettre en œuvre et l'objectif est de travailler le plan. Il faut mettre en œuvre les activités nécessaires.

La dernière étape est le déroulement, l'objectif est de s'assurer que les améliorations sont disponibles et utilisées efficacement au sein de l'organisation. Il faut communiquer sur les améliorations et mesurer l'efficacité.

4) Conclusion

Le projet OpenSAMM permet aux entreprises de mieux comprendre et gérer les risques liés à la sécurité tout au long du cycle de vie du développement logiciel. Une entreprise qui adopte OpenSAMM progresse vers une meilleure sécurité informatique.