AGILITÉ & SÉCURITÉ NUMÉRIQUES

Méthode et outils à l'usage des équipes projet

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Direction interministérielle du numérique et du système d'information et de communication de l'État

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

SOMMAIRE

AGILITÉ & SÉCURITÉ NUMÉRIQUES

Méthode et outils à l'usage des équipes projet

PRÉFACE

La maîtrise pleine et entière du numérique – de ses programmes, de ses outils, de ses méthodes et même de ses codes – est aujourd'hui une dimension essentielle de la sécurité et de la souveraineté. L'État, au même titre que les entreprises, ne peut se contenter d'être le consommateur passif de solutions développées par d'autres, pas plus qu'il ne peut se satisfaire d'anciennes méthodes et de protocoles figés.

C'est pourquoi l'agilité et la sécurité doivent désormais être intégrées, au plus tôt et en permanence, dans la conduite de projets et ainsi nourrir efficacement la prévention des risques numériques et la détection des cyberattaques. Si l'idée fait son chemin, sa mise en œuvre tarde encore à se généraliser.

C'est donc avec beaucoup d'enthousiasme que l'ANSSI et la DINSIC ont décidé de conjuguer leurs expertises respectives en matière de sécurité numérique et de gestion de projet agile pour proposer une méthodologie commune résolument pratique et concrète.

Pour la DINSIC, la sécurité des services dématérialisés qu'elle développe est une valeur cardinale qui conditionne l'efficacité de tout projet, la sûreté de l'État et, bien souvent, la protection de la vie privée des citoyens. Pour l'ANSSI, l'agilité est un impératif face à un état de la menace en mouvement permanent.

La méthode que propose ce document repose donc avant tout sur l'expérience de celles et ceux qui, conscients de la valeur de cette alliance, la mettent en œuvre et la font évoluer à chaque nouveau projet. Pour preuve, le cœur de la démarche repose sur l'organisation d'ateliers d'appréciation des risques et prépare efficacement à l'homologation des services numériques et applications.

Nous tenons à remercier nos équipes qui ont su partager et enrichir leurs convictions et priorités respectives ainsi que tous ceux qui, par leur participation à l'appel à commentaires, ont fait de ce guide un outil qui saura faire écho à la réalité des équipes projet !

Guillaume Poupard
Directeur général de l'Agence nationale
de la sécurité des systèmes d'information (ANSSI)

Henri Verdier
Directeur interministériel du numérique et du système
d'information et de communication de l'État (DINSIC)

1 À QUI S'ADRESSE CE GUIDE ?

À QUI S'ADRESSE CE GUIDE ?

Intitulé *« Agilité & sécurité numériques – Méthode et outils à l'usage des équipes projet »*, ce guide explique de manière pratique et concrète aux équipes d'entités publiques et privées comment conduire un développement numérique dans le cadre d'une *équipe agile* tout en considérant le volet *sécurité*.

De l'analyse au traitement des risques numériques, des fiches mémo, exemples et ressources documentaires **vous accompagnent pas à pas dans le développement sécurisé de vos *services* ou *produits*.**

Plus précisément, sont concernées par ce document les équipes dont :

- le principal objectif est de livrer rapidement et fréquemment un produit ou un service à ses usagers, pour résoudre un problème auquel ceux-ci sont confrontés ;
- les membres sont dotés de compétences diverses – techniques ou non – et travaillent ensemble au quotidien ;
- les membres sont suffisamment autonomes pour décider ensemble de l'organisation de leur propre travail ;
- l'attention est prioritairement tournée vers la qualité de ce qu'elles produisent et qui s'outillent en conséquence dans un souci permanent d'amélioration.

Généralement, ces caractéristiques – sans être individuellement essentielles à « l'agilité » – s'observent dans des équipes plutôt réduites de cinq à dix personnes et s'accompagnent de pratiques telles que le management visuel (*task board*, etc.), l'utilisation systématique de tests automatisés, le déploiement continu, les outils DevOps et le cadencement du travail en itérations. Nous désignons l'ensemble des intervenants d'une telle équipe par le terme *équipe produit*.

La sécurité numérique concerne toute organisation et tous types de projets. La méthode d'identification et de traitement des risques décrite dans ce guide permet de mettre en évidence quels sont, parmi ces risques numériques, les plus conséquents dans le contexte d'usage du service ou du produit. La nature des risques à considérer est variée.

Citons, par exemple, les actions de sabotage par déni de service distribué, le vol de données économiques ou à caractère personnel, la fraude ou le détournement d'usage à des fins lucratives, l'usurpation d'identité ou encore les actions de déstabilisation et d'atteinte à la réputation.

NOTES

1/ À QUI S'ADRESSE CE GUIDE ?

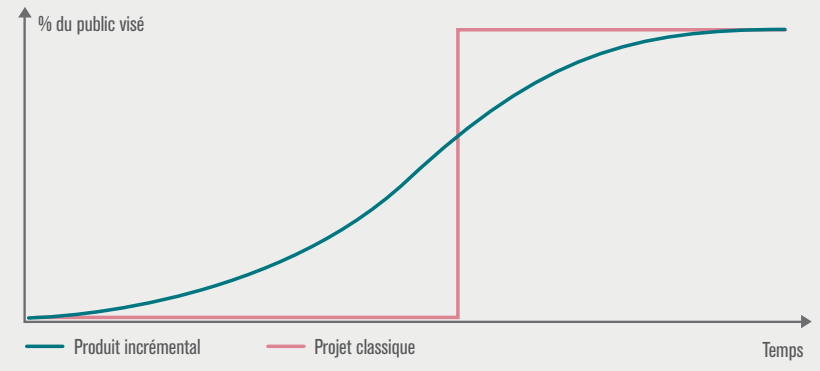
2/ LA PRISE EN COMPTE INCRÉMENTALE DU RISQUE

LA PRISE EN COMPTE INCRÉMENTALE DU RISQUE : LA CLÉ DE LA COMPATIBILITÉ AGILE

Dans une démarche sécuritaire classique, l'équipe définit les besoins de sécurité et les façons d'y répondre dès la phase de conception d'un **projet**, les mesures de sécurité étant très souvent définies et mises en œuvre pour le périmètre final et son cas d'usage à la cible. Dans une démarche agile, l'équipe cherche à livrer très tôt de la valeur à un public donné avec un **produit** incomplet, tout en cherchant à susciter l'adhésion d'autres publics en étoffant ce produit.

Voici, illustrées, deux conceptions opposées : ce que peut être la courbe de diffusion d'un produit, comparée à celle résultant de la livraison d'un projet.

Diffusion d'un produit vs livraison d'un projet

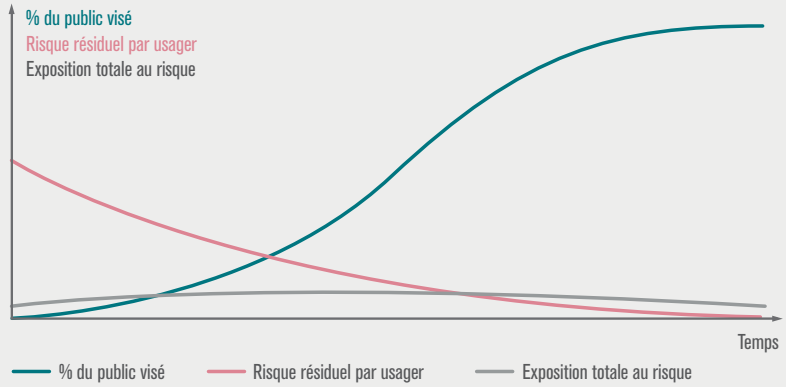


Pour une équipe dont l'objectif est de livrer rapidement de la valeur à ses utilisateurs, une évaluation pertinente du risque est donc obtenue en considérant simultanément le nombre d'usagers et le risque encouru par chacun, pour déterminer une exposition globale au risque.

