# <VADE MECUM DES SECURITY CHAMPIONS ET SME APPSEC>

## GROUPE DE TRAVAIL CYBERSÉCURITE AGILE

**CAMPUS CYBER** 2025

# < SOMMAIRE >

# 1. PRÉAMBULE

Le présent document a pour objectif d'aider les responsables de sécurité, les responsables de programmes de Sécurité Applicative et DevSecOps et les chefs de projet, à concevoir une organisation au niveau de leurs équipes pour répondre aux enjeux de sécurité dans les projets agiles, en incluant les principaux rôles et les principales activités de Sécurité Applicative.

Ce guide peut être appliqué pour tout projet (ou toute équipe) pour lequel une méthodologie de gestion agile est mise en place. Ce guide n'a pas vocation à couvrir d'autres méthodologies de gestion de projet telles que le Waterfall ou le cycle en V/W.

Ce guide a été construit de manière agnostique dans le sens où aucune méthodologie agile n'est mise en avant par rapport à une autre. Des terminologies relatives à l'agilité y sont présentes (produit, backlog, etc.).

Ce guide vise à établir un modèle où l'ensemble des rôles et activités des Security Champions et des SME (Subject Matter Expert) AppSec sont pris en compte. Libre à chacun de décliner ce modèle en fonction de ses besoins et du contexte de son organisation, en incluant toute ou partie des éléments définis dans ce guide.

# 2. INTÉGRATION DE LA SÉCURITÉ DANS LES PROJETS : VERS L'AGILITÉ

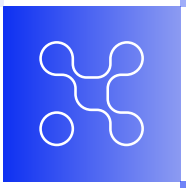
La sécurité dans les projets, généralement assimilée à la pratique connue sous le nom de « Intégration de la Sécurité dans les Projets » (ISP), est une activité visant à déterminer les besoins de sécurité en lien avec un projet de développement, d'intégration et/ou de maintenance logicielle et à s'assurer que ces besoins sont bien pris en compte.

La démarche d'ISP se base généralement sur l'approche par le risque avec des activités en amont du développement telles que l'évaluation des besoins DICT (Disponibilité - Intégrité - Confidentialité - Traçabilité), la classification de la donnée, l'analyse des risques, la détermination des exigences de sécurité et l'établissement des mesures qui en découlent; puis une évaluation du niveau de sécurité de l'application est réalisée en aval, souvent au travers de prestations d'audit de sécurité (code, configuration, tests d'intrusion, etc.), pour s'assurer que les exigences ont bien été prises en compte et les mesures correctement mises en place une fois les phases de développement et d'intégration réalisées.

Plusieurs problématiques apparaissent lorsque cette démarche est appliquée de manière « classique », que nous classons selon les trois piliers People - Process - Technology :

- **People** ⟶ Les activités décrites sont souvent réalisées de manière silotée par une équipe sécurité / SSI spécifique, extérieure au projet, avec des objectifs parfois distincts de ceux du projet et de son équipe. L'avis de l'équipe projet, ainsi que les enjeux et les contraintes du projet, ne sont pas assez considérés. L'accompagnement dont les parties prenantes (en particulier les développeurs) ont besoin est soit sous-évalué, soit non considéré. Tout ceci provoque généralement la non-adhésion de l'équipe projet à la démarche et peut mener à une mauvaise voire une absence totale de mise en œuvre des mesures de sécurité préconisées.

- **Process** ⟶ Les activités décrites sont réalisées de manière statique et séquentielle, en amont et en aval du cycle de vie du projet. Ce faisant, elles ne permettent pas d'assurer que les mesures de sécurité sont en adéquation avec l'évolution des exigences du produit. Elles ne sont pas mises en place tout au long du cycle de vie du projet, ne sont pas industrialisées dans les chaines CI/CD et soutiennent mal la démarche DevSecOps. Parfois prises en compte au dernier moment en vue d'obtenir une autorisation de mise en production, les exigences de sécurité sont rediscutées sous la contrainte du calendrier et peuvent venir affecter les performances et l'expérience utilisateur du produit final.



- **Technology** ⟶ Le processus étant généralement siloté, il y a un écart entre les outils employés et ceux utilisés par l'équipe projet, ce qui accentue le risque de non-adhésion de l'équipe projet. Le processus étant séquentiel, les outils généralement utilisés ne sont pas souples et s'adaptent assez mal aux besoins du projet ainsi qu'au processus agile. Ainsi, on observe par exemple que des outils de type « tableur » sont utilisés pour lister les exigences de sécurité et les mesures correspondantes à mettre en place. Les tableurs sont ensuite mis à jour (ou non) manuellement au gré des évaluations et des audits de sécurité. Ils peuvent parfois devenir le principal outil de suivi des risques et des vulnérabilités. Les dépendances entre les exigences/mesures des différentes briques logicielles qui composent le produit final sont également maintenues manuellement, menant à des erreurs, des oublis et une perte de temps considérable à réaliser des activités « bureautiques » plutôt qu'à réellement évaluer et sécuriser le produit.

Ces problématiques en lien avec une application « classique » de la démarche ISP peuvent avoir les conséquences suivantes :

- Développement d'une vision où la sécurité est conçue comme étant imposée et contraignante. Les équipes projet doivent se conformer aux directives qui leurs sont données au début du projet et des contrôles sont effectués (uniquement) en fin de projet. Par conséquent, l'équipe projet cherche davantage à se mettre en conformité par rapport aux exigences de sécurité qu'à réellement améliorer la sécurité de son application. Cela peut provoquer un rapport biaisé à la sécurité et être contre-productif.

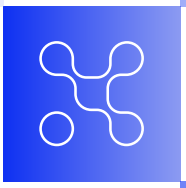
- Le niveau de sécurité réel de l'application étant évalué en fin de cycle, des vulnérabilités structurantes impliquant des risques importants peuvent être détectées à un moment où il est plus compliqué d'apporter une remédiation. En effet, en fin de cycle de vie du projet, il n'y a souvent plus suffisamment de budget et de ressources pour implémenter les remédiations, surtout si des vulnérabilités remettant en cause tout ou partie de l'architecture logicielle ont été détectées. Dépendamment de la stratégie adoptée pour y faire face, il peut soit y avoir un impact négatif sur le ROI prévu du projet et le délai de mise en production de l'application (et donc un Time To Market moins bon), soit occasionner une acceptation des risques (parfois critiques ou majeurs) lors de la mise en production de l'application et l'ouverture aux utilisateurs.

- Ce type de démarche ne convient pas du tout aux méthodologies agiles, qui permettent par essence de revoir les spécifications et de changer les exigences fonctionnelles et non fonctionnelles de manière itérative. La définition d'exigences de sécurité uniquement en début de projet et la vérification des mesures spécifiquement mises en place pour ces exigences en fin de projet pourraient présenter un biais où les changements et évolutions que l'application a connus au travers des itérations successives ne sont pas inclues dans le processus. Cela aurait un impact sur la bonne évaluation du niveau de sécurité de l'application et pourrait laisser croire qu'elle est suffisamment sécurisée.

- Ces risques non couverts au niveau applicatif sont souvent compensés par le déploiement systématique de solutions de sécurité génériques qui ne s'adaptent pas aux projets.

- L'équipe SOC est bien souvent en peine pour identifier des règles d'analyse de log pertinentes, ces derniers n'ayant pas été identifiés entre autres par une démarche de scénarios redoutés.

- Dans ce contexte, la responsabilité au regard du risque Cyber reste flou entre équipe projet et équipes sécurités.



En résumé, l'utilisation d'une démarche statique, séquentielle et silotée de la sécurité dans les projets ne permet pas d'aboutir aux résultats escomptés, en particulier dans les contextes agiles.

Les méthodologies agiles nécessitent une plus grande adaptabilité dans la manière de travailler, ce qui impacte nécessairement la manière de concevoir des logiciels de manière sécurisée.

Dans un tel contexte, une méthodologie de sécurité adaptable d'un point de vue opérationnel aux méthodologies agiles doit avoir les caractéristiques suivantes :

- Privilégier le support et l'accompagnement, en livrant rapidement et fréquemment de la valeur, à la contrainte et la conformité.
- Accueillir positivement les demandes de changement, même tard dans le projet.
- Vérifier fréquemment la qualité (et donc aussi la sécurité) du logiciel.
- Faire collaborer étroitement les équipes projet et les équipes de sécurité.
- Respecter les compétences de chacun et être capable de faire confiance pour atteindre les objectifs.
- Privilégier le dialogue au fait d'imposer ses exigences et ses manières de travailler.
- Mesurer l'avancement en termes de fonctionnalités, y compris de sécurité, délivrées.
- Avancer à un rythme soutenable et constant, y compris pour les fonctionnalités de sécurité.
- Porter une attention continue à l'excellence technique et la conception, qui ne doit pas occulter les critères DICT (Disponibilité, Intégrité, Confidentialité et Traçabilité).
- Viser la simplicité, tant dans l'élaboration du produit que les méthodologies de vérification et de remédiation.
- Responsabiliser les équipes et leurs différentes parties prenantes, car tout le monde est concerné par la sécurité et chacun a son rôle à jouer.
- Ajuster régulièrement son comportement et ses processus pour être plus efficace.
- PS : Toute ressemblance avec les 12 principes généraux du manifeste Agile ne serait pas du tout fortuite.

Une telle méthodologie de sécurité agile a des implications au niveau de :

- L'axe People, dans la mesure où les rôles au sein et en dehors des équipes projet sont revus et où les différentes parties prenantes au sein du projet sont toutes responsables de la sécurité, à leur niveau. Elles doivent être formées de manière adéquate et collaborer afin de viser les mêmes objectifs de réussite du projet. Les équipes de sécurité ne sont plus considérées comme des organismes de contrôle qui empêchent le projet d'avancer, mais comme un soutien utile à qui on peut remonter des informations et obtenir de l'aide sans tabou, ce qui favorise le bon développement du projet.

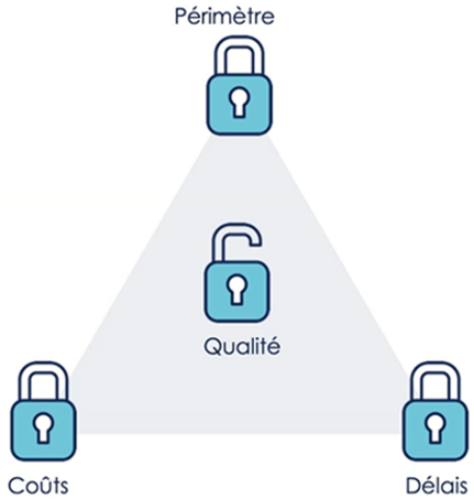
C'est principalement sur cet aspect que se concentre la suite de ce document.

- L'axe Process, dans la mesure où la démarche de sécurité doit s'intégrer complètement avec la méthodologie (agile) du projet. Les activités de sécurité doivent pouvoir s'adapter et être réalisées de manière itérative et régulière dans toutes les étapes correspondantes du cycle de vie du projet. En mode agile, toutes les fonctionnalités ne sont pas présentes dès la première livraison mais apparaissent progressivement au fil des itérations. Le concept est d'appliquer le même principe d'agilité (ajout dans le backlog) pour les fonctionnalités et activités de sécurité, en priorisant en fonction du niveau de risque. La définition même des DOR (Definition Of Ready) et DOD (Definition Of Done) doit également prendre en considération la sécurité comme la présence d'abuse case ou encore la spécification des logs de sécurité associés à une User Story.

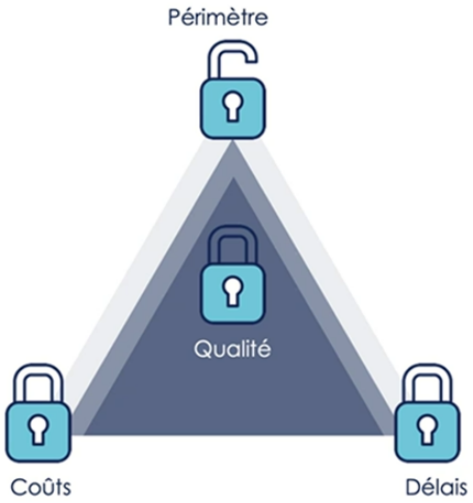
- L'axe Technology, dans la mesure où les outils doivent s'adapter également à l'organisation et aux pratiques de l'équipe projet ainsi qu'aux processus de sécurité mis en place. Ils doivent faciliter le suivi de sécurité dans le temps, en permettant aux différentes parties prenantes de se concentrer sur leur valeur ajoutée.

Enfin, il est important de considérer l'agilité comme une opportunité à saisir plutôt qu'une contrainte supplémentaire sur la sécurité. Inversement, la sécurité ne doit pas être un frein à l'innovation : Elle l'accompagne afin qu'elle puisse se développer sereinement.

C'est en partie ce que le « triangle de fer », une fois transposé vers l'agilité, nous apprend :




**Méthodologie de projet classique**

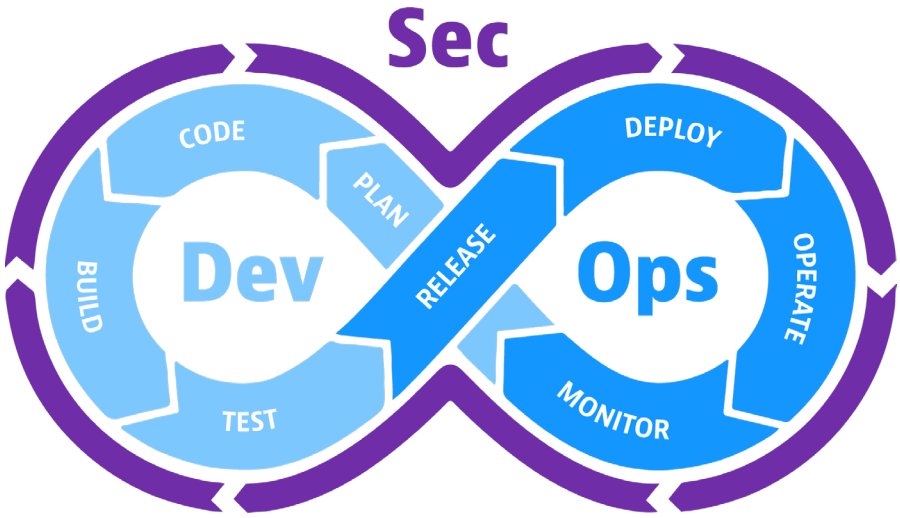



**Méthodologie de projet agile**

→ Les méthodologies agiles visent à assurer la qualité, les coûts et les délais en assouplissant le périmètre du produit.

→ La sécurité pouvant être considérée comme une partie intégrante de la qualité, les méthodologies agiles sont propices à la création de produits sécurisés. Elles ne consistent pas uniquement en l'apport de nouvelles fonctionnalités métier aux applications, mais aussi en une optimisation et amélioration systématique de l'existant.

**Remarque :** La Sécurité Agile est un prérequis à la mise en place d'une démarche DevSecOps cohérente et efficace, mettant en œuvre les activités de sécurité en symbiose avec les activités « classiques » de développement et d'exploitation.



# 3. INTÉGRATION DE LA SÉCURITÉ DANS DES CONTEXTES AGILES

Comme évoqué précédemment, les méthodologies agiles nécessitent une plus grande adaptabilité dans la manière de travailler, étant donné le rythme du cycle de développement avec des itérations courtes - parfois appelées les « sprints » - et l'évolution constante des besoins. Cela impacte nécessairement la manière de concevoir des logiciels de manière sécurisée.

Comment s'assurer que la sécurité pourra suivre les évolutions des besoins et le développement de nouvelles fonctionnalités métier ? Qu'elle ne sera pas laissée de côté ? La problématique est déjà de taille pour un seul projet ou une seule équipe produit (squad), comment assurer la mise à l'échelle au sein de toute une organisation et la pérennité dans le temps ?

Pour répondre à ces enjeux, plusieurs axes se dessinent :

- La mise en place d'une organisation projet adaptée, permettant d'embarquer la sécurité dans un contexte agile et, dans la mesure du possible, à l'échelle.

C'est dans cette démarche que s'intègrent les rôles de Security Champion et de SME (Subject Matter Expert) AppSec.

- La sensibilisation de toutes les parties prenantes à la sécurité et la formation des membres des équipes produits, en particulier les développeurs, aux principaux risques de sécurité applicative et au développement sécurisé.

Il est important d'avoir les bons « sponsors » pour soutenir tout changement de culture et d'organisation, obtenir l'adhésion des décideurs et de toutes les parties prenantes et pour soutenir la mise en place un plan de formation approprié.

Cf. la section Eléments clés de performance pour plus d'informations à ce sujet.

## 3.1 POURQUOI LE SECURITY CHAMPION (SC) ?

Partons tout d'abord d'un constat : il est difficile d'intégrer les enjeux et exigences de sécurité dans un projet informatique.

Au-delà des problématiques évoquées précédemment en lien avec l'intégration « classique » de la sécurité dans les projets, un point critique est le manque de ressources ayant à la fois des compétences en Cybersécurité et des connaissances en développement et gestion de projet. Il est difficilement concevable, pour tout type d'organisation, de prévoir à l'échelle un ETP (Equivalent Temps Plein), ou même un demi-ETP, dédié aux tâches de sécurité d'un seul produit ou d'une seule équipe. Les équipes SSI n'ont pas les ressources et le budget pour cela.

Or, dans un contexte agile, il est nécessaire que les tâches de sécurité soient alignées avec les pratiques et la chronologie du projet. Le besoin d'accompagnement et de supervision de l'équipe produit pour gérer ces tâches est réel.

C'est dans ce contexte que le concept de Security Champion est apparu.

Le concept de Security Champion vise à renforcer la sécurité au sein des équipes de développement, en désignant une personne qui agit comme point de contact pour les questions de sécurité, qui coordonne les activités de sécurité et promeut les bonnes pratiques. L'organisation OWASP (Open Worldwide Application Security Project) a été un précurseur en ce qui concerne la théorisation de ce rôle. Voir l'un des articles de référence ici https://owasp.org/www-project-security-culture/stable/4-Security_Champions/.

Le Security Champion est, dans le concept d'origine, un membre de l'équipe, généralement un développeur expérimenté ou le Tech Lead, ce qui lui permet de continuer de participer aux activités de développement et de partager les enjeux et pratiques de l'équipe dans laquelle il est complètement intégré. L'objectif n'est pas qu'il porte toutes les responsabilités de sécurité, mais qu'il soit un référent sur lequel le reste de l'équipe peut se reposer, de manière à ce que la sécurité soit bien intégrée au sein des activités de l'équipe, des fonctionnalités du produit, et qu'elle devienne l'affaire de tous. On peut faire le parallèle avec la thématique de la qualité, qui a demandé un changement de culture et un fort accompagnement pour arriver à l'état de l'art actuelle ou elle fait partie intégrante de l'activité d'une équipe de développement.

Un modèle organisationnel alternatif peut être envisagé pour le Security Champion, dans lequel ce rôle est porté par une ou plusieurs personne(s) agissant pour plusieurs produits de manière transverse. Dans ce cas, le Security Champion n'est pas nécessairement membre d'une équipe produit en particulier. Néanmoins, il est fortement recommandé qu'il ait tout de même des compétences avancées en développement, intégration et maintenance des logiciels, ainsi qu'une connaissance de base des projets sur lesquels il intervient. En étant transverse à plusieurs projets, il risque de ne pas avoir une aussi bonne vision et maitrise d'un produit en particulier, mais il pourra plus aisément capitaliser sur les connaissances et pratiques entre les différents produits.

Libre à chaque organisation de décliner le rôle de Security Champion en fonction de ce qui est le plus pertinent par rapport à son contexte et ses besoins. Les deux principaux modèles organisationnels, leurs avantages et inconvénients, sont présentés en détail dans la section Les modèles organisationnels pour les Security Champions.

**Remarque :** Le terme « Security Champion », venant du monde anglophone et que nous avons repris au sein de ce document, peut être trompeur. Il ne représente pas nécessairement un expert ayant des compétences avancées en Cybersécurité, mais plutôt un « ambassadeur », servant de référent et de point de contact privilégié au sein d'une équipe produit. L'expertise poussée en Sécurité Applicative est portée par le SME AppSec.

## 3.2 SENSIBILISATION DES PARTIES PRENANTES ET FORMATION DES DÉVELOPPEURS

Pour que la sécurité soit correctement mise en place à tous les niveaux, dans chaque étape du cycle de vie des applications, il est nécessaire de faire prendre conscience aux parties prenantes de leurs responsabilités afin qu'elles puissent correctement les assumer.

Qui de mieux qu'un analyste fonctionnel pour définir avec justesse les workflows métier et par extension les use cases, les abuse cases et les user security stories ?

Qui de mieux qu'un architecte logiciel pour intégrer dans l'architecture de l'application et de ses composants les principales briques de sécurité, leur fonctionnement et les interactions avec les autres briques ?

Qui de mieux qu'un développeur pour appliquer les bonnes pratiques de sécurité pour tout nouveau développement et pour effectuer des revues de code manuelles ?

Qui de mieux qu'un exploitant pour s'approprier l'infrastructure cible et sa configuration afin de s'assurer qu'elles sont conformes aux standards et/ou bonnes pratiques ?

Etc.

Obtenir l'adhésion et l'engagement de toutes les parties prenantes autour de la sécurité est certainement une tâche complexe à réaliser, mais elle est tout aussi fructueuse :

- Si pour un projet, les différentes parties prenantes sont alignées sur les enjeux et la démarche de sécurité, les processus et outils adéquats suivront.
- A l'inverse, si des processus à l'état de l'art sont mis en place conjointement avec les meilleurs outils existants sur le marché, mais que l'équipe produit n'est pas sensibilisée à la sécurité et ne se sent pas concernée, alors les processus ne seront pas suivis efficacement et les outils ne seront pas exploités.

Il y a donc un enjeu majeur d'adhésion de l'équipe produit et des personnes qui la composent.

Pour répondre à cet enjeu et s'assurer que la culture et les bonnes pratiques de sécurité soient bien répandues, en complément du modèle de Security Champion, il est structurant de prévoir des sensibilisations (pour divers profils) et des formations (pour les développeurs a minima) sur le sujet de la Sécurité Applicative.

## 3.3 POURQUOI LE SUBJECT MATTER EXPERT (SME) APPSEC ?

Comme évoqué précédemment, le Security Champion (SC) est un référent au sein d'une ou plusieurs équipe(s) produit, selon le modèle mis en place (cf. Les modèles organisationnels pour les Security Champions), servant de point de contact privilégié pour les sujets de sécurité et s'assurant que les enjeux de sécurité soient pris en compte pour le ou les produit(s) qu'il traite. Le SC n'est pas nécessairement un expert en sécurité, non seulement pour une raison de complexité de formation et de manque de ressources (cf. Pourquoi le Security Champion (SC) ?), mais aussi car une partie plus ou moins importante de son temps peut être dédiée à d'autres activités, comme le développement. Il lui est impossible de tout connaître et maitriser dans le détail. Le SC doit au moins être en mesure d'identifier les problèmes de sécurité et les ressources l'aidant à les résoudre, à défaut de savoir comment les traiter directement. Il doit donc pouvoir se reposer sur une personne (ou un ensemble de personnes selon la taille de l'organisation), qui a des connaissances et des compétences techniques avancées sur les sujets de sécurité, et qui peut prendre du recul grâce à une vision externe au projet et transverse sur la composition du SI et de ses besoins.

C'est là que la notion de SME (Subject Matter Expert) entre en jeu. Comme son nom l'indique, un SME est expert dans un sujet et sert de référent et de conseiller dans ce domaine. Là où le SME s'est spécialisé - à la suite d'années d'expérience - pour ensuite restituer ses connaissances, le SC connait des notions et concepts sur de nombreux sujets et sait s'adresser au bon SME pour trouver l'information qui convient à son besoin. Ainsi, le SC n'a pas à tout connaître, mais il a besoin de savoir comment détecter les problèmes et où trouver les informations nécessaires pour réussir à les résoudre, notamment en posant les bonnes questions aux bons interlocuteurs, si ses connaissances et recherches ne lui permettent pas d'obtenir une réponse rapidement. Le SME est là pour apporter des éléments de réponse qui ne sont pas facilement identifiables à partir des sources documentaires communes (recherches sur Internet, articles communautaires, documentation des langages de programmation, etc.). Il est un facilitateur pour apporter de l'agilité, de la flexibilité et de la cohérence dans la résolution des problèmes. En effet, dans un contexte agile, il n'est pas possible de passer trop de temps sur la résolution d'un problème - de sécurité ou non. Il est donc utile d'avoir un expert qui sait si une solution déjà existante est présente ou si c'est un besoin récurrent qui mériterait plus d'attention - par le biais de communications auprès des SC.

Le SME ayant un rôle transverse, il a une vision d'ensemble du SI et des équipes IT. Il favorise la centralisation des solutions aux problèmes connus et peut rediriger au besoin vers une équipe ou un SC qui a déjà rencontré le même problème. Cette vision transverse permet également au SME de déceler les besoins qui sont communs à plusieurs équipes ou produits pour mettre en place des solutions adaptées, qu'il peut ensuite répertorier dans une base de connaissances. Il peut éventuellement dispenser des formations sur des sujets tels que le développement sécurité, ou sensibiliser plus largement aux enjeux de sécurité (cf. Sensibilisation des parties prenantes et formation des développeurs). Le SME peut également conseiller les équipes de sécurité opérationnelle et de gouvernance sécurité, pour qu'elles fassent les meilleurs choix, en demandant un avis de terrain aux Security Champions. C'est aussi en cela que le SME peut apporter de la cohérence sur l'ensemble du SI.

Dans le cadre de la sécurité applicative, des exemples de sujets sur lesquels le SME peut développer une expertise sont la modélisation des menaces, la conception de l'architecture logicielle, le développement sécurisé, la cryptographie, les protocoles et frameworks d'authentification et d'autorisation, l'utilisation des outils de test de sécurité, le choix des technologies (langages, Frameworks, bibliothèques, APIs), la gestion des vulnérabilités, etc. Les spécificités de chaque SI peuvent déterminer les autres sujets sur lesquels un SME peut être associé.

Prenons l'exemple d'une équipe dont le SC identifie un secret écrit en clair dans le code. Le SC sait que ce n'est pas une bonne pratique et que cela a déjà mené à des vulnérabilités critiques, mais il n'a jamais eu à régler ce genre de problème. Il va donc contacter un SME (i.e. en charge de l'architecture sécurisée) qui va lui indiquer les solutions de coffre-fort (Vault) qui sont outillées dans l'entreprise pour le Framework utilisé. Si aucune documentation n'est existante, le SME se chargera d'en rédiger une. Les prochains SC confrontés à ce problème sauront où trouver la réponse et pourront se référer au SME s'ils ont besoin de compléments. Ainsi, le SC a fait usage de son appétence à la sécurité pour identifier une faiblesse dans le code qui a pu être résolue dans les normes de l'entreprise grâce au SME qui a apporté les éléments techniques spécifiques à la résolution du problème.

En résumé, un Subject Matter Expert de Sécurité Applicative, qu'on abrégera SME AppSec par la suite, est un expert technique qui facilite la résolution des problèmes de Sécurité Applicative et DevSecOps et favorise la centralisation des connaissances concernant leurs solutions, afin d'apporter les meilleures réponses sur ces sujets à tous les Security Champions, avec le plus de cohérence possible. Il permet également d'accompagner les Security Champions dans leur montée en compétences en les aiguillant au mieux dans leurs choix.
Si un problème est récurrent, le Subject Matter Expert se doit d'y répondre avec une solution collective, facilitant la résolution de manière agile des problèmes. Grâce à sa vision d'ensemble, il s'assure que les Security Champions se synchronisent et répond à leurs besoins en faisant preuve de curiosité et d'anticipation.

On peut aussi représenter le Security Champion comme un référent sécurité, à l'échelle de son (ou ses) produit(s) pour son ou ses équipe(s), tandis que le SME AppSec est un référent sécurité à l'échelle d'un département ou de l'organisation pour les différents Security Champions.

# 4. LE RÔLE DU SECURITY CHAMPION

Dans une équipe de développement agile, le Security Champion est le point focal pour les questions de sécurité relatives à l'application développée.

A ce titre, il peut intervenir sur l'ensemble du cycle de vie, depuis les phases amont (études préalables, architecture, conception) jusqu'aux opérations après livraison, en passant par le développement, l'intégration et le déploiement, en y intégrant à chaque fois les tests et les validations de sécurité appropriées.

Néanmoins, ce rôle ne signifie pas qu'il soit le seul à se préoccuper de la sécurité : tous les membres de l'équipe doivent être impliqués car la sécurité est l'affaire de tous. Ainsi, au sein de l'équipe, le Security Champion est reconnu comme un sachant, auquel tous les autres vont pouvoir se référer. Il y promeut les bonnes pratiques, explique les tenants et aboutissants et implique le reste de l'équipe.

Le Security Champion est aussi un point focal pour les autres parties prenantes au sein de l'organisation. Il assure un rôle d'interface, notamment avec les équipes de gouvernance Sécurité. Il est en relation avec le ou les SME AppSec, dont le rôle est détaillé dans la suite de ce document, et participe à l'animation d'une communauté technique avec ses pairs.

En définitive, le rôle de « point focal » du Security Champion peut s'articuler autour de trois axes :

1. Les activités de sécurité dans le cycle de vie de l'application.
2. L'accompagnement des membres de l'équipe de développement sur les questions de sécurité.
3. L'interface entre l'équipe de développement et le reste de l'organisation pour les problématiques de sécurité de l'application développée.

Les activités, compétences requises et responsabilités relatives à ces trois axes sont détaillées dans la sous-section suivante « Les activités du Security Champion ». Attention toutefois, différentes organisations définissent différents ensembles d'activités pour le Security Champion. Il s'agit là d'une proposition générique, qui se veut relativement exhaustive, et qui a tout intérêt à être contextualisée en fonction de l'organisation, de ses processus et de sa culture.

Nous aborderons ensuite la question clé de La charge des activités du Security Champion et le dimensionnement de l'organisation.

Enfin, nous détaillerons deux potentiels modèles d'organisation, dans la sous-section « Les modèles organisationnels pour les Security Champions », leurs avantages, leurs inconvénients et les implications associées.

## 4.1 LES ACTIVITÉS DU SECURITY CHAMPION

Nous détaillons ici les principaux types d'activité d'un Security Champion. En fonction des organisations, peut-être que seules des parties de ces activités seront couvertes. Le rôle est à clarifier en tenant compte du contexte de l'entreprise, de la maturité du modèle et aussi des compétences des ressources identifiées pour le tenir.

### 4.1.1 Les activités de sécurité dans le cycle de vie de l'application

Les activités de sécurité à mener dans le cycle de développement sont notamment décrites en détail dans le SSDLC, objet de la première partie des travaux de ce GT, ainsi que dans le RACI, annexe du présent document. En première approche, on peut considérer que le Security Champion est le principal interlocuteur qui va intervenir, organiser et participer à la réalisation de ces activités de sécurité.

- **Conception:** Pendant les phases d'architecture et de conception, le Security Champion identifie les enjeux, les besoins et les exigences de sécurité, analyse les risques de sécurité et modélise les menaces, propose des mesures adéquates pour couvrir les risques et les besoins de conformité, participe à la rédaction des spécifications de sécurité (incluant par exemple les User Security Stories, les Abuse Cases), détaille le volet sécurité de l'architecture, décline et adapte la politique de sécurité, participe à la planification des activités de sécurité au sein de la chaine CI/CD et la définition des indicateurs clés de suivi. Il peut pour cela s'appuyer sur la politique de sécurité globale de l'organisation concernant les applications, sur des référentiels d'exigences, de bonnes pratiques, d'architecture, sur des méthodologies d'analyse des risques et de modélisation de menaces (Threat Modeling). Il accompagne le choix des dépendances (typiquement les bibliothèques logicielles et frameworks open-source) et l'élaboration de la chaine d'approvisionnement logicielle (software supply chain) pour s'assurer du bon niveau de sécurité de celles-ci.

- **Développement :** Lors du développement, le Security Champion s'assure du respect de l'implémentation des exigences et mesures de sécurité, insuffle les bonnes pratiques de développement sécurisé et participe à l'identification et la remédiation au plus tôt des vulnérabilités. Il participe aussi grandement à la priorisation des tâches de sécurité dans le backlog. Il peut procéder à des revues de code, s'assure de la bonne intégration et configuration des outils d'analyse statique de sécurité (détection des secrets, SAST –

Static Application Security Testing, analyse de la sécurité des modèles d'Infrastructure as Code…) pour son produit, prend en compte les résultats de ces outils afin de les trier (vrais et faux positifs) et qualifier les risques, puis participe à l'élaboration et au suivi des plans d'action et de remédiation. Son périmètre couvre potentiellement tout ce qui est relié à l'application: le code produit par l'équipe, les dépendances mais aussi le code Infrastructure et Cloud.

- **Construction et intégration :** Lors des phases de construction et intégration de l'application, le Security Champion s'assure de la cohérence et de la sécurité de la chaine d'approvisionnement logicielle. Il vérifie la provenance et l'intégrité des dépendances (vérification des signatures), s'assure qu'elles sont correctement inventoriées et que l'inventaire est maintenu dans le temps (approche SBOM – Software Bill Of Materials), s'assure de la bonne intégration et configuration des outils d'analyse de sécurité des dépendances logicielles (SCA – Software Composition Analysis) pour son produit, aide son équipe à qualifier l'exploitabilité et les risques réels relatifs aux vulnérabilités publiques détectées (CVE – Common Vulnerabilities and Exposures), puis participe à l'élaboration et au suivi des plans d'action et de remédiation.

- **Tests et déploiement :** Lors des phases de tests et de déploiement, le Security Champion s'assure de la bonne intégration et configuration des outils d'analyse dynamique et hybride de sécurité (DAST – Dynamic Application Security Testing, IAST – Interactive Application Security Testing…) pour son produit, aide son équipe à trier les résultats et qualifier les risques, puis participe à l'élaboration et au suivi des plans d'action et de remédiation. Il participe aussi au suivi des audits et évaluations de sécurité (tests d'intrusion, revue des configurations, …) réalisés sur les environnements déployés. Lors des livraisons, il peut être consulté pour la méthodologie de signature des artefacts produits.

- **Maintien en condition de sécurité :** Le Security Champion intervient pour le maintien en condition de sécurité de l'application, en particulier sur le volet des vulnérabilités publiques affectant les dépendances externes (bibliothèques open-source, frameworks, etc.). Il effectue une veille sur les vulnérabilités publiques connues, entres autres sujets de sécurité pouvant avoir un intérêt pour son rôle et son produit. Il s'assure de la bonne intégration et configuration des outils de supervision de sécurité pour son produit (analyse dynamique des conteneurs, RASP – Runtime Application Self-Protection, WAAP – Web Application and Api Protection…) et que les logs nécessaires et suffisants, concernant l'application et son écosystème, remontent bien au niveau des processus et outils de sécurité opérationnelle, afin que les incidents de sécurité puissent être détectés efficacement. Il reste vigilant quant aux remontées des outils de détection et supervision déployés et est le point focal pour toute remontée de vulnérabilité, d'alerte

de sécurité sur l'application, en particulier en production, provenant par exemple des processus de sécurité opérationnelle, des revues de code externes, des tests d'intrusion, des blocages d'un RASP ou WAAP, ou encore d'un programme de bug bounty.

- **Suivi de sécurité transverse :** Le Security Champion s'assure de l'implémentation des activités de sécurité au sein de la chaine CI/CD du produit et suit, régulièrement et de manière transverse aux étapes du cycle de vie de l'application, l'implémentation des mesures de sécurité, le traitement des risques analysés, des défauts identifiés et des vulnérabilités détectées. L'ensemble de ces éléments (et les autres indicateurs définis lors de la phase de conception) constituent les indicateurs clés de suivi de l'état de la sécurité du produit.

D'une manière générale, sur le cycle de vie de l'application, le Security Champion va coordonner les activités de sécurité et en réaliser certaines : il va évidemment contribuer à ces activités, mais il va aussi et surtout les gérer et les planifier pour et avec les autres membres de l'équipe, tout en favorisant leur montée en compétence sur la sécurité. Il participe notamment à la constitution du backlog et des itérations/sprints (le cas échéant), évalue les priorités concernant les tâches de sécurité et définit les échéances. En fin d'itération, il n'hésite pas à partager l'avancement des différentes tâches de sécurité (mise en place et utilisation des outils, vulnérabilités détectées, risques identifiés et qualifiées, mesures implémentées, etc.) et à faire le bilan de ce qui a fonctionné et de ce qui pourrait être amélioré, dans une logique d'amélioration continue.

Sur ce premier axe définissant les activités du Security Champion, les compétences de celui-ci sont avant tout techniques : le Security Champion est un développeur, voire un architecte logiciel et un testeur, expérimenté, capable de participer à la conception d'une architecture sécurisée, de produire du code sécurisé et d'en comprendre les tenants et aboutissants. Il possède une très bonne compréhension des problématiques de sécurité applicative, il connait les différents types de vulnérabilités, est capable de les identifier, de les expliquer et d'y remédier. Il maitrise les outils d'analyse sécurité qui sont mis à disposition de l'équipe et dispose d'un certain degré d'expertise et d'autonomie en matière d'ingénierie DevOps.

### 4.1.2 L'accompagnement de l'équipe de développement

Le Security Champion a pour mission d'accompagner l'équipe de développement dans la prise en compte des enjeux de sécurité dans toutes les phases du cycle de vie applicatif. Il sensibilise les développeurs et explicite les problématiques.

Dans cette optique, il intervient de manière réactive sur demande des membres de l'équipe de développement, mais aussi de manière proactive en étant à l'initiative d'actions de sensibilisation particulières :

- **Réactif :** Selon le modèle organisationnel mis en place, la sollicitation du Security Champion par un développeur peut se faire de manière plus ou moins formelle et structurée. La colocalisation des membres de l'équipe et les échanges de vive voix dans l'espace de travail (ou à la machine à café) permettent souvent une communication fluide et efficace sur des sujets plus ou moins complexes. Dans d'autres contextes, les échanges par email ou système de tickets peuvent aussi être envisagés.

- **Proactif :** Le Security Champion peut être à l'initiative d'actions de sensibilisation, voire de formation, ciblées au sein de l'équipe de développement. Par exemple, s'il constate une récurrence de certaines pratiques de code inadaptées ou si une question soulevée mérite d'être partagée plus largement. Il pourra, pour ce faire, organiser une réunion de présentation et d'échange, écrire une documentation particulière ou encore organiser une session de formation dans un outil adapté (certains outils de formation permettent de définir des parcours spécialisés et d'organiser des tournois).

Sur ce deuxième axe concernant l'accompagnement de l'équipe de développement, les compétences du Security Champion sont plus transverses. Il s'agit avant tout de compétences de communication, d'écoute, d'empathie, de transmission des connaissances de manière didactique. Il doit faire preuve de conviction et de persuasion afin d'obtenir la confiance de l'équipe pour y être considéré comme un véritable référent et un coach sur les sujets de sécurité. Il doit aussi savoir se remettre en question et être ouvert d'esprit.

### 4.1.3 L'interface avec le reste de l'organisation

Le Security Champion est le principal interlocuteur sur les questions de sécurité concernant la ou les applications auxquelles il est rattaché. Ainsi, il est en contact avec d'autres équipes de l'organisation, en particulier la gouvernance sécurité et la sécurité opérationnelle, sans oublier le SME AppSec qui est son principal référent et gère la communauté des Security Champions.

Pour la gouvernance, il assiste le chef / manager / product owner de l'équipe en charge de l'application sur les questions de sécurité applicative :

- Le Security Champion va, par exemple, prendre en charge la documentation pour tous les processus de sécurité : demandes de dérogations, assurance sécurité, vérifications de conformité… Dans certains modèles, il peut agir directement sur délégation du responsable du périmètre applicatif concerné.

- Le Security Champion sera sollicité pour les questions de gouvernance sécurité sur le périmètre : production d'indicateur et constitution de tableaux de bords. Il pourra aussi être l'interlocuteur privilégié sur le périmètre en cas d'audit.

Sur ce plan, les compétences du Security Champion ont plus trait à la gouvernance sécurité : capacité d'analyse des risques, d'abstraction des problématiques, de synthèse des enjeux, de présentation de la posture, de déclinaison d'exigences et proposition de mesures de sécurité.

En matière de sécurité opérationnelle, le Security Champion peut être sollicité (par exemple par le SOC) pour participer à diverses activités :

- L'analyse d'incidents en production concernant la ou les applications sur lesquelles il travaille. Il peut contribuer aux activités de réponse, de restauration voire forensiques dans certains cas particuliers.
- Une fois l'urgence passée, il s'assure que les causes racines ayant provoqué (ou pouvant être à l'origine) de certains incidents sont traitées.

Ses compétences sont assez générales en matière de sécurité opérationnelle sans être un expert. Il contribue sur sollicitation des équipes concernées et sera accompagné dans la démarche. Il peut aussi remonter des alertes aux équipes Cyber.

En cas de doute ou s'il a besoin d'un avis plus expérimenté, le Security Champion peut solliciter le SME AppSec (correspondant de l'équipe Cyber qui a l'expertise pour proposer des solutions concrètes). Le Security Champion discute de l'avancement des travaux, de ses difficultés et tout changement pouvant impacter les besoins de sécurisation de l'application avec ce correspondant Cyber.

A l'inverse, il peut (et devrait) partager ses retours d'expérience, les articles et autres ressources intéressantes qu'il a découvert, au SME AppSec et de manière plus générale à l'ensemble de la communauté de Sécurité Applicative de son organisation, à laquelle il contribue activement.

Enfin, le Security Champion a la responsabilité de partager les efforts de sécurisation à son équipe. Cf. la section L'accompagnement de l'équipe de développement pour de plus amples informations.

## 4.2 LA CHARGE DES ACTIVITÉS DU SECURITY CHAMPION ET LE DIMENSIONNEMENT

Une des questions clés relatives au rôle de Security Champion est la charge de travail que représente ses activités et le dimensionnement de l'organisation afférente.

La question n'est pas aisée et reste à ce jour éminemment variable d'une organisation à une autre, d'une équipe à une autre, influencée par de nombreux facteurs que nous détaillons ci-après :

- **Les enjeux, risques, besoins en conformité et appétence sécurité de l'organisation**. On pourrait regrouper ces facteurs sous la dénomination de « sensibilité sécurité ». On comprend bien que l'effort en matière de sécurité alloué à une application critique, opérée par une organisation fortement soumise à des contraintes réglementaires et à l'appétence au risque faible, sera bien plus important que pour une autre organisation ayant des enjeux de sécurité moins importants. Au sein d'une même organisation, aussi, divers degrés d'investissement pour la sécurité peuvent être constatés d'une application à une autre.

- **La couverture des activités.** Nous avons énoncé précédemment les activités que le rôle de Security Champion est susceptible d'adresser. Il n'est pas exclu que certaines organisations décident, en fonction de leur contexte et de leur historique, de ne couvrir qu'une partie de ces activités. Le reste étant alors pris en charge par d'autres moyens ou à d'autres niveaux dans l'organisation. La charge du Security Champion s'en trouve alors modifiée.

- **Le niveau d'automatisation et l'adéquation des outils de sécurité.** La maturité des outillages de sécurité mis à disposition, leur adéquation à un mode de fonctionnement agile et les niveaux d'automatisation qui en découlent influent sur la charge des équipes. Par exemple, un outil d'analyse performant, avec des taux de faux-positifs faibles, des conseils de remédiations adaptés et « clés en main », ainsi que des capacités d'intégration adaptées aux environnements techniques de l'organisation, sera un atout décisif pour réduire la charge de travail du Security Champion.

- Enfin et non des moindres : **la maturité sécurité des équipes produit**. C'est un leitmotiv en matière de sécurité des applications : plus les vulnérabilités sont évitées ou détectées tôt et remédiées promptement, moins cela représente d'effort pour les équipes. Les statistiques sont sans appel, le coût de remédiation d'une vulnérabilité peut être multiplié par des facteurs de plusieurs centaines quand on cherche à remédier plus tard dans le cycle de vie de l'application. Ce coût s'évalue notamment en effort humain et donc se reflète mécaniquement sur la charge de travail du Security Champion. La sensibilité et les compétences des développeurs influent aussi sur l'effort que le Security Champion doit allouer aux activités d'accompagnement et de formation.

Cela dit, la question du dimensionnement reste entière. Cette question épineuse revient, en quelque sorte, à se demander combien doit-on investir pour la sécurité d'une application. Au premier abord, en prenant en compte les activités à couvrir et les facteurs pouvant les influencer, la tendance est à envisager une charge de travail plutôt importante, parfois irréaliste au regard des contraintes organisationnelles et budgétaires des organisations.

Toutefois, il faut tenir compte du fait qu'il est rare que la sécurité applicative soit complétement délaissée par une équipe de développement. Certes, cela dépend du niveau de maturité, mais il y a toujours plus ou moins d'effort qui y est alloué. Une partie non négligeable de cette charge de travail est généralement transférée dans un modèle Security Champion.

Il convient donc de décorréler les deux aspects de cette transformation : le transfert de charge et l'amélioration de la sécurité.

D'un point de vue théorique, dans un tout premier temps, une organisation pourra concentrer une grande partie de l'effort sécurité d'une application sur le Security Champion, à charge égale. « Théorique », car évidemment, quand il s'agit d'activités opérationnelles, ces transferts ne sont pas aisés ni toujours réalisables.

Ensuite, la charge peut être augmentée dans une optique d'amélioration de la sécurité. Vient s'ajouter dans cette dynamique un gain d'efficacité des activités consolidées sur un même acteur qui contribue activement à cette amélioration.

Enfin, une fois qu'un bon niveau de maturité est atteint et qu'un mode de fonctionnement rodé est mis en place, chaque acteur et chaque développeur au sein du projet intègre les activités de sécurité parmi ses activités courantes, dans une optique de prise en compte de la sécurité à tous les niveaux et d'amélioration continue.

En pratique, l'expérience montre des cas très variés. Le dimensionnement d'une organisation Security Champion ne suit pas de règles prédéfinies ou établies. Chaque organisation alloue une charge qui dépend de son contexte, de sa maturité, de ses capacités et de son avancement dans une transformation en cours. Ce dimensionnement n'est pas réellement figé et évolue souvent dans le temps.

On prêtera attention à ne pas allouer une charge trop faible au risque de diluer l'effort. Suivant le modèle organisationnel adopté, voir à ce sujet la section concernant Les modèles organisationnels pour les Security Champions, il sera plus ou moins difficile pour le Security Champion d'allouer efficacement du temps aux activités de sécurité dans son quotidien ou d'adresser plusieurs sujets (et de surcroît plusieurs projets) en parallèle.

Pour conclure, de manière très approximative, un ratio d'1 ETP de Security Champion pour 20 ETP développeurs semble assez souvent être adopté dans une première approche et peut être un bon point de départ. **Pour un Security Champion complètement intégré dans une équipe de développement** d'environ 5 personnes, cela représente à peu près 2 heures par jour consacrées aux activités de sécurité. Pour des équipes de 5 développeurs, cela signifie qu'un Security Champion qui dédie 100% de son temps à la sécurité peut couvrir un maximum de 4 équipes en parallèle.

## 4.3 LES MODÈLES ORGANISATIONNELS POUR LES SECURITY CHAMPIONS

Il est possible d'envisager le rôle de Security Champion selon différents modèles organisationnels. Nous en présentons deux par la suite : Le Security Champion comme rôle au sein d'une équipe produit ou le Security Champion comme rôle transverse à plusieurs équipes produit.

Le premier modèle est aligné avec la spécification de l'OWASP : https://owasp.org/www-project-security-culture/stable/4-Security_Champions/. Le second est principalement issu des retours d'expérience des membres de la communauté d'intérêt en lien avec ce groupe de travail.

Les implications de l'un et l'autre des modèles diffèrent et les deux sous-sections qui suivent visent à aborder les avantages et inconvénients de chacun des modèles. L'objectif est d'aider le lecteur à trouver des éléments clés lui permettant d'identifier l'approche la plus adaptée à son contexte.

A noter que, pour le cas particulier où un ETP (Equivalent Temps Plein) serait nécessaire et alloué pour gérer les tâches de Security Champion relatives à une équipe produit, les deux modèles se rejoignent.

### 4.3.1 Le Security Champion comme rôle spécifique à une équipe produit

**Dans ce premier modèle, les activités du Security Champion sont prises en charge par un membre de l'équipe produit.** La personne assumant ce rôle **se concentre essentiellement sur les activités relatives au produit** auquel elle contribue activement. Elle a un profil technique et dispose des compétences et de l'expérience que celui-ci exige. **Elle partage en premier lieu les enjeux de l'équipe dans laquelle elle est complètement intégrée,** en particulier ceux de qualité et de sécurité du produit, et **participe aux activités de développement (entres autres) au sein de cette équipe.** Il s'agit en général d'un développeur senior voire du « Tech Lead », ou dans certains cas de « l'architecte logiciel ».

Comme nous l'avons vu dans la section relative à La charge des activités du Security Champion et le dimensionnement, il est rare que les activités du Security Champion nécessitent un temps complet (ETP) pour une seule équipe produit. Cela réside en partie dans le fait que le Security Champion n'a pas vocation à assumer toutes les responsabilités et à gérer toutes les tâches de sécurité : Il se positionne comme référent sécurité au sein de l'équipe et agit en tant que « coach » afin de faire monter en compétence les autres membres sur les sujets de sécurité, tout en s'assurant qu'ils sont bien pris en compte. Ainsi, pour combler sa charge de travail en plus des activités de sécurité, **le Security Champion assume plusieurs types d'activité** (développement, architecture, tests, etc.) **au sein de son équipe produit**. Cela lui **permet de maintenir sa connaissance du produit et d'entretenir des compétences variées**.

**Un tel modèle organisationnel est généralement plus simple à mettre en œuvre pour une organisation ayant adopté l'agilité à l'échelle**. Le Security Champion est généralement désigné par ses pairs au sein de l'équipe (après s'être porté volontaire) ou nommé par la chefferie du projet.

Ce modèle opérationnel présente les avantages et inconvénients suivants :

| Avantages | Inconvénients |
|---|---|
| Le SC a une vision holistique du fonctionnement de son produit et de l'organisation de son équipe, ce qui peut lui permettre de détecter et traiter efficacement les problématiques de sécurité. | Le SC doit faire attention à ne pas s'enfermer dans une vision interne du produit et doit être en mesure de prendre le recul nécessaire à la détection et au traitement des problématiques de sécurité. |
| Faisant partie de l'équipe produit et partageant les enjeux du produit (et de son équipe), le SC est à même de prendre les décisions qui sont les plus propices à son bon développement.<br>Il est plus facilement accepté et reconnu par le reste de l'équipe. | Faisant partie de l'équipe produit, le SC peut être influencé par le responsable d'équipe ou par ses coéquipiers, pouvant altérer la bonne prise en compte des tâches techniques de sécurité. |
| Le SC ayant connaissance des enjeux globaux (métier et sécurité) de l'application, il est l'un des mieux placés pour arbitrer et prioriser entre les tâches fonctionnelles et les tâches techniques de sécurité.<br>Lors des rétrospectives, le tir peut être ajusté pour les prochaines itérations, en en discutant avec les autres membres de son équipe. | Il peut y avoir des conflits d'intérêt entre les tâches fonctionnelles (par exemple, développement d'une nouvelle fonctionnalité métier) et les tâches techniques de sécurité. Le SC doit prioriser les tâches en prenant en compte les besoins métier, les risques de sécurité, les ressources et les délais à respecter. |
| Le Security Champion peut se concentrer sur les activités en lien avec son équipe et son produit, il n'y a pas de « context switching » et de priorisation à faire entres différents produits. | Le Security Champion peut être en proie au « context switching » entre les activités de sécurité et les autres activités concernant son produit. |
| Le SC ayant capacité à réaliser des tâches diverses et variées (sécurité et autres), il peut mettre ses compétences au service de son équipe et de son produit de manière harmonieuse et efficace, ce qui peut s'avérer bénéfique pour son équipe et lui-même. | Le SC peut éprouver des difficultés à trouver un équilibre entre les différentes tâches qui lui incombent, si la charge allouée à chacune est trop faible ou diluée dans son quotidien.<br>Elles pourraient ne pas être correctement adressées, y compris celles de sécurité. |
| Quel que soit le projet/produit et son niveau de sensibilité, la sécurité est prise en compte (avec plus ou moins d'implication du SC selon les cas). | Au niveau de l'organisation, il peut être difficile d'identifier l'implication réelle nécessaire pour chaque produit/projet et d'ajuster le dispositif : Il y a dans tous les cas un SC par équipe, qui peut passer trop ou pas assez de temps sur les tâches de sécurité par rapport à ce qu'il faudrait. Cela peut occasionner un manque de vision et de gestion transverse de la sécurité. |
| Ce modèle favorise le développement et le maintien de compétences diverses et variées. | Il peut s'avérer compliqué pour le SC de monter efficacement en compétences sur les sujets de sécurité, dépendamment de son équipe et des enjeux de sécurité de son produit. |

### 4.3.2 Le Security Champion comme rôle transverse à plusieurs équipes produit

**Dans ce second modèle, les activités du Security Champion sont prises en charge par un membre transverse à plusieurs équipes produit**. La personne assumant ce rôle **se concentre essentiellement aux activités de sécurité concernant ces différents produits**. Elle a un profil technique et dispose des compétences et de l'expérience que celui-ci exige. **Elle partage en premier lieu les enjeux de Sécurité du Système d'Information (SSI) de l'organisation** à laquelle elle appartient, qu'elle essaye de retranscrire au sein des différents produits. **Elle participe peu au développement et autres activités des équipes produit, hormis celles ayant un lien avec la sécurité**. Il s'agit en général d'un spécialiste en Sécurité Applicative, ayant des connaissances en développement, tel qu'un auditeur ou intégrateur de sécurité, ou encore un « ancien » développeur expérimenté.

Comme nous l'avons vu dans la section relative à La charge des activités du Security Champion et le dimensionnement, il est rare que les activités du Security Champion nécessitent un temps complet (ETP) pour une seule équipe produit. Cela réside en partie dans le fait que le Security Champion n'a pas vocation à assumer toutes les responsabilités et à gérer toutes les tâches de sécurité : Il se positionne comme référent sécurité au sein des équipes et agit en tant que « coach » afin de faire monter en compétence les autres membres sur les sujets de sécurité, tout en s'assurant qu'ils sont bien pris en compte. Là où ce modèle diffère avec le précédent se situe dans le fait que **le Security Champion ne traite que les activités de sécurité pour plusieurs équipes/produits**. Il n'assume pas d'autres activités au sein des équipes produit, ce qui lui permet de **se concentrer uniquement sur la sécurité** et augmente de facto sa charge de travail sur cet aspect.

**Un tel modèle organisationnel est généralement plus simple à mettre en œuvre pour une organisation ayant une approche « Top-Down » de la sécurité et/ou n'ayant pas adopté l'agilité à l'échelle**. Le Security Champion est généralement nommé par le responsable de sécurité de son entité/organisation ou par la chefferie des projets auxquels il contribue.

Ce modèle opérationnel presente les avantages et inconvénients suivants :

| Avantages | Inconvénients |
|---|---|
| Le SC a la vision sur la sécurité de plusieurs équipes et produits, lui permettant de prendre du recul et de mutualiser les connaissances et les bonnes pratiques. Il peut détecter et traiter les problématiques de sécurité dans leur ensemble. | Le SC doit sanctuariser du temps pour chaque équipe, de manière à bien se synchroniser avec ses membres, et chaque produit, de manière à bien comprendre son fonctionnement et son évolution, au risque de survoler les sujets et de ne pas appréhender efficacement les problématiques de sécurité de chacun. |
| Etant transverse à plusieurs équipes et produits, le SC est généralement moins influencé par une équipe ou un responsable en particulier. Il est dans une situation favorisant l'objectivité des constats et analyses et moins propice aux conflits d'intérêts. | Ne faisant généralement partie d'aucune équipe produit (ou étant rattaché à plusieurs équipes à la fois), le SC peut ne pas bien partager les enjeux des produits auxquels il contribue et prendre des décisions uniquement au travers du prisme de la sécurité. Cela pourrait ralentir voire freiner le développement du produit, par excès de zèle. |
| Le SC se concentrant sur les tâches de sécurité, il est à même de les pousser au niveau des équipes produits, en adoptant une approche par le risque et la complexité de mise en œuvre et en faisant preuve de pédagogie. Lors des rétrospectives, le tir peut être ajusté pour les prochaines itérations, en discutant avec les équipes produit. | Le SC se concentrant sur les tâches de sécurité, il peut ne pas bien appréhender les autres tâches fonctionnelles et techniques relatives à la vie du produit. Il n'est pas bien placé pour arbitrer et prioriser les différentes tâches pour un même produit. |
| Le Security Champion peut se concentrer sur les activités de sécurité transverses à plusieurs produits, il n'y a pas de « context switching » entre les activités de sécurité et les autres activités des produits. | Le Security Champion peut être en proie au « context switching » et à des problématiques de priorisation à faire entres différents produits. Il peut avoir du mal à trouver un bon équilibre pour adresser les sujets de sécurité des différents produits. |
| La mise en place d'un SC transverse à plusieurs équipes permet de lisser sa charge de travail dans le temps. Par exemple, le SC peut être plus présent pour un produit lors de la phase de conception de celui-ci, puis une fois que l'organisation et les activités de sécurité sont bien définies et « sous-contrôle », il peut se concentrer sur un autre produit. | Il existe un risque de laisser de côté certains produits, en cas de manque de temps du SC ou de dépriorisation. Dans les meilleurs cas, seuls des produits peu sensibles seront mis de côté, néanmoins il peut arriver que des (petits) projets sensibles voient le jour pour lesquels la sécurité serait oubliée. |
| Ce modèle favorise la montée en compétences du SC sur les sujets de sécurité. | Il peut être compliqué pour le SC de maintenir ses compétences en développement et exploitation de logiciels. |

# 5. QUI EST LE SECURITY CHAMPION ?

## 5.1 PROFIL TYPE

Le Security Champion est une personne compétente en développement et possédant des connaissances générales (voire spécifiques selon les cas) en sécurité applicative pour pouvoir effectuer les activités de sécurité au sein de son/ses équipe(s) produit(s). Il n'est pas nécessairement expert en cybersécurité, comme le SME AppSec sur qui il peut compter lorsqu'il a besoin d'aide ou de conseils en la matière.

Le SC doit bien évidemment posséder d'excellente capacités d'analyse pour pouvoir qualifier et traiter efficacement les vulnérabilités remontées en cours de développement. Au-delà des compétences techniques nécessaires, certaines qualités de savoir-être sont également primordiales pour assumer ce rôle.

Le Security Champion occupe une position unique, possédant, figurativement parlant, un pied dans l'équipe de cybersécurité locale et un pied dans l'équipe de développement. Dans l'équipe de développement, il est le porte-étendard des enjeux sécuritaires et essaie de sensibiliser au mieux ses collègues aux bonnes pratiques de développement sécurisé. Il est aussi en communication permanente avec l'équipe de cybersécurité locale et/ou le SME AppSec (si son organisation en comporte un), vers qui il se tourne pour obtenir du support ou rapporter des statistiques sur l'évolution de la sécurité de son/ses application(s). Enfin, il doit s'investir en interne au sein de son organisation, typiquement en « faisant communauté » avec les autres Security Champions, pour partager ses connaissances et expériences et contribuer ainsi à la progression en maturité sur la sécurité de l'ensemble de l'organisation. Pour gérer ces situations, il doit être un bon communiquant et posséder des qualités pédagogiques afin de mieux sensibiliser ses collègues et conseiller ou former d'autres Security Champion à travers sa communauté.

Par conséquent, un développeur souhaitant découvrir le monde de la cybersécurité ou orienter sa carrière vers des sujets de cybersécurité serait un bon candidat pour devenir Security Champion. Un expert en cybersécurité ayant de bonnes connaissances en développement et souhaitant rester proche de l'opérationnel ou garder une forte composante technique dans son métier pourrait aussi être un bon candidat.

## 5.2 COMPÉTENCES RECHERCHÉES

Pour faciliter l'identification des compétences clés des SC et les besoins de formation qui en découlent, voici une proposition de panel de compétences pour un Security Champion, en trois niveaux :

**Niveau 'Débutant'**
L'emphase est mise sur les compétences fondamentales, indispensables à la bonne exécution des activités les plus critiques concernant le rôle de Security Champion, comme la revue du code ainsi que la qualification et le traitement des vulnérabilité remontées par les outils d'AST (Application Security Testing).

**Niveau 'Intermédiaire'**
Une fois que le Security Champion a plus d'expérience et est plus à l'aise avec ses responsabilités, il peut se concentrer sur l'acquisition de compétences pour mener à bien les activités les plus complexes du rôle comme la modélisation des menaces (Threat Modeling), les bonnes pratiques de sécurité de l'IaC (Infrastructure as Code) ou encore la gestion des secrets.

**Niveau 'Confirmé'**
A ce stade, le Security Champion possède une solide expérience et maîtrise bien l'ensemble de ses responsabilités. Il peut alors consacrer du temps au mentorat d'autres Security Champions et participer plus activement aux ateliers pour faire vivre la communauté de Security Champions.

Un Security Champion évolue donc naturellement de 'Débutant' à 'Confirmé' avec le temps et n'a pas besoin d'acquérir toutes les compétences identifiées pour son rôle d'un seul coup, ce qui serait impraticable.

Pour mieux visualiser les compétences essentielles pour débuter en tant que Security Champion puis celles pouvant être acquises au fur et à mesure de sa montée en expérience, voici une proposition de matrice de compétences montrant leur évolution (capable, compétent puis expert) à travers les trois niveaux d'expérience précédemment cités.

| | Security Champion 'Débutant' | Security Champion 'Intermédiaire' | Security Champion 'Confirmé' |
|---|---|---|---|
| **Compétences fonctionnelles et techniques** | | | |
| Fondamentaux DevOps | Capable | Compétent | Compétent |
| Fondamentaux de gestion des risques et des exigences de sécurité | Capable | Compétent | Compétent |
| Modélisation des menaces - Threat Modeling | - | Capable | Compétent |
| Fondamentaux en sécurité d'architecture | - | Capable | Compétent |
| Design patterns de sécurité | - | Capable | Compétent |
| Développement sécurisé et revue de code | Compétent | Compétent | Expert |
| Manipulation d'outils AST (Application Security Testing) | Compétent | Compétent | Expert |
| Gestion des vulnérabilités en environnement agile | Capable | Compétent | Compétent |
| Fondamentaux en Infrastructure as Code | - | Capable | Compétent |
| Fondamentaux en sécurité du Cloud | - | Capable | Compétent |
| Bonnes pratiques relatives à la pile technologique de l'équipe projet | - | Capable | Compétent |
| **Compétences comportementales** | | | |
| Autonomie et proactivité | Capable | Compétent | Expert |
| Esprit d'analyse et de synthèse | Compétent | Compétent | Expert |
| Aisance relationnelle et pédagogie | Capable | Compétent | Expert |
| Aisance rédactionnelle et communication | Compétent | Compétent | Expert |
| Capacité à diriger et à motiver l'équipe | - | Capable | Compétent |

Légende :

- **Expert** : Très grande expérience ou connaissances
- **Compétent** : bonne expérience ou connaissances
- **Capable** : peu d'expérience ou de connaissances
- | - | : pas d'expérience ou de connaissances

## 5.3 RECRUTEMENT ET FORMATION

Comme discuté dans Le rôle du Security Champion, le Security Champion est impliqué dans de nombreuses activités techniques liées à la sécurité au sein du cycle de vie de son ou ses produit(s) et il peut être audacieux de s'attendre à recruter des candidats possédants déjà toutes les compétences requises pour effectuer ces tâches. La façon la plus simple pour remédier à cela est de former des profils prometteurs. Malheureusement, il n'existe actuellement que très peu de formations (certifiantes) sur le marché qui sont dédiées à l'apprentissage du rôle de Security Champion. De plus, une partie non négligeable des activités liées au rôle dépend de l'environnement dans lequel le Security Champion évolue, comme la manipulation des outils d'AST (Application Security Testing) tels qu'ils ont été configurés dans l'entreprise ou bien la stratégie locale de traitement des vulnérabilités. Ces connaissances devront nécessairement être enseignées en interne.

En outre, le rôle de Security Champion est relativement nouveau car il est surtout présent dans les entreprises possédant une bonne maturité en sécurité applicative et plus particulièrement une stratégie 'shift-left' en cours d'implémentation. Ainsi, les profils de Security Champion déjà formés sont rares et leur recrutement peut se révéler compliqué. Ceux qui ont le plus d'expérience dans le domaine vont recevoir beaucoup d'offres tandis que les profils moins expérimentés mettront plus de temps à remplir correctement leurs responsabilités, feront plus d'erreurs et auront sûrement besoin de compléments de formations pour acquérir les compétences qui leur manquent.

Si le recrutement externe de Security Champions, via le marché du travail, peut être compliqué et lent, il est également possible de recruter des profils en interne en offrant des mobilités aux employés. Ces mobilités peuvent être verticales, un développeur souhaitant endosser les responsabilités supplémentaires d'un Security Champion pour se challenger et mettre un pied dans le domaine de la cybersécurité, ou bien horizontales, un expert en cybersécurité souhaitant diversifier son expérience ou avoir une composante plus technique ou proche de la production dans son travail. Ceci a un autre avantage : les personnes en interne connaissent déjà le contexte de leur organisation et éventuellement la/les application(s) qu'elles vont gérer en tant que Security Champion, leur permettant d'être plus rapidement efficaces.

Quelle que soit la méthode de recrutement, interne ou externe, il est important d'avoir défini clairement les responsabilités et les objectifs du Security Champion dans une fiche de rôle ou de poste et d'inclure le département des ressources humaines de l'organisation dans la discussion. C'est avec eux qu'il faudra réfléchir au profil type et aux compétences à privilégier pour le recrutement ou comment communiquer sur les possibilités de mobilité interne vers le rôle de Security Champion.

Au regard de ces différents défis, il apparaît comme essentiel de former en interne les profils issus de recrutement (interne ou externe), pour faciliter leur apprentissage du rôle et leur permettre de développer les Compétences recherchées du Security Champion. Comme pour le recrutement, il est important de construire les parcours et plans de formation avec le département des ressources humaines de l'organisation.

## 5.4 RÉTENTION DES PROFILS

Un effet de bord découlant de la volonté de former les Security Champions en interne est qu'en les faisant monter en compétence sur ce nouveau rôle émergeant, ils deviennent très attractifs sur le marché du travail et seront susceptibles d'être tentés de vendre leur nouvelle expertise au plus offrant. Il est donc important d'établir une stratégie de rétention des profils en place pour éviter que cela ne se produise souvent. L'objectif étant d'essayer de valoriser au maximum les talents nouvellement acquis des Security Champions pour les fidéliser et les impliquer dans la stratégie de l'entreprise.

Les Security Champions étant des profils plutôt techniques, ce souvent des personnes curieuses qui apprécient les défis. Il est possible de retenir leur intérêt en les objectivant financièrement sur leur montée en compétence pour atteindre les différents niveaux d'expérience en tant que Security Champion comme cités précédemment. Il est aussi utile de leur proposer des mobilités en interne pour pérenniser l'évolution de leur carrière au sein de l'entreprise et nourrir leurs ambitions. A terme, il peut être intéressant de proposer au(x) plus expérimenté(s) un poste de SME AppSec.

Il est également très important de les accompagner dans leur mission pour qu'ils n'aient pas l'impression d'être livrés à eux même mais qu'ils se sentent soutenus et faisant partie d'une communauté. Des évènements et ateliers peuvent être organisés pour maintenir leur intérêt dans leur rôle et les faire monter en compétence par la même occasion.

# 6. LE RÔLE DU SUBJECT MATTER EXPERT (SME) APPSEC

Pour rappel, le SME AppSec est un expert technique qui facilite la résolution des problèmes de Sécurité Applicative et DevSecOps, ainsi que la centralisation des connaissances concernant leurs solutions, afin d'apporter les réponses les plus cohérentes possibles sur ces sujets à tous les Security Champions de son organisation. Il accompagne les Security Champions dans leur montée en compétences. Le besoin concernant le rôle de SME AppSec est détaillé dans Pourquoi le Subject Matter Expert (SME) ?.

## 6.1 LES ACTIVITÉS DU SME APPSEC

Cette section consiste à lister les activités typiques réalisées par un SME AppSec. Attention toutefois, différentes organisations définissent différents ensembles d'activités pour le SME. Il s'agit là d'une proposition générique, qui n'est pas forcément exhaustive, et qui a tout intérêt à être contextualisée en fonction de l'organisation, de ses processus et de sa culture.

A noter que les activités de sécurité pour un périmètre transverse (plusieurs produits ou même l'ensemble de l'organisation) sont définies dans le RACI, annexe du présent document. Le SME AppSec est l'un des principaux interlocuteurs pour mener à bien ces activités transverses de sécurité.

Les activités du SME AppSec peuvent inclure :

⟶ **L'élaboration de la stratégie de sécurité applicative**

- Définition d'un programme de Sécurité Applicative et sa feuille de route, établissant un modèle opérationnel avec les parties prenantes, leurs rôles et responsabilités, les activités à mettre en place (BUILD), l'exploitation et la maintenance de ces activités (RUN), les outils transverses déployés, les étapes successives sur du court-moyen-long terme, etc..
- Identification des enjeux et des besoins de sécurité des produits de l'organisation, définition des exigences globales de sécurité, analyse des risques de sécurité transverses aux produits, conception d'architectures applicatives de référence incorporant les exigences et les risques de sécurité identifiés.
- Elaboration de la politique de Sécurité Applicative globale, en indiquant les niveaux de sécurité à atteindre en fonction des typologies d'application (sensibilité, architecture, etc.) et éventuellement des niveaux de maturité de sécurité des équipes, en listant les activités pour les atteindre (méthodologies, processus, outillage, etc.), en établissant ce qui est accepté pour une livraison et/ou une mise en production et ce qui ne l'est pas, en définissant les indicateurs clés de suivi correspondants.
- Proposition de chaine(s) CI/CD type(s) visant à implémenter la politique de Sécurité Applicative globale et intégrant les activités de sécurité préalablement définies.

- Préparation des plans et des parcours de sensibilisation/formation à la Sécurité Applicative, en fonction des profils cibles, ainsi que des supports de formation (diapositives, Labs d'entrainement, environnements/matériels spécifiques, etc.).
- Préparation des programmes d'audit de sécurité (revues d'architecture, de code, des configurations, tests d'intrusion) et de Bug Bounty.
- Mise en place d'une communauté de Sécurité Applicative, regroupant a minima le(s) SME AppSec et les Security Champions, ainsi que toutes les parties prenantes intéressées dans la démarche (notamment les développeurs), pour favoriser les échanges, le partage des documentations, des guides, des bonnes pratiques et des solutions aux problèmes connus.

⟶ **La mise en œuvre de la stratégie de sécurité**

- Implémentation des étapes de la feuille de route du programme de Sécurité Applicative.
- Dispense des sessions de sensibilisation (pour toute partie prenante et toute personne intéressée par la démarche de Sécurité Applicative) et de formation (pour les Security Champions, les développeurs, les testeurs, les exploitants, etc.), selon les plans de formation définis préalablement, sur des sujets tels que les principaux risques de sécurité applicative, l'exploitation des vulnérabilités, la mise en place des remédiations, le développement sécurisé, les activités de sécurité qui peuvent/doivent être intégrées dans le cycle de vie des produits, la mise en place des outils et l'intégration dans les chaines CICD.
- Animation de la communauté de Sécurité Applicative (organisation d'événements, de tables rondes, partage d'informations/communications, etc.) et gestion de la contribution au sein de cette communauté, en organisant le partage des connaissances et des solutions aux problèmes connus, le support aux personnes (en particulier les Security Champions) qui viendraient solliciter de l'aide, la mise en place de formations sur des sujets spécifiques évoqués lors des tables rondes, etc..
- Mise à jour régulière des référentiels de sécurité (exigences, architectures, politiques, chaines CI/CD types, guides, supports de formation, etc.).
- Gestion de la maintenance des plateformes et outils de Sécurité Applicative (SAST, SCA, DAST, IAST, RASP, analyse des conteneurs, des modèles d'IaC, des APIs, des secrets, etc.)
- Récolte (automatisée) et centralisation des indicateurs clés de suivi des différents produits et équipes.
- Gestion des audits de sécurité et programmes de Bug Bounty.
- Participer à la gestion des risques de sécurité transverses, en particulier les risques résiduels qui n'ont pas pu être complètement traités à la suite de l'analyse des risques, à la gestion des vulnérabilités transverses et des contre-mesures au niveau de l'organisation.

### → Le soutien aux contrôles et validations de sécurité

- Suivi des étapes de la feuille de route du programme de Sécurité Applicative.
- Contrôle du traitement, au sein des produits, des risques, défauts, vulnérabilités et de l'implémentation des mesures permettant de répondre aux exigences de sécurité, en particulier pour les applications les plus sensibles et les équipes ayant le plus besoin d'accompagnement.
- Contrôle de l'inventaire des applications et de leurs composants (approche SBOM).
- Contrôle de l'implémentation des activités de sécurité au sein des chaines CI/CD des produits et de l'utilisation des outils de Sécurité Applicative par les équipes produit.
- Contrôle du respect et de l'implémentation de la politique de Sécurité Applicative au niveau des produits, suivi des indicateurs clés de sécurité et remontée des informations aux décideurs, au Responsable de la Sécurité des Systèmes d'Information et à la DSI.
- Validation de sécurité des applications en fonction des résultats des audits de sécurité et des programmes de Bug Bounty, entres autres.

Au travers de ces activités, ce qu'il faut surtout retenir est le soutien qu'apporte le SME AppSec à la communauté de Sécurité Applicative, en particulier à l'ensemble des Security Champions de l'organisation, sur des sujets tels que :

- La compréhension et la résolution des problèmes de Sécurité Applicative (méthodologie d'analyse et de remédiation, compréhension d'une vulnérabilité particulière, état de l'art et bonnes pratiques, etc.) ;
- La mise en place des processus de sécurité (Threat Modeling – modélisation des menaces, gestion des exigences et mesures de sécurité, scan statique/dynamique/hybride des vulnérabilités, gestion des dépendances / approche SBOM, gestion des configurations, etc.) ;
- La mise en place des outils de sécurité (plateforme de gestion des risques/vulnérabilités, outil de modélisation de l'architecture et des menaces, SAST, DAST, SCA, IAST, RASP, scan de la sécurité des API, des modèles IaC, des conteneurs, etc.).

**Concernant l'animation de la communauté de Sécurité Applicative :**

- Quels que soient les outils utilisés pour supporter cette communauté (généralement cela implique au moins la mise à disposition d'une plateforme favorisant la communication et d'un Wiki), elle permet d'échanger (messages instantanés ou « posts », appels et visioconférences, etc.), de partager des ressources (documents de travail, études, exemples de configuration ou d'analyse, méthodologies d'analyse, plans de remédiations types, etc.), d'organiser des événements (sensibilisations, formations, ateliers techniques et pratiques, retours d'expérience thématiques, défis de hacking ou de secure coding, afterworks, etc.).

- Elle permet aussi de répondre aux demandes d'information et d'assistance (typiquement des Security Champions vers le SME), ainsi que de partager les communications et directives de l'organisation vers les équipes produit, telles que la politique de Sécurité Applicative, les exigences de sécurité à prendre en compte, les architectures de référence, des notes d'information sur les actualités et tendances Cyber (vulnérabilités publiques, attaques, APT, etc.), etc.

**Le SME AppSec peut aussi participer aux activités suivantes :**

- Participation ponctuelle, voire exceptionnelle (dépendamment du niveau de sensibilité de l'application et/ou de maturité de l'équipe produit) aux phases d'analyse des risques, de définition des exigences de sécurité, de modélisation des menaces, de conception, de construction, de validation de sécurité de certaines applications / MVP.
- Participation aux phases de prospection et avant-vente pour des marchés ayant des enjeux de Sécurité Applicative et gestion opérationnelle des contrats qui en découlent.
- Participation plus ou moins active au sein des communautés de développement, de DevOps, d'architectes, présentes au sein de l'organisation.
- Participation au sein des communautés de Sécurité Applicative et DevSecOps extérieures à l'organisation, dans le cadre de la veille technique et technologique que le SME AppSec doit mener régulièrement et, éventuellement, pour représenter son organisation lors d'événements importants et construire son réseau avec des confrères SME et SC (entres autres) appartenant à d'autres organisations.

## 6.2 LA CHARGE DES ACTIVITÉS DU SME APPSEC ET LE DIMENSIONNEMENT

Les activités relatives à la sécurité du SME AppSec lui prennent généralement tout son temps, sauf éventuellement pour des organisations de petite taille. Le rôle de SME AppSec est donc un rôle à temps plein qui devrait faire l'objet d'une fiche de poste à part entière.

Il peut y avoir plusieurs SME AppSec au sein d'une seule et même organisation. Cela dépend généralement de la taille de l'organisation et de ses enjeux et objectifs de Sécurité Applicative. Plus le nombre de SME AppSec est élevé, plus les problématiques de Sécurité Applicative sont traitées en anticipation et meilleur est l'accompagnement proposé aux Security Champions, en particulier sur les sujets spécifiques et potentiellement complexes concernant leur(s) produit(s).

## 6.3 LE PRINCIPAL MODÈLE ORGANISATIONNEL POUR LE SME APPSEC

A contrario des Security Champions, les SME AppSec ne font pas partie d'une (ou plusieurs) équipe(s) produit. En général, ils sont rattachés au service du RSSI. Ils interagissent régulièrement avec les autres SME, les équipes d'audit, les équipes ISP, les équipes en charge des plateformes numériques (Cloud ou On-Premises) et des outils AppSec et DevSecOps, les équipes en charge de l'industrialisation des chaines CI/CD, les équipes de gouvernance, de sécurité opérationnelle, etc.

Néanmoins, cela ne doit pas leur faire perdre de vue les objectifs fonctionnels et métier des produits sur lesquels ils interviennent indirectement, généralement au travers de l'aide qu'ils apportent aux Security Champions.

# 7. QUI EST LE SUBJECT MATTER EXPERT (SME) APPSEC ?

## 7.1 PROFIL TYPE

LE SME AppSec a besoin de connaissances et compétences techniques, transverses et fonctionnelles. Il est intéressant qu'il ait aussi des connaissances métier fines, sans que cela ne soit une obligation. En effet, en abordant les problèmes d'un point de vue technique, il lui sera toujours possible de prodiguer des conseils avisés que les développeurs sauront adapter au contexte métier. Cependant, une polyvalence et une adaptabilité dans les connaissances et dans les compréhensions d'architecture sont nécessaires, afin de comprendre les spécificités de chacun des cas auxquels il peut être confronté.

Il est également nécessaire d'avoir un esprit de synthèse et rédactionnel afin de mettre à plat les idées nécessaires à la création de documentations à destination des développeurs. Dans cette même veine, des compétences pédagogiques peuvent être bénéfiques, assurant ainsi une meilleure compréhension des sujets abordés par ses interlocuteurs du fait de l'application de méthodes d'apprentissage éprouvées.

Le rôle de SME AppSec doit être incarné par une personne ayant développé une expertise importante en Cybersécurité (en particulier la Sécurité Applicative) et une compréhension avancée des pratiques de développement, intégration et exploitation des logiciels (de surcroit dans un contexte agile).

**Il s'agit généralement soit :**

- D'un profil de type spécialiste en Cybersécurité, s'étant fortement intéressé au domaine du développement logiciel et au SDLC ;
  - En venant d'une équipe dédiée à la sécurité, s'intéresser aux problématiques de Sécurité Applicative et accompagner régulièrement des équipes métier/produit en recherchant des solutions adaptées à leur contexte, permet d'acquérir l'expertise nécessaire au rôle de SME AppSec.

- D'un ancien développeur confirmé et/ou Security Champion, s'étant passionné pour les sujets de sécurité et ayant ainsi développé des compétences importantes dans ce domaine.
  - Une bonne source d'apprentissage dans un contexte agile est d'avoir été Security champion pendant plusieurs années et d'avoir ainsi été au contact de SME et de la sécurité suffisamment longtemps.

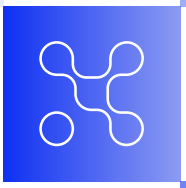
L'expertise s'acquiert principalement par l'expérience. Il ne sera pas possible d'obtenir des SME à partir d'une simple formation. Il est en revanche important de continuer à former les SME, soit en leur accordant du temps pour s'auto-documenter et faire une veille technique et technologique, soit en leur proposant des formations avancées.

## 7.2 COMPÉTENCES RECHERCHÉES

Le SME AppSec est essentiellement expérimenté en sécurité des applications.

**Ainsi, il a généralement des connaissances et compétences poussées concernant :**

- Les programmes de Sécurité Applicative / DevSecOps à l'échelle d'une organisation (stratégie, feuille de route, étapes, déclinaison opérationnelle, pilotage, etc.).
- Les activités de sécurité au sein du SDLC – cycle de vie des applications, les moyens de les mettre en œuvre (quels processus/outils) et de les exploiter.
- La gestion des risques et des exigences de sécurité portant sur les applications, ainsi que la validation de sécurité.
- La modélisation des menaces et les architectures logicielles (N-tiers, On-Premises, Cloud, IaaS, PaaS, SaaS, CaaS, Micro services, Mobile, etc.).
- La mise en place des solutions technologiques de test de sécurité applicative (SAST, SCA, DAST, IAST, RASP, analyse des conteneurs et des modèles IaC, détection des secrets, etc.), notamment dans les environnements agiles et les chaînes CI/CD, et leur utilisation avancée.
- Les langages, frameworks et autres technologies de programmation et de déploiement des applications utilisées au sein de l'organisation.
- Les analyses de sécurité, telles que l'analyse de la sécurité de l'architecture, du code source et de la configuration d'une application, la capacité à mener des tests d'intrusion applicatifs/externes/web.
- L'accompagnement au traitement des vulnérabilités applicatives (analyse technique, recommandations de remédiation, vulgarisation, contre-audits…).
- La sensibilisation et la formation (théorique et pratique) sur la Sécurité Applicative, les risques de sécurité, l'exploitation des vulnérabilités et les moyens d'y remédier, le développement sécurisé, l'intégration des outils dans les chaines CI/CD.



- Les méthodologies agiles de gestion de projet, l'approche Dev(Sec)Ops et les technologies émergentes (Conteneurisation, Configuration as Code, Infrastructure as Code, architectures micro-services, architecture Cloud, etc.).

**En outre, le SME AppSec dispose des compétences comportementales suivantes :**

- Grande autonomie et capacité d'adaptation à des contextes nouveaux ;
  - Cela implique que, même s'il n'a pas immédiatement la solution à un problème donné, il met en œuvre des moyens pour le résoudre ou déterminer une stratégie de contournement, en creusant le sujet et en cherchant au sein des sources d'information internes (documentations, autres SME, etc.) et externes (sites et articles, communautés de Sécurité Applicative, événements, etc.).

- Esprit d'analyse et de synthèse ;
- Communication (à des publics divers et variés, techniques ou non) écrite et orale ;
- Capacité à partager et retranscrire des connaissances - pédagogie ;
- Animation communautaire.

De plus, comme pour tout métier relatif au domaine de la sécurité, le SME AppSec doit être curieux et se tenir informé des actualités Cyber (vulnérabilités, attaques, découvertes en matière d'exploitation et de remédiation, frameworks de développement, etc.).

## 7.3 RECRUTEMENT ET FORMATION

Le recrutement interne et le recrutement externe proposent tous les deux des bénéfices pour le rôle de SME AppSec :

- Interne ⟶ Connaissance du SI et du fonctionnement de l'organisation plus complète.
- Externe ⟶ Apport d'un regard extérieur et de connaissances nouvelles.

La principale difficulté du recrutement interne est de trouver une personne disposant du Profil type et de compétences parmi celles recherchées (ou au moins de prédispositions) au sein de l'organisation. La principale difficulté du recrutement externe est d'attirer ce type de profil, ce qui nécessite de pouvoir faire une offre pertinente et adaptée. Dans les deux cas, l'organisation doit fournir des efforts pour rester compétitive et fidéliser le profil retenu.

Quelle que soit la méthode de recrutement (interne ou externe), le rôle de SME AppSec devrait faire l'objet d'un poste à part entière, dont il est important de définir clairement les responsabilités et les objectifs conjointement avec le département des ressources humaines de l'organisation.

C'est aussi avec les Ressources Humaines qu'il faudra réfléchir au profil type et aux compétences à privilégier pour le recrutement ou comment communiquer sur les possibilités de mobilité interne vers le rôle de SME AppSec (par exemple depuis un rôle de Security Champion confirmé).

Le besoin en formation interne est moins important que celui relatif au rôle de Security Champion, dans la mesure où une même organisation compte moins de SME AppSec que de SC. De surcroit, le SME AppSec est déjà censé disposer de compétences avancées qu'il est capable de faire évoluer de manière autonome. Ceci étant dit, il est important de réfléchir aux parcours et plans de formation avec le département des ressources humaines de l'organisation.

## 7.4 RÉTENTION DES PROFILS

Le SME AppSec a un profil versatile disposant d'une forte expertise technique, confirmée après des années d'expérience en tant que développeur et/ou Security Champion confirmé et/ou spécialiste en Cybersécurité. Il occupe un poste d'autant plus sensible et stratégique que l'organisation dispose d'applications elles-même sensibles et stratégiques.Par conséquent, il s'agit d'un poste qui devrait être valorisé pour éviter un risque de départ anticipé pouvant avoir un impact néfaste important sur la stratégie de sécurité de l'organisation.

# 8. ÉLÉMENTS CLÉS DE PERFORMANCE

Déployer un modèle opérationnel avec des Security Champions n'est pas une décision triviale pour une organisation. Cela implique une planification longue et minutieuse. Une multitude de questions doivent être adressées avant de tenter un déploiement. L'ajout d'un rôle supplémentaire au sein des équipes de développement peut être un changement important pour certains, les bénéfices du modèle peuvent mettre du temps à arriver et ne sont pas faciles à mettre en exergue auprès des décideurs.

Néanmoins, voici quelques conseils sur les points clés auxquels prêter attention si l'on souhaite se lancer dans un tel projet.

**Le Shift-left dans l'agilité sans Security Champions**

- La vitesse de livraison dépend des développeurs qui ne sont pas des experts en sécurité, ils ne peuvent traiter correctement la sécurité de leur code du jour au lendemain sans aménagement et accompagnement spécifiques.
- Le département de sécurité bloque car ne peut pas suivre le rythme des livraisons (difficultés de recrutement + explosion de la quantité de travail).
- Le nombre de vulnérabilités relatives à la sortie fréquente de nouvelles fonctionnalités peut augmenter, ce qui augmente par conséquent l'exposition du parc applicatif aux menaces.

**L'importance du parrainage**

- Il est fondamental d'avoir le soutien de la Direction ET du RSSI dès le début car un modèle Security Champion demande des efforts en ressources et introduit des changements pas forcément appréciés, donc les avoir en support peut débloquer des situations épineuses.
- Fait partie intégrante du programme de Sécurité Applicative de l'organisation, qui ne doit pas être perçu comme un projet à part ou isolé.

**Mesurer l'impact des Security Champions sur la sécurité applicative**

- Pour vérifier l'efficacité du modèle, il est important de mesurer l'impact qu'ont les Security Champions sur la maturité en sécurité applicative de l'organisation.
- Pour cela, il faut définir des indicateurs clés de performance et les suivre dans le temps.
- Ces indicateurs permettent de voir si le modèle est correctement déployé et de faire des ajustements.
- Ils permettent de justifier la pertinence du modèle, ainsi que de rassurer la Direction et les autres parties prenantes.

**Exemples d'indicateurs clés pour mesurer l'efficacité du modèle Security Champion**

- Couverture du parc applicatif
  - Nombre total d'applications
  - Nombre d'applications éligibles aux scans des outils d'AST (compatibilité avec les langages supportés par les outils par exemple)
  - Nombre d'applications actuellement scannées via les outils d'AST

- Avancement de la sécurité du parc applicatif
  - Nombre de vulnérabilités non qualifiées (backlog)
  - Nombre de vulnérabilités qualifiées
  - Nombre de vulnérabilités traitées

- Déploiement du modèle
  - Nombre de Security Champions VS le besoin
  - Nombre de sessions de sensibilisation ou formation dispensées
  - Nombre d'articles ou de sections de documentation de sécurité rédigés

# 9. ÉCUEILS POSSIBLES ET POINTS DE VIGILANCE

Les SME et les Security Champions sont essentiels pour assurer une intégration efficace de la sécurité dans le cycle de vie du logiciel. Il est recommandé de s'appuyer sur des Security Champions pour promouvoir et améliorer les pratiques de sécurité au sein des équipes de développement. Toutefois, la mise en place et le suivi des Security Champions ne sont pas sans défis, et il faut éviter certains pièges pour garantir le succès du programme AppSec. Dans cette section, à l'aide des retours d'expérience de la communauté d'intérêt et des membres de ce GT, nous allons présenter les écueils identifiés, des solutions possibles pour les prévenir ou les surmonter, ainsi que les points de vigilance liés aux activités des SME et des Security Champions.

## 9.1 OBSTACLE 1 : MANQUE DE SOUTIEN DE LA DSI, DE LA CYBERSÉCURITÉ OU DU MÉTIER

Causes possibles :

- La direction et/ou les équipes manquent de maturité sur les risques et les enjeux liés à la cybersécurité.
- Il n'existe pas de preuve tangible de l'intérêt de mettre en place des security champions.
- Les équipes métier et de développement ne reconnaissent pas la valeur de son rôle ni ses besoins.

Solutions envisageables :

- Sensibiliser les équipes dirigeantes, métier et de développement aux enjeux de la cybersécurité par des communications, des présentations et des sessions de vulgarisation.
- Définir des indicateurs clés de performance (KPI) et des métriques pour mesurer l'efficacité des activités de sécurité.
- Tester le programme AppSec sur un pilote ou un échantillon de projets pour démontrer la valeur ajoutée de l'intégration de la sécurité et du Security Champion.

## 9.2 OBSTACLE 2 : FORMATION INSUFFISANTE DES ÉQUIPES DE DEV/OPS

Causes possibles :

- Temps contraint qui empêche les équipes de se consacrer à la formation sans nuire à la productivité et aux délais.
- Volonté de ne pas prioriser l'investissement dans la formation.
- Gouvernance et répartition budgétaire des activités de formation (les équipes RH ne sont pas suffisamment sollicitées).
- Le recours à des prestataires externes limite la possibilité de les former (risque de requalification du contrat de travail, prise en charge des coûts, etc.).

Solutions envisageables :

- Inscrire la formation au même titre que les autres activités du projet.
- Prioriser les formations et les sensibilisations pour les équipes projets les plus sensibles.
- Coordonner les formations avec le service des ressources humaines.
- Exiger des garanties et des justificatifs de la part des prestataires.

## 9.3 OBSTACLE 3 : RESSOURCES TEMPORELLES LIMITÉES POUR MENER LES ACTIVITÉS DU SECURITY CHAMPION

Causes possibles :

- Les activités du Security Champion sont mal définies ou inexistantes, ce qui rend difficile leur planification et leur suivi.
- La charge de travail du Security Champion pour les activités de sécurité n'est pas bien évaluée ou sanctuarisée. Les autres tâches peuvent alors venir empiéter sur ces activités, ce qui réduit son efficacité et sa motivation.

Solutions envisageables :

- Etablir clairement un RACI (Responsible, Accountable, Consulted, Informed) pour les activités de sécurité au sein du projet, définissant le rôle du Security Champion ainsi que les interactions avec toutes les parties prenantes (Subject Matter Expert AppSec, équipes produit, équipe de Cybersécurité, etc.).
- Evaluer la charge de manière pragmatique et sanctuariser le temps dédié aux activités liées à la sécurité.
- Former le Security Champion à communiquer efficacement sur son rôle, ses objectifs et ses résultats, ou recruter un Security Champion ayant déjà ces compétences.
- Se concentrer sur les applications les plus critiques/sensibles pour le fonctionnement de l'entreprise.

## 9.4 OBSTACLE 4 : RESSOURCES HUMAINES LIMITÉES POUR PRENDRE LE RÔLE DE SECURITY CHAMPION

Causes possibles :

- Absence de volontariat et/ou nomination imposée des Security Champions.
- Les potentiels Security Champions manquent de temps pour assumer ce rôle en plus de leurs activités habituelles.
- Ils ignorent le rôle, les actions et les responsabilités d'un Security Champion, ce qui les rend réticents à s'engager.
- Ils ne perçoivent pas de contrepartie à leur investissement, ni de reconnaissance de la part de leur hiérarchie ou de leurs pairs.
- Equipes RH peu sensibilisées aux métiers et compétences de la sécurité.
- Le recrutement interne n'est pas toujours envisagé ou n'est pas priorisé.

Solutions envisageables :

- Etablir clairement un RACI (Responsible, Accountable, Consulted, Informed) pour les activités de sécurité au sein du projet, définissant le rôle du Security Champion ainsi que les interactions avec toutes les parties prenantes (Subject Matter Expert AppSec, équipes produit, équipe de Cybersécurité, etc.).
- Fournir un accompagnement et un suivi rapproché des Security Champions juniors, pour les former et les soutenir dans leur montée en compétences.
- Animer une communauté de Security Champions, pour favoriser les échanges de bonnes pratiques, les retours d'expérience et la reconnaissance mutuelle.
- Sensibiliser les RH aux métiers et aux compétences de la sécurité.
- Considérer le recrutement interne de profils qui disposent des prérequis et connaissent déjà le fonctionnement de l'organisation, son métier, ses environnements techniques.
- Mettre en avant l'investissement des Security Champions lors des cycles RH et des entretiens professionnels, afin de reconnaitre leur travail à tous les niveaux (responsabilité, organigramme, etc.) et le prendre en compte pour les revalorisations salariales.

## 9.5 POINTS DE VIGILANCE

- Disposer des bons KPIs et métriques pour évaluer la performance des activités de sécurité.
- Clarifier les interactions entre le Security Champion et les autres équipes.
- Fournir un accompagnement et un suivi rapproché des Security Champions junior.
- Préférer des profils techniques Dev, QA ou Ops pour endosser le rôle du Security Champion.
- Avoir un Security Champion sachant communiquer, ou le former.
- Éprouver le programme AppSec à travers un pilote avant de le déployer pour tous les projets.
- Assurer la mise en place, la gestion et la maintenance d'une base de connaissances.
- Animer une communauté Security Champions.

# 10. CONCLUSION

L'agilité a changé la manière de concevoir, développer, déployer et maintenir des logiciels, forçant la sécurité à s'adapter aux nouveaux enjeux qui en découlent.

Pour s'adapter au fonctionnement des méthodologies agiles (itérations courtes, changements fréquents, assouplissement du périmètre, livraisons régulières, etc.), la démarche de sécurisation nécessite un remaniement profond, afin que la sécurité soit prise en compte à tous les niveaux et dans toutes les phases du SDLC (Software Development Life Cycle).

Une pierre angulaire de ce remaniement consiste en une appropriation des activités de sécurité par les équipes produit, à l'instar des autres activités fonctionnelles et techniques, facilitée par la mise en place de modèles organisationnels basés sur deux rôles : Le Security Champion, agissant au niveau des équipes produit, et le SME (Subject Matter Expert) AppSec, agissant de manière traverse au sein de l'organisation. De cette manière, la sécurité est embarquée dans les contextes agiles des produits et, dans la mesure du possible, à l'échelle de l'organisation.

Le Security Champion est généralement un développeur qui accompagne le reste de son (ou de ses) équipe(s) produit dans la gestion des tâches de sécurité, tout en continuant d'effectuer d'autres tâches pour son produit (cas du 1er modèle organisationnel) ou se concentrant sur les tâches de sécurité de 3-4 produits différents (cas du 2nd modèle organisationnel). Dans tous les cas, les Security Champions assurent la bonne prise en compte de la sécurité au sein des produits et de leur cycle de vie, en l'insérant dans les pratiques agiles des équipes qui les développent et en sensibilisant par la même occasion les membres de ces équipes. Le Security Champion est le point de contact privilégié pour les questions de sécurité concernant son ou ses produit(s). Il y coordonne les activités de sécurité et promeut les bonnes pratiques.

Le SME AppSec est un expert en Sécurité Applicative sur lequel se reposent les Security Champions si besoin d'assistance (en cas de problème complexe, d'un conseil concernant la gestion d'une vulnérabilité ou la mise en place d'une remédiation, l'utilisation d'un outil d'analyse de sécurité applicative - AST, etc.). Le SME AppSec réalise des activités de sécurité transverses à l'organisation, pouvant servir de base à la démarche de sécurité déclinée au niveau des produits par les Security Champions. Il peut gérer et animer une communauté de Sécurité Applicative interne regroupant, a minima, les Security Champions, s'assurer du partage des bonnes pratiques au travers de référentiels de sécurité, du partage d'informations et de la dispense de sessions de formations.

Généralement, un développeur peut devenir Security Champion si la sécurité l'intéresse et s'il dispose des compétences nécessaires pour ce rôle, tandis que ce sont généralement des spécialistes en Cybersécurité ou d'anciens Security Champions qui endossent le rôle de SME AppSec. Il ne s'agit pas d'une règle inscrite dans le marbre et différents cas de figure sont envisageables. Le plus important est de s'assurer que les Security Champions et le(s) SME AppSec disposent des compétences techniques, fonctionnelles et comportementales attendues pour assumer leur rôle, ou ont la capacité de les développer efficacement.

Déployer un modèle opérationnel avec des Security Champions n'est pas une décision triviale pour une organisation. Une multitude de considérations sont à prendre en compte telles que la culture de l'organisation, la place de la sécurité dans sa stratégie, le soutien/parrainage de personnes influentes, la formation des parties prenantes, le manque de ressources et de temps pour réaliser les activités de sécurité, etc.
Les bénéfices du modèle peuvent mettre du temps à arriver et ne sont pas faciles à mettre en exergue auprès des décideurs, d'où l'importance de la mise en place et du suivi d'éléments clés de performance au cours du temps.

# REMERCIEMENTS

Ce livrable a été produit dans le cadre du groupe de travail Cybersécurité Agile - Stream Security Champions & SME AppSec.

Coordinateur du stream : Antoine RICHER, ACCENTURE

Contributeurs :

Benjamin CHOBERT, BNPP
François-Xavier DE BOUËT DU PORTAL, EURO-INFORMATION
Jean-Christophe DELABARRE, I-TRACING
Olivier DUPUY D'UBY, IBM
Marie MOIN, EPITA
Quentin NICOLAS, BNPP
Victor PINSEMBERT, BNPP
Benoît TRINITE, RENAULT

< Studio des Communs >

CAMPUS CYBER

POUR EN SAVOIR PLUS : **WIKI.CAMPUSCYBER.FR**
ADRESSE MAIL DE CONTACT : **COMMUNAUTES@CAMPUSCYBER.FR**
5 - 7 RUE BELLINI 92800, PUTEAUX



CE PROJET A ÉTÉ FINANCÉ PAR LE GOUVERNEMENT DANS LE CADRE
DU PROGRAMME D'INVESTISSEMENTS D'AVENIR