Ainsi, la prise en compte des enjeux de sécurité par une équipe agile se veut continue (tout au long de la construction et de l'amélioration du service) et pragmatique puisqu'elle priorise les efforts en fonction du risque réel et assume l'existence de risques résiduels. **Ce principe de management de la sécurité numérique par les risques est celui qui guide la démarche proposée.**

La figure ci-dessous superpose à la courbe de diffusion une courbe hypothétique représentant le risque résiduel auquel un seul usager serait exposé. Initialement, le risque par usager est substantiel, mais avec une poignée d'utilisateurs, il reste globalement acceptable. En revanche, lorsque le produit devient un succès, l'équipe doit alors renforcer le traitement des risques résiduels.

Exposition au risque résiduel d'un produit



L'important est donc de s'assurer d'arriver au point d'inflexion en ayant couvert les risques numériques les plus importants, la recherche de l'exhaustivité n'étant pas forcément prioritaire, sous peine d'allouer des ressources conséquentes pour un résultat mitigé alors que ces dernières auraient pu être investies dans une meilleure compréhension du besoin.

NOTES

2/
LA PRISE EN COMPTE INCRÉMENTALE DU RISQUE

3/ L'ATELIER D'ANALYSE DE RISQUE

L'ATELIER D'ANALYSE DE RISQUE : LE CŒUR DE LA DÉMARCHE

Nos recommandations concrètes envers les équipes agiles peuvent se résumer ainsi : **l'équipe se réunit, à intervalles réguliers, pour discuter des risques numériques qui peuvent impacter les usagers de son service ou produit et décider de la meilleure manière de traiter ces risques.**

Un atelier type d'analyse de risque se déroule dans les conditions suivantes :

- présence de toute l'équipe et seulement de l'équipe ;
- durée fixe et limitée (une à trois heures), mieux vaut privilégier la programmation de plusieurs ateliers.

Le support d'animation de l'atelier peut reposer sur l'utilisation d'un *paper board* ou de Post-it pour accompagner la discussion et animer les éléments d'analyse de risque qui auront été consignés sur des feuillets.

/ QUAND FAUT-IL TENIR CES ATELIERS ?

L'adage est bien connu : *« Le meilleur moment pour planter un arbre, c'était il y a 20 ans ; le deuxième meilleur moment, c'est maintenant. »* Il n'est jamais trop tard pour parler de sécurité numérique et évaluer les risques inhérents à la conduite d'un projet donné, idéalement **avant même le début des travaux de réalisation, voire d'investigation**. Néanmoins, le fait que l'équipe ait déjà réalisé un ou plusieurs incréments de fonctionnalité, voire que son produit soit déjà accessible à de premiers usagers, ne saurait constituer une raison valable de ne pas se livrer à l'exercice.

/ COMMENT ANIMER L'ATELIER ?

Les conditions du succès d'un atelier d'analyse de risque sont à rapprocher de celles d'autres « rituels » agiles, comme par exemple la rétrospective. **Véritable facilitateur, l'animateur de ces ateliers assume un rôle particulièrement important dont voici quelques-unes des principales responsabilités :**

- s'assurer que la prise de parole est répartie de façon équilibrée entre les différents participants à l'atelier ;
- veiller à ce que le groupe ne dévie pas du sujet à traiter ;
- maintenir un climat bienveillant ;
- surveiller l'horloge… Un bon atelier ne déborde pas (trop) du temps imparti.

Une animation efficace suppose également de bien maîtriser le canevas d'analyse de risque ; celui-ci est présenté schématiquement plus loin (section *« L'appréciation des risques : les bases à connaître et à transmettre »* page 20) et de façon plus détaillée et analytique en fiche mémo page 42.

/ FAUT-IL SE FAIRE ACCOMPAGNER ?

La présence d'un expert en sécurité numérique n'est pas indispensable à la réussite de la démarche. Quelles que soient les conclusions de l'analyse de risque, c'est à l'équipe dans son ensemble qu'il incombera de mettre en œuvre les actions qui s'en dégagent et c'est notamment en cela que s'illustre l'agilité d'une équipe.

Un atelier de travail n'est pas une réunion. L'efficacité d'un atelier est conditionnée par une prise de parole et d'initiative équilibrée entre participants. Elle risque d'être diminuée par la présence d'observateurs ou de personnes non impliquées (ou très indirectement) dans la réalisation du produit.

Le niveau de maturité et de compétence au sein de l'équipe en matière de sécurité numérique pèsera lui aussi de façon déterminante sur les résultats de la démarche. Si l'équipe ne maîtrise pas suffisamment ces compétences au démarrage, il lui faudra donc les acquérir. La présence d'un expert en sécurité numérique, dans une posture de service et d'accompagnement, peut donc être un facteur de réussite. Il ou elle pourra jouer un rôle d'animation ou de facilitation, mais également faire bénéficier de son expertise lorsque c'est opportun.

3
L'ATELIER D'ANALYSE DE RISQUE

4 LE PREMIER ATELIER

LE PREMIER ATELIER

En amont du premier atelier voire en début de séance, il est important de définir le périmètre de l'analyse.

- Y est inclus : ce qui engage la responsabilité de l'équipe et de sa hiérarchie.
- En est exclu : ce qui relève éventuellement d'autres acteurs.

Pour lancer ce premier atelier, vous pouvez proposer le cadrage suivant :

- *Un mois après le lancement du produit, vous découvrez avec horreur un article dans la presse nationale qui fait état d'une énorme faille de sécurité exploitée avec succès. Quels scénarios de menaces possibles vous viennent à l'esprit ?*

Cet exercice permettra de concentrer l'attention des participants sur les enjeux et besoins de sécurité les plus importants tout en amorçant la discussion. Lorsque celle-ci cesse de faire émerger de nouvelles idées, proposez aux participants de formaliser ce qui ressort de l'atelier en consultant la section suivante.

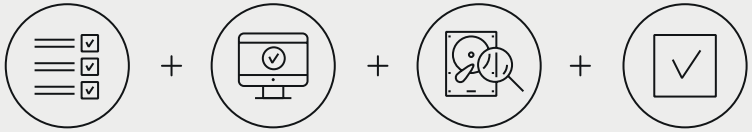
N'hésitez pas à ordonnancer dès ce premier atelier les grandes étapes qui guideront votre démarche de sécurité numérique. Si celle-ci s'inscrit dans une homologation de sécurité, consultez la section *« Se préparer à une démarche d'homologation »* page 31.

/ Un exemple suivi pas à pas : Le.Taxi

Afin d'illustrer concrètement la démarche proposée, nous avons choisi de rendre compte du premier cas réel dans lequel elle a été utilisée. Il s'agit de la plateforme nationale Le.Taxi dont la mission est d'informer sur la disponibilité et la géolocalisation des véhicules des opérateurs de taxi participants.

Pour ce système d'information, nous avons souhaité retracer dans ce guide l'ensemble de la démarche, du premier atelier à la constitution du dossier d'homologation. L'analyse de risque complète est disponible en fiche mémo page 49 et les exemples à suivre sont issus de ces ateliers et de leurs livrables.

/ Ressources utiles



Référentiels réglementaires et normatifs + Guides d'hygiène informatique + Bases de connaissances d'analyse de risque + Stratégie d'homologation visée

NOTES

4
LE PREMIER ATELIER

5 L'APPRÉCIATION DES RISQUES

L'APPRÉCIATION DES RISQUES : LES BASES À CONNAÎTRE ET À TRANSMETTRE

La valeur métier correspond à la valeur livrée aux utilisateurs et s'articule en *user stories*. Les *user stories* au niveau le plus macroscopique (parfois appelées *epics*) revêtent généralement un enjeu de sécurité significatif vis-à-vis de l'un ou l'autre des critères ci-dessous.

- **[D] Disponibilité :** la fonctionnalité peut être utilisée au moment voulu ;
- **[I] Intégrité :** les données sont exactes et complètes ;
- **[C] Confidentialité :** les informations ne sont divulguées qu'aux personnes autorisées ;
- **[P] Preuve :** les traces de l'activité du système sont opposables en cas de contestation.

De par leur criticité vis-à-vis des enjeux opérationnels et réglementaires de l'organisme, ces qualités doivent être protégées face aux menaces jugées vraisemblables (attaques informatiques, actes de fraude, erreurs, défaillances, etc.).

/ Exemple : Le.Taxi

User stories	[D]	[I]	[C]	[P]
Un client transmet son identifiant, sa position et son numéro de téléphone	●	●●	●●	
Un client peut émettre une demande (« héler virtuellement » un taxi)	●	●●	●	●
Un client peut évaluer une course effectuée ou déclarer un incident		●		●
Un administrateur peut enregistrer ou radier un taxi		●		●

● Besoin important ●● Besoin très important

/ DES BESOINS DE SÉCURITÉ AUX ÉVÉNEMENTS REDOUTÉS

Chaque besoin de sécurité identifié constitue le point de départ pour décrire un ou plusieurs événements redoutés susceptibles de compromettre la valeur d'usage.

/ Exemple : Le.Taxi

Événements redoutés	Impacts métier	Gravité
Le système ne répond pas	Expérience utilisateur dégradée ▸ Perte de clients	●
Un opérateur de taxis émet de fausses positions	Qualité de service dégradée ▸ Perte de clients	●
Un taxi fait une course d'approche en pure perte	Perte de confiance et d'adhésion des taxis ▸ Désengagement aboutissant à une réduction de l'offre de taxis	●●

● Modérée ●● Très élevée

/ LES RISQUES RÉSULTENT DE LA COMBINAISON DES ÉLÉMENTS DE L'ANALYSE

Un risque décrit la réalisation d'un scénario de menace intentionnel ou accidentel :

1/ une source de risque (un cybercriminel ou un fraudeur, par exemple)

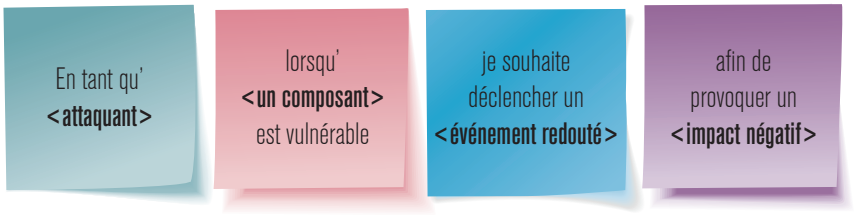
2/ par le biais d'un composant vulnérable du produit ou service

3/ provoque un événement redouté

4/ occasionnant des impacts sur la valeur métier, directs et indirects (humains, opérationnels, juridiques, etc.).

On lui associe une criticité basée sur l'estimation conjointe de la gravité des impacts et de la vraisemblance du scénario de menace conduisant à l'événement redouté.

Chacune des quatre catégories pré-citées correspondra à une couleur de Post-it. Voici une suggestion pour la correspondance entre les couleurs :



Commencez par ces quatre catégories qui ont tendance à constituer « l'angle mort » pour beaucoup d'équipes. Réservez une couleur plus classique, le jaune par exemple, pour lister séparément à la fin de l'exercice :

Les scénarios de risques peuvent être nommés *abuser stories* car ils correspondent au revers néfaste d'une *user story* et engendrent une perte de valeur.

6 QUE FAIRE APRÈS CHAQUE ATELIER ?

QUE FAIRE APRÈS CHAQUE ATELIER ?

L'atelier initial ne suffira peut-être pas à placer l'équipe en situation de confiance vis-à-vis du traitement des risques numériques, particulièrement s'il s'agit de la première mise en œuvre d'une telle démarche ou d'un sujet particulièrement sensible.

Pour favoriser la continuité de ce travail d'un atelier à l'autre, il est utile d'en formaliser les résultats de manière cohérente avec la démarche agile choisie par l'équipe. Les détails dépendront, bien entendu, de chaque équipe et de ses pratiques d'organisation et d'ingénierie, mais voici quelques pistes :

- l'analyse de risque peut être consignée dans un Wiki ou tout autre espace documentaire, pourvu qu'il soit facilement accessible par tous les membres de l'équipe ;
- les *abuser stories* pourront être traitées comme les *user stories* et ajoutées au *backlog* ;
- si l'équipe le fait pour les *user stories*, elles peuvent être priorisées, annotées par leurs définitions de « fait » et éventuellement « prêt » ;
- la démonstration de la prise en compte des risques associés à une *abuser story* peut être faite par le biais de tests automatisés, comme c'est le cas pour les *user stories* : au lieu de démontrer par un test qu'un scénario fonctionnel aboutit, on cherchera à démontrer, au contraire, qu'un vecteur d'attaque n'aboutit pas.

7 LES ATELIERS SUIVANTS

LES ATELIERS SUIVANTS, ITÉRATION APRÈS ITÉRATION

Au fil des itérations, il deviendra périodiquement nécessaire d'actualiser ou d'affiner le résultat du premier atelier, par exemple lors des événements suivants :

- la réalisation d'une *user story* induit des évolutions d'architecture telles que l'ajout ou la modification d'un composant technique ;
- la réalisation d'une *user story* amène à exposer des données d'une autre nature que celles précédemment traitées (des données personnelles par exemple, alors que ce n'était pas le cas auparavant) ;
- l'équipe réalise un atelier dédié à une fonctionnalité spécifique du produit, qui adresse une ou plusieurs *user stories* plus particulièrement sensibles en termes de sécurité ;
- les retours des usagers amènent à évaluer différemment la valeur métier des différentes *user stories* ou les besoins de sécurité qui leur sont associés ;
- le nombre d'usagers ou le volume de transactions métier a sensiblement évolué, de telle sorte que l'exposition totale au risque a, elle aussi, évolué.

À l'image des autres activités menées par les équipes agiles, le travail à réaliser est alors presque identique à celui du premier atelier. Au fil des itérations, l'équipe apprendra ainsi à tenir compte, dans son plan de charge, du temps consommé par les activités liées à la sécurité afin de lisser ce travail dans le temps, comme elle le fait pour les activités liées à la qualité.

/ DETTE SÉCURITAIRE

On appelle « dette technique » le choix que fait une équipe de privilégier temporairement la livraison de nouvelles fonctionnalités, au détriment de pratiques de conception telles que le *refactoring*, l'automatisation en soutien du test ou la mise en commun des connaissances. Cette stratégie peut s'avérer payante mais doit résulter d'un choix délibéré et non d'un manque

de compétences dans ces domaines. L'intention est de mettre plus rapidement de nouvelles versions du produit ou du service entre les mains des usagers et d'obtenir des retours de ces derniers, avant de « rembourser » la dette dans un second temps.

Par analogie, on peut parler de « dette sécuritaire » lorsque l'équipe est amenée à différer le traitement de certains risques dans le but de mettre plus rapidement le produit à l'épreuve de ses premiers usagers. De la même façon, cette stratégie doit résulter d'un choix délibéré et non d'un manque d'attention portée à l'analyse de risques ou de compétences en la matière.

Dans les deux cas, un atelier d'analyse de risque tel que nous l'avons décrit ci-dessus peut amener l'équipe à réserver une part importante de sa capacité, ou consacrer une itération entière, à la prise en compte de la sécurité du système.

NOTES

8

SE PRÉPARER À UNE DÉMARCHE D'HOMOLOGATION

SE PRÉPARER À UNE DÉMARCHE D'HOMOLOGATION

L'homologation de sécurité est un acte formel par lequel l'autorité responsable d'un système engage sa responsabilité en matière de gestion du risque. Elle est rendue obligatoire, pour les administrations, par le décret n°2010-112 du 2 février 2010, selon des modalités précisées par le Référentiel général de sécurité (RGS). De même, elle est obligatoire pour tout produit traitant d'informations relevant du secret de la Défense nationale, comme précisé dans l'Instruction générale interministérielle 1300 (IGI 1300). Citons également la loi de programmation militaire, dont le volet *cyber* (loi n° 2013-1168 du 18 décembre 2013 - article 22), impose aux opérateurs d'importance vitale le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent, mené dans le cadre d'une démarche d'homologation.

Lorsqu'elle n'est pas réglementairement imposée, **la démarche d'homologation reste toutefois une excellente façon de témoigner, vis-à-vis des usagers, de la volonté de prendre en compte la sécurité numérique des services proposés et de valoriser le niveau de maîtrise des risques atteint** (la méthode présentée peut également servir de point de départ à une démarche de certification ou de qualification de solutions de sécurité).

Comme le rappelle le guide « *L'homologation de sécurité en neuf étapes simples* » :

> L'objectif de la démarche d'homologation [...] est de trouver un équilibre entre le risque acceptable et les coûts de sécurisation, puis de faire arbitrer cet équilibre, de manière formelle, par un responsable qui a autorité pour le faire.

Les livrables de l'atelier d'analyse de risque, tel que nous l'avons présenté dans ces pages, constituent un entrant nécessaire mais généralement insuffisant dans le cadre d'une démarche d'homologation. Par conséquent, nous recommandons de dédier un atelier à la préparation de la commission d'homologation (formalisation du dossier de sécurité, bilan des tests et audits de sécurité, consolidation des risques résiduels, suivi des mesures de sécurité et du plan d'action correctif).

/ HOMOLOGATION PROVISOIRE

Par hypothèse, l'équipe à laquelle s'adresse le présent guide cherche à mettre rapidement en service une première version incomplète du produit, puis à l'étoffer par incréments fonctionnels.

Dans ce contexte, l'équipe se dirigera donc naturellement vers **une décision d'homologation provisoire, afin d'adapter le niveau de risque résiduel accepté à un contexte donné.** Sa validité sera limitée dans le temps et conditionnée par des critères liés au volume ou à l'intensité d'exploitation, dans une unité appropriée : en nombre d'usagers, en volume de transactions, etc.

Ces **critères de validité** doivent pouvoir être mesurés et surveillés afin d'objectiver que l'on respecte encore les conditions de validité de l'homologation provisoire. L'équipe pourra moduler la durée et les critères de validité des homologations provisoires successives en fonction de la diffusion réellement constatée du service.

Une stratégie d'homologation pour la plateforme Le.Taxi pourrait ainsi se décliner en trois jalons :

- un jalon « *autorisation de tests* » d'une durée d'un à trois mois, menée exclusivement auprès d'usagers volontaires sur consentement explicite ;
- un jalon « *autorisation provisoire d'exploitation* », d'une durée maximale de 12 mois et un plafond de 1 000 courses cumulées ;
- un jalon « *mise en service ferme* » tel que décrit ci-après.

/ HOMOLOGATION FERME

Une décision d'homologation ferme pourra être prononcée dès lors qu'un produit ou un service aura atteint son « régime de croisière ». Elle est généralement assortie d'une période de validité plus longue (trois ans étant une valeur typique) et vise le contexte d'exploitation normalement prévu, sans restrictions particulières d'usage.

Si l'équipe n'a pas eu recours aux services d'un expert en sécurité numérique lors des ateliers d'analyse de risque, ni à l'intervention d'un auditeur externe pour réaliser, par exemple, des tests d'intrusion ou une revue de code axée sur les besoins de sécurité, ces vérifications extérieures s'imposent généralement comme préalables à une décision ferme.

La mise en place d'un **plan d'amélioration continue de la sécurité** pour les versions successives à venir du produit ou du service est également un élément important de la décision d'homologation. Ce plan garantit la montée en puissance et en maturité de la sécurité du produit et permet une gestion priorisée des **risques résiduels** selon leur criticité.

Notez enfin que l'on prend soin de ne pas parler d'homologation « définitive ». En effet, le caractère évolutif d'un produit doté d'une forte composante logicielle impose de réévaluer périodiquement les risques, quand bien même le produit serait resté inchangé. Chose qui n'arrive, en pratique, que très rarement.

/ FORMALISER LE DOSSIER D'HOMOLOGATION

Le guide *L'homologation de sécurité en neuf étapes simples* détaille les étapes de la constitution du dossier de sécurité en vue d'une commission d'homologation. Simple, pratique et concis, l'expérience prouve qu'il sera un compagnon précieux pour toutes les équipes agiles qui souhaitent aboutir à une décision d'homologation.

À retrouver sur : **www.ssi.gouv.fr**

9 FICHES MÉMO

FICHE MÉMO 1 / STRUCTURER SA POLITIQUE DE SÉCURITÉ

La politique de sécurité d'un système d'information (PSSI) s'articule autour de trois niveaux de mesures de sécurité :

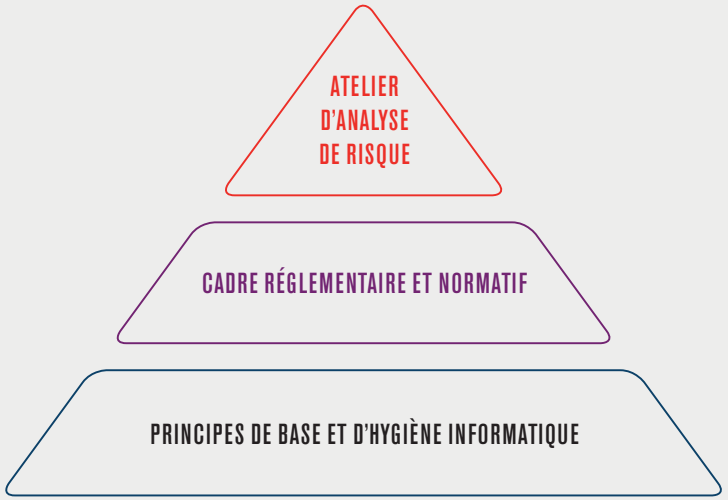
- **Les mesures d'hygiène informatique** couvrent divers domaines : sensibilisation et formation, authentification, sécurisation des postes et réseaux, administration, nomadisme, etc. Elles constituent un « socle de bonnes pratiques » applicables de façon systématique et conférant un niveau de protection capable de résister aux menaces les plus courantes.

- **Les mesures réglementaires et normatives** complètent ce socle d'hygiène par des exigences sectorielles applicables dans des domaines précis, selon les enjeux de sécurité identifiés (disponibilité, intégrité, confidentialité, preuve). Ainsi, la loi de programmation militaire (LPM) dicte-t-elle des obligations aux opérateurs d'importance vitale, le référentiel général de sécurité (RGS) s'applique aux systèmes d'information de l'administration, les règlements de la CNIL et le règlement général sur la protection des données (RGPD) européen s'appliquent à tout opérateur traitant de données à caractère personnel, l'instruction générale interministérielle 1300 (IGI 1300) définit les règles relatives à la protection du secret de la Défense nationale, etc.

- **Les mesures issues des ateliers d'analyse** de risque complètent ce socle par des mesures contextuelles, spécifiques aux cas d'usage du produit ou du service dans son écosystème (exemples : mise en place d'une liste blanche pour sécuriser un processus de traitement automatisé, durcissement d'une mesure d'hygiène, adaptation d'une mesure réglementaire, etc.). Ces mesures confèrent au produit robustesse et résilience face aux menaces ciblées et/ou sophistiquées jugées vraisemblables.

L'analyse de risque n'a donc pas vocation à procéder à une nouvelle identification des mesures de sécurité connues ou imposées, qui relèvent respectivement de l'hygiène et de la règlementation.

Structuration des mesures de sécurité d'un produit



FICHE MÉMO 2 / LES CLÉS POUR IDENTIFIER LES RISQUES NUMÉRIQUES CRITIQUES

Les activités de sécurité visent à identifier les scénarios de risques critiques et les mesures de sécurité permettant de les traiter. L'objectif est d'atteindre un niveau de sécurité correspondant aux enjeux et besoins sécuritaires dans une démarche agile, un scénario de risque est décrit sous la forme d'une *abuser story* de nature intentionnelle ou d'un scénario d'origine accidentelle. Cette fiche mémo recense les aspects méthodologiques à considérer en priorité lors des ateliers d'analyse de risque.

User story, abuser story et scénario accidentel

***User story* :** *« En tant qu'utilisateur, je réserve en ligne mon billet de spectacle. »*

Abuser story (scénario intentionnel) : *« En tant qu'hacktiviste, j'empêche les clients de réserver en ligne leur billet de spectacle en saturant le serveur applicatif par une attaque en déni de service. Ceci conduit à un impact préjudiciable sur l'image et la crédibilité du gestionnaire du service, voire une perte de clients. »*

Scénario accidentel : *« Le service de réservation en ligne est rendu indisponible en raison d'une erreur de mise à jour du serveur applicatif par le prestataire en charge de la maintenance du système. Ceci conduit à un impact préjudiciable sur l'image et la crédibilité du gestionnaire du service, voire une perte de clients. »*

/ SE CONCENTRER SUR LES RISQUES NUMÉRIQUES LIÉS AUX CAS D'USAGE DU PRODUIT

L'analyse de risque doit s'attacher à identifier les *abuser stories* spécifiques, c'est-à-dire significatives en termes d'impact et qui relèvent de menaces – intentionnelles ou accidentelles – non couvertes par les mesures d'hygiène informatique ou réglementaires. Ces *abuser stories* permettent de compléter, d'orienter et de consolider la politique de sécurité du produit ou du service.

En termes de volumétrie, l'identification et le traitement de cinq à dix *abuser stories* constituent une première base solide pour définir les mesures de sécurité structurantes liées aux cas d'usage courants du produit.

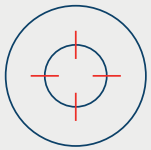
L'analyse de risque n'a pas vocation à identifier de nouvelles mesures de traitement connues ou imposées, qui relèvent respectivement de l'hygiène informatique et de la réglementation, et qui sont considérées comme nativement intégrées dans la politique de sécurité du produit (voir fiche mémo page 35). En revanche, elle a vocation à :

- valider ou non les dérogations éventuelles à ce socle de sécurité ;
- identifier le besoin de durcir ce socle ;
- identifier des mesures complémentaires *ad hoc* liées aux conditions d'emploi du produit, à ses processus métier, à son écosystème, etc.

/ PRIVILÉGIER LES *ABUSER STORIES* (SCÉNARIOS INTENTIONNELS)

Parmi les scénarios de risques à prendre en compte dans une analyse de risque, ceux de nature intentionnelle peuvent s'avérer particulièrement redoutables lorsque l'attaque est menée avec la volonté d'atteindre l'objectif visé en engageant des moyens particulièrement importants. Les éléments constitutifs classiques à prendre en compte dans une *abuser story* intentionnelle sont les suivants :

Un ou plusieurs attaquant(s)



Une cible

Un chemin d'attaque exploitant généralement plusieurs vecteurs et/ou vulnérabilités

Une ou plusieurs finalité(s)

La réussite d'une attaque sur un système d'information ne relève que rarement de l'exploitation d'une seule faille. Les attaques intentionnelles suivent généralement une démarche séquencée exploitant de façon coordonnée plusieurs vulnérabilités de nature informatique ou organisationnelle. C'est en raison de telles séquences que des failles d'apparence anodine peuvent devenir lourdes. Plusieurs modèles existent et peuvent être utilisés (exemple : *cyber kill chain* de Lockheed Martin). L'équipe pourra exploiter le modèle suivant, donné à titre d'information.

1 Reconnaissance externe

L'attaquant recueille des informations sur la cible par tous les moyens possibles : sources ouvertes (réseaux sociaux) ou non (officines).

2 Intrusion

L'attaquant s'introduit via un courriel piégé, un maliciel, des droits usurpés, une injection SQL, une faille non corrigée, un zero-day, etc.

3 Reconnaissance interne

L'attaquant mène des activités de reconnaissance interne lui permettant de cartographier l'architecture réseau, identifier les mécanismes de sécurité mis en place, recenser les vulnérabilités exploitables et localiser les services, informations et composants stratégiques.

4 Latéralisation et élévation de privilèges

À partir de son point d'accès initial, l'attaquant va progresser dans le système d'information et acquérir des droits lui permettant de se déplacer « n'importe où » dans le réseau, de propager les outils malveillants et de maintenir son accès en toute discrétion.

5 Pilotage et exploitation de l'attaque

Selon les objectifs de l'attaquant : sabotage, altération de service, vol de données, fraude, falsification, détournement d'usage, usurpation d'identité, défiguration de site, etc.

Nous vous recommandons d'adopter une vision globale des séquences d'attaques possibles dans vos ateliers de sécurité, afin de ne pas minimiser à tort un scénario dont la vraisemblance et l'impact pourraient se révéler disproportionnés. Cette approche doit vous permettre d'identifier facilement les composants critiques susceptibles de servir de vecteurs d'entrée ou d'exploitation, de relais de propagation, etc. Ces composants – de nature technique, humaine ou organisationnelle – feront alors l'objet de mesures *ad hoc* ou d'un durcissement du socle existant

/ CONSIDÉRER L'ÉCOSYSTÈME COMME UNE SOURCE DE RISQUE POTENTIEL

On entend par écosystème l'ensemble des parties prenantes qui gravitent autour du produit ou du service et qui sont généralement nécessaires à son fonctionnement. Un nombre croissant de modes opératoires d'attaques exploite les vulnérabilités d'un écosystème pour atteindre leur cible. C'est ainsi qu'aux États-Unis, un casino a fait les frais d'une attaque menée par le biais… d'un aquarium connecté ! L'analyse de risque doit alors prendre en compte ces éléments de l'écosystème, susceptibles de rendre possible ou de faciliter la réalisation d'*abuser stories*.

/ Exemple

Injection de code malveillant par rebond via un partenaire tiers connecté facilitant l'exfiltration de données sensibles, etc.

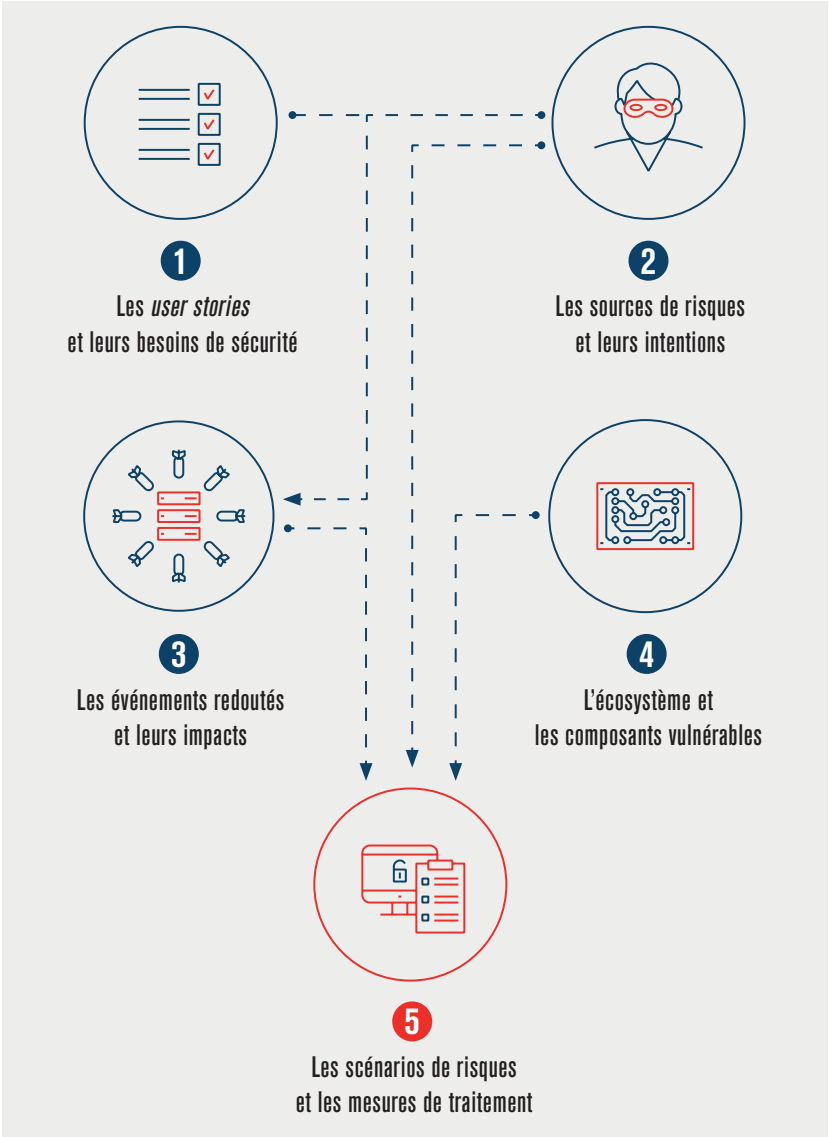
Les parties prenantes critiques d'un écosystème, à prendre en compte dans l'analyse de risque, peuvent par exemple être identifiées en vous posant les questions suivantes :

- La relation avec cette partie prenante est-elle essentielle pour mon activité ? Suis-je dépendant de services ou de bases de données hébergés ou exploités par la partie prenante ?
- Jusqu'à quel point la partie prenante accède-t-elle à mes ressources internes (mes locaux, mes réseaux informatiques, mon organisation) ?
- Ses services et réseaux informatiques sont-ils exposés sur Internet ? Sont-ils suffisamment sécurisés ?
- Puis-je considérer que ses intentions sont favorables à mon égard ?

Une méthode simple et pragmatique d'évaluation de la menace d'un écosystème est proposée dans le guide EBIOS de l'ANSSI.

L'identification des scénarios de risque, particulièrement ceux de nature intentionnelle, nécessite une certaine expertise en sécurité numérique. Un constat d'autant plus vrai pour les cas d'attaques sophistiquées, mettant en œuvre un séquencement planifié de modes d'action sur plusieurs composants – techniques et humains généralement – du produit et de son écosystème. Comme nous l'avons précisé plus haut, l'accompagnement de l'équipe par un expert dans ce domaine peut donc être un atout pour la réussite de l'atelier, en proportion avec le degré de complexité du produit et de l'écosystème.

FICHE MÉMO 3 / LE CANEVAS DE L'ANALYSE DE RISQUE



❶ / LES *USER STORIES* ET LEURS BESOINS DE SÉCURITÉ

Dans cette rubrique, il s'agit de recenser les principaux éléments de valeur d'usage mis en œuvre par le produit, et d'estimer leurs besoins de sécurité (DICP : disponibilité, intégrité, confidentialité, preuve). Ces éléments seront généralement exprimés sous forme de *users stories.*

L'objectif est d'identifier, pour chaque *user story*, quels sont les besoins de sécurité les plus importants afin d'orienter par la suite le travail d'identification des scénarios de risques pertinents. Le degré d'importance peut être pondéré par un indice simple. Par exemple, **• pour un besoin important et •• pour un besoin très important.** Un schéma similaire pourra être adopté pour les autres éléments de l'analyse. L'évaluation de l'importance d'un besoin de sécurité est souvent itérative et obtenue par comparaison au fur et à mesure de l'atelier ; un besoin identifié comme « très important » traduit le fait qu'il est essentiel pour le produit.

Le point de départ de l'atelier – les *user stories* – est essentiel. En commençant par là, l'équipe ancre dans le reste de l'atelier l'idée que les mesures de sécurité servent la valeur livrée aux usagers. En effet, pour chaque besoin de sécurité important relatif à une *user story*, il y a un ou plusieurs événements redoutés et au moins un scénario de risque susceptible de compromettre la proposition de valeur.

/ Exemple

Un client peut émettre une demande (« héler virtuellement un taxi »), évaluer une course effectuée ou déclarer un incident.

❷ / LES SOURCES DE RISQUES ET LEURS INTENTIONS

Il s'agit de recenser les sources de risques – accidentelles ou intentionnelles, externes ou internes – susceptibles d'impacter la valeur d'usage : qui ou quoi pourrait porter atteinte aux besoins de sécurité. Le schéma ci-dessous résume quelques-unes des motivations à l'origine d'attaques intentionnelles, et peut constituer un point de départ intéressant à la discussion lors de l'atelier.

/ Identification des sources de risques

Il est recommandé de recenser des sources de risques de natures et de motivations variées pour disposer d'un échantillon de risques représentatif à partir duquel bâtir des scénarios dont les menaces et modes opératoires diffèrent.

/ Exemple

- Opérateur concurrent cherchant à discréditer, voire saboter le service Le.Taxi (malveillance).
- Mafia cherchant à collecter des données à caractère personnel pour les monnayer (appât du gain).

❸ / LES ÉVÉNEMENTS REDOUTÉS ET LEURS IMPACTS

Un événement redouté (ER) correspond au non-respect d'un besoin de sécurité : chaque besoin de sécurité associé à une *user story* de l'étape ❶ se décline donc selon un ou plusieurs événements redoutés. Il convient de préciser les impacts (sur les missions ou la sécurité des personnes, financiers, juridiques, d'image, environnementaux, etc.) ainsi que le niveau de gravité estimé, l'objectif étant d'identifier en priorité les événements redoutés dont les conséquences seraient difficilement surmontables.

En première approche, l'échelle de cotation adoptée peut se limiter à un indice de priorité (P), par exemple : P1 – ER à retenir, P2 – ER à considérer dans un second temps. De façon plus élaborée, une échelle de cotation à trois niveaux ou plus pourra être adoptée : • **gravité faible,** • • **moyenne,** • • • **élevée**.

Un événement redouté est exprimé sous la forme d'une expression courte qui permet de comprendre facilement le préjudice lié à la *user story* concernée. Il est recommandé de mentionner dans l'intitulé de l'ER la source de risque la plus vraisemblable susceptible d'en être à l'origine. Enfin, dans un souci d'efficacité, l'équipe s'intéresse en première approche aux événements redoutés associés aux besoins de sécurité « très importants ».

/ Exemple

- Un opérateur concurrent, se faisant passer pour un client, hèle un taxi qui réalise une course d'approche en pure perte.

❹ / L'ÉCOSYSTÈME ET LES COMPOSANTS VULNÉRABLES

Il s'agit d'identifier parmi les composants du produit ceux contribuant à la réalisation des *user stories* identifiées dans l'étape ❶ et susceptibles d'être concernés ou ciblés par les sources de risques de l'étape ❷. Il est recommandé de préciser, pour chaque composant, quelles sont les vulnérabilités que ces sources de risques pourraient exploiter.

/ Exemple

- Base de données Le.Taxi (vulnérabilités exploitables : accès en lecture/écriture depuis Internet, modification fréquente).

L'identification des composants peut être structurée comme suit :

- **infrastructures physiques :** bâtiments, locaux, espaces physiques permettant l'activité et les échanges de flux ;
- **organisations :** structures organisationnelles, processus métiers et supports, ressources humaines ;
- **systèmes numériques matériels et logiciels :** systèmes informatiques et de téléphonie, réseaux de communication.

Le degré de granularité dans la description des composants sera adapté au niveau de connaissance du produit lors de l'atelier. Enfin, les composants prioritaires à recenser sont ceux qui contribuent (de façon directe ou indirecte) aux *user stories* ayant des besoins de sécurité « importants ».

Afin d'étendre le périmètre de l'appréciation des risques, vous pouvez compléter cette étape en identifiant quelles parties prenantes de l'écosystème seraient susceptibles d'être exploitées pour faciliter une attaque sur un composant du produit (reportez-vous à la fiche mémo précédente). Les parties prenantes critiques à considérer en priorité sont celles qui ont un lien avec un des composants recensés.

/ Exemple

- Prestataire informatique assurant la télémaintenance du serveur qui héberge la base de données Le.Taxi.

❺ / LES SCÉNARIOS DE RISQUES (*ABUSER STORIES*) ET LES MESURES DE TRAITEMENT

La finalité de l'atelier est d'identifier les risques numériques de référence à prendre en compte pour bâtir ou compléter la politique de sécurité du produit.

L'équipe commence par dresser une liste de **scénarios de risques** – *abuser stories* – en confrontant les sources de risques ❷, les événements redoutés ❸ et les composants vulnérables ❹. Concrètement, il s'agit de voir de quelle façon chaque source de risque retenue peut impacter des composants du produit, par exploitation notamment de leurs vulnérabilités ou d'un facteur externe aggravant, pour générer un événement redouté. Chaque *abuser story* peut ensuite être évaluée en termes de vraisemblance puis de criticité à partir de la gravité de l'événement redouté associé.

/ Exemple

- Un attaquant externe accède aux informations à caractère personnel de clients en usurpant l'identité du serveur Le.Taxi ou en exploitant une vulnérabilité non corrigée.
- Un client de mauvaise foi attribue abusivement une mauvaise note à un taxi.

Pour chaque *abuser story* répertoriée, l'équipe peut définir si besoin **l'option de traitement du risque** la plus appropriée (éviter, réduire, transférer, accepter). Dans le cas où le risque doit être réduit, les participants identifient les **mesures de sécurité** complémentaires qu'il faudra mettre en œuvre, en plus des mesures existantes ou déjà prévues. Leur réalisation est consignée par l'équipe au même titre que les autres *user stories*.

Enfin, l'équipe peut clore l'atelier en identifiant les **risques résiduels.** Ces derniers concernent :

- les *abuser stories* non traitées (acceptées en l'état) ou seulement partiellement (mesures de sécurité mises en place, mais ne réduisant pas complètement ou suffisamment le risque) ;
- les *abuser stories* faisant l'objet d'un transfert du risque, lequel ne couvre généralement pas l'ensemble des impacts (exemple : l'assurance ne couvre pas l'atteinte à l'image) ;
- pour affiner, dans un deuxième temps : les besoins de sécurité de l'étape ❶ et les événements redoutés de l'étape ❸ non déclinés en *abuser stories*.

Un certain travail (souvent subjectif) de consolidation des risques résiduels est à effectuer par l'équipe afin de disposer d'un bilan à jour et reflétant l'état de maîtrise du risque numérique du produit. Les risques résiduels les plus significatifs seront en priorité recensés et mis en évidence. Par exemple, l'usage d'échelles de gravité, vraisemblance et criticité, associées à des seuils d'acceptation du risque, constituera une aide précieuse pour hiérarchiser les risques résiduels avec objectivité et cohérence. Notons enfin que ce bilan, enrichi au fil des ateliers d'analyse de risque, sera complété par d'éventuelles vulnérabilités résiduelles identifiées à l'issue des audits de sécurité.

De façon alternative, l'équipe peut choisir de différer l'identification et la consolidation des risques résiduels lors d'un atelier de synthèse dédié, notamment pour la préparation d'une commission d'homologation.

La section suivante présente l'intégralité de l'analyse de risque pour la plateforme Le.Taxi et vous permettra d'observer l'articulation des différents éléments présentés ici sur un cas pratique.

FICHE MÉMO 4 / UN EXEMPLE COMPLET

Voici, à titre d'illustration, l'exemple détaillé du service Le.Taxi développé par l'incubateur de services numériques de la DINSIC.

Les tableaux que nous livrons ci-dessous correspondent à la restitution formelle d'un des ateliers d'analyse de risque, sans ajout ni retouches autres que des évolutions de terminologie en cours de rédaction.

User stories	Besoins de sécurité
Un taxi peut remonter sa position via l'interface de programmation applicative (API)	**Disponibilité :** une position doit remonter sous cinq minutes **Intégrité :** altérations détectables
Un client et un taxi conviennent d'une course (scénario global décomposé en sous-scénarios ci-dessous) : ▸ Un client peut connaître les taxis à proximité (ou suivre un taxi en approche) ▸ Un client peut émettre une demande (« héler virtuellement » un taxi) ▸ Le taxi, puis le client, peuvent confirmer la prise en charge ▸ Le taxi ou le client peut annuler la course	**Disponibilité :** sous cinq minutes **Intégrité :** altérations détectables et corrigeables **Confidentialité :** l'information sur les courses est à diffusion limitée
Un client peut évaluer une course effectuée ou déclarer un incident	**Disponibilité :** sous 72 h
Un taxi peut signaler un problème lié à une course	**Disponibilité :** sous 72 h
Un partenaire peut enregistrer un véhicule	**Disponibilité :** sous 72 h **Intégrité :** altérations détectables
Un administrateur peut enregistrer ou radier un partenaire	**Disponibilité :** sous 72 h **Intégrité :** altérations détectables
Un administrateur peut consulter les statistiques partenaires	**Confidentialité :** les statistiques sont à diffusion limitée

FICHE MÉMO 4 / UN EXEMPLE COMPLET

Sources de risques	Modes opératoires	Vraisemblance
Attaquants externes (clients, *hackers*)	Un attaquant externe accède à la base de données	●
	Un attaquant externe surcharge le système	●●
Acteurs agréés de mauvaise foi (taxis, opérateurs)	Un partenaire surcharge le système	●●
	Un partenaire tente de fausser la concurrence en envoyant de fausses positions	●

Événements redoutés	Impacts métier	Gravité
Le système ne répond pas	**Expérience utilisateurs dégradée** ▸ **perte de clients**	●
Un opérateur de taxis émet de fausses positions	**Qualité de service dégradée** ▸ **perte de clients**	●
Un taxi fait une course d'approche en pure perte	**Perte de confiance et d'adhésion des taxis** ▸ **désengagement aboutissant à une réduction de l'offre de taxis**	●●
Un taxi s'enregistre avec de fausses informations	**Captation abusive de courses** ▸ **perte de confiance, risque juridique**	●

Composants du système
API Taxi Exchange Point (TXP)
Serveurs (1 serveur actuellement)
Données stockées
Administrateurs
Partenaires

Risques	Mesures existantes ou prévues
Un partenaire tente de fausser la concurrence en envoyant de fausses positions	Signature cryptographique des remontées de positions par les partenaires
Un attaquant externe accède à des informations confidentielles en exploitant une faille	Fermeture des ports autres que HTTP/HTTPS au trafic issu d'adresses IP inconnues
Un attaquant externe accède à des informations confidentielles en usurpant l'identité du serveur	Échanges sécurisés par HTTPS
Un client de mauvaise foi commande un taxi sans intention d'honorer sa commande	Transaction en deux étapes, bannissement temporaire des clients abusifs
Un taxi fournit des courses ne respectant pas la qualité de service attendue	Enregistrement d'une notation attribuée par le client au taxi
Un client de mauvaise foi attribue abusivement une mauvaise note au taxi	Les notations sont associées à une course réelle spécifique

FICHE MÉMO 4 / UN EXEMPLE COMPLET

Les risques résiduels suivants sont provisoirement acceptés mais doivent être traités par les mesures citées en regard :

Risques résiduels majeurs	Mesures à prendre
Le système est indisponible suite à un déni de service	Redonder les serveurs
Un taxi usurpe l'identité d'un véhicule légitime	À instruire lors de la montée en puissance

NOTES

9/ FICHES MÉMO
AGILITÉ & SÉCURITÉ NUMÉRIQUES

ANNEXES

GLOSSAIRE

Termes	Définitions
Abuser story	Brève description d'un scénario de risque (sous une forme analogue à celle d'une *user story*) qui sera utilisé pour déterminer les mesures de sécurité à implémenter et réaliser les tests de couverture du risque.
Analyse de risque	Sous-processus de gestion des risques visant à identifier, analyser et évaluer les risques.
Backlog	Liste de fonctionnalités ou de tâches (cf. *user stories*) jugées nécessaires à la bonne réalisation du produit.
Besoin de sécurité	Définition précise et non ambiguë du niveau d'exigences opérationnelles relatives à une valeur métier pour un critère de sécurité donné (disponibilité, confidentialité, intégrité, preuve, etc.).
Composant du système d'information (bien support)	Ressource sur laquelle reposent des fonctionnalités et qu'il convient de sécuriser en fonction de sa criticité. On distingue notamment : les systèmes numériques, les organisations et ressources humaines, les locaux et infrastructures physiques.
DevOps	Désigne une communauté réunie autour de pratiques visant à réduire l'écart entre les personnes qui développent un produit ou un service, et celles qui sont chargées de l'héberger, l'opérer, le surveiller, etc. Par exemple, les équipes de développement sont alertées et mobilisées sur tous les incidents de production.
DICP	Acronyme désignant les différentes catégories de besoins de sécurité qu'il convient usuellement de prendre en compte lors d'une analyse des risques numériques : disponibilité, intégrité, confidentialité, preuve.
Écosystème	Parties prenantes qui gravitent autour du système d'information (SI) et interagissent au travers d'interfaces logiques ou physiques. Il peut s'agir des clients ou usagers d'un service, de partenaires, de cotraitants, etc. L'écosystème inclut également l'ensemble des services et réseaux supports indispensables au bon fonctionnement du SI.
Événement redouté	Situation crainte par l'organisme. Il s'exprime par la combinaison des sources de menaces susceptibles d'en être à l'origine, d'une *user story*, du besoin de sécurité concerné et des impacts potentiels. Un événement redouté correspond à une violation d'un besoin de sécurité d'une *user story*.

Termes	Définitions
Homologation de sécurité	Attestation, par une autorité responsable, que le niveau de sécurité est conforme aux attentes et que les risques résiduels sont acceptables dans un contexte d'emploi donné.
Impact	Conséquence directe ou indirecte de l'insatisfaction des besoins de sécurité sur l'organisme ou sur son environnement.
Mesure de sécurité	Moyen de traiter un risque de sécurité. Une mesure peut être de nature technique, physique ou organisationnelle.
Objectif de sécurité	Dans le présent guide, un objectif de sécurité correspond à l'option de traitement décidée pour un scénario de risque. Typiquement : éviter, réduire, transférer, accepter.
Refactoring	Pratique technique consistant à améliorer la conception (lisibilité, modularité, etc.) d'un code source existant sans en modifier la fonctionnalité, et plus largement à prendre en compte la conception tout au long du développement d'un logiciel, plutôt que lors d'une phase distincte au début.
Risque résiduel	Risque subsistant après le traitement du risque et la mise en œuvre des mesures de sécurité. Il peut être présent dès la conception (l'équipe a accepté la présence du risque) ou identifié *a posteriori* (par exemple lors d'un audit externe).
Scénario de risque	Scénario décrivant la survenue d'un événement redouté. Il combine les sources de risques susceptibles d'en être à l'origine, les composants du SI visés, des modes d'action opérés sur ces composants et les vulnérabilités exploitables pour qu'ils se réalisent. Dans le présent guide, un scénario de risque est également désigné sous l'appellation *« abuser story »*.
Source de risque	Entité ou personne à l'origine de scénarios de risque.
User story	Au lieu de faire l'objet d'un cahier des charges, la réalisation d'un produit par une équipe agile suppose de découper le travail à réaliser en incréments de valeur métier appelés *« user stories »*.
Valeur métier	Information ou processus jugé important pour l'organisme et qu'il convient donc de protéger. On appréciera ses besoins de sécurité. En démarche agile, la valeur métier est généralement exprimée sous la forme d'une *user story*.
Vulnérabilité	Caractéristique d'un composant du SI qui peut constituer une faiblesse ou une faille au regard de la sécurité numérique.

BIBLIOGRAPHIE

Les sources ci-après constituent un bon point de départ pour tout organisme souhaitant approfondir ses connaissances ou bâtir son propre référentiel en matière de démarche agile, de développement sécurisé ou de pratiques d'homologation. Cette bibliographie ne se veut pas exhaustive.

/ DÉMARCHE AGILE

- *Le manifeste agile* est le document « historique » et de fait incontournable pour qui souhaite maîtriser le sujet. Toute la littérature qui suit se répartit en deux catégories, des gloses sur le Manifeste et des retours d'expériences du terrain.
  www.agilemanifesto.org/iso/fr/manifesto

- *Le référentiel des pratiques agiles* de l'Institut Agile, avec le soutien de l'association Agile Alliance, vise un recensement des pratiques les plus répandues dans la communauté. On l'utilisera avec profit comme un glossaire étendu permettant d'éviter des incompréhensions : la littérature sur le sujet est en effet riche en jargon, souvent anglophone, qui déroute parfois les néophytes.
  www.referentiel.institut-agile.fr

- *Gestion de projet agile, avec Scrum, Lean, eXtreme Programming…* de Véronique Messager, propose aux personnes ayant le rôle – formel ou informel – de chef de projet un tour d'horizon, tenant compte des spécificités du contexte français, de l'historique des démarches agiles et des principales ruptures avec les doctrines antérieures de gestion de projet. Il s'appuie sur les témoignages de nombreux experts issus de la communauté agile francophone.

- *The Phoenix Project,* de Gene Kim, Kevin Behr et George Spafford est une bonne introduction à l'un des domaines les plus récemment développés par la communauté agile : les principes et pratiques regroupées sous l'étiquette DevOps. Sous une forme inédite (c'est un roman), il constitue une entrée en matière accessible et efficace.

/ DÉVELOPPEMENT SÉCURISÉ

Vous trouverez sur le **site de l'ANSSI** un ensemble de guides, recommandations et bonnes pratiques (cryptographie, postes de travail et serveurs, liaisons sans fil et mobilité, réseaux, applications Web, externalisation, systèmes industriels, technologies sans contact, archivage électronique, etc.) :
www.ssi.gouv.fr/entreprise/bonnes-pratiques

OWASP Proactive Controls (*Open Web Application Security Project*) propose une liste de dix contrôles de sécurité préventifs dédiés au développement logiciel. Ces techniques sont classées par ordre d'importance décroissant. Ce document a été écrit par des développeurs pour des développeurs :
www.owasp.org/index.php/OWASP_Proactive_Controls

SAFECode – Security Guidance for Agile Practitioners – propose des recommandations pratiques sous forme de *user stories* centrées sur la sécurité et les tâches de sécurité qu'ils peuvent facilement intégrer dans leurs environnements de développement agile :
www.safecode.org/publications

/ PRATIQUES D'HOMOLOGATION ET D'ANALYSE DE RISQUE

- **Guide ANSSI** *L'homologation de sécurité en neuf étapes simples* :
  www.ssi.gouv.fr/guide-homologation-securite

- **Base de connaissances EBIOS de l'ANSSI** :
  www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager

- Vous trouverez également sur le **site de l'ANSSI** d'autres guides vous permettant d'approfondir vos pratiques en matière par exemple de défense en profondeur, d'élaboration d'une PSSI ou d'un plan de montée en maturité SSI :
  www.ssi.gouv.fr/entreprise/bonnes-pratiques/methodologie

Outils pratiques pour l'identification et l'évaluation de scénarios de risque numérique (exemples) :

- *Tactical Threat Modeling* de SAFECode :
  www.safecode.org/publications

- *STRIDE Threat Model* de Microsoft :
  www.owasp.org/index.php/Threat_Risk_Modeling#STRIDE

- *DREAD Risk Rating Security Threats* :
  www.wiki.openstack.org/wiki/Security/OSSA-Metrics#DREAD
  ou www.owasp.org/index.php/Threat_Risk_Modeling#DREAD

/ RÉGLEMENTATION (DE SÉCURITÉ)

- Le lecteur pourra se reporter au site de l'ANSSI qui présente un panorama des textes réglementaires en matière de sécurité numérique relatifs à la protection des systèmes d'information, à la confiance numérique, ainsi que plus spécifiquement à la cryptographie ou à d'autres réglementations techniques :
  www.ssi.gouv.fr/entreprise/reglementation

- Concernant la sécurité numérique des systèmes d'information d'importance vitale (SIIV), régie par l'article 22 de la loi de programmation militaire, le lecteur pourra consulter le lien suivant :
  www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france

CONTRIBUER À CE GUIDE

La présente version du guide ne constitue qu'un point de départ. Comme toute équipe agile, nous nous engageons à tenir compte des enseignements que nous apportera sa mise en œuvre réelle par des équipes que nous espérons variées autant que motivées.

Nous vous invitons donc à essayer pour vous-même, en l'état ou en les adaptant, les conseils et pratiques qui y sont décrits et à nous transmettre vos retours à l'adresse **securite-agile@beta.gouv.fr** – afin que d'autres équipes puissent, à leur tour, profiter de votre expérience et continuer à l'enrichir.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Coréalisé par l'ANSSI et la DINSIC, ce guide explique de manière pratique et concrète comment l'agilité et la sécurité concourent au développement sécurisé des projets et à la gestion du risque numérique. En s'appuyant sur l'expérience de celles et ceux qui la mettent en œuvre et la font vivre au quotidien, la présente méthode fait écho aux enjeux auxquels sont confrontées les équipes chargées de livrer à leurs usagers un produit ou un service dans un temps contraint.

Octobre 2018

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI – 51, boulevard de la Tour-Maubourg – 75700 PARIS 07 SP
www.ssi.gouv.fr / communication@ssi.gouv.fr

-

DIRECTION INTERMINISTÉRIELLE DU NUMÉRIQUE ET DU SYSTÈME D'INFORMATION ET DE COMMUNICATION DE L'ÉTAT
DINSIC - 20, avenue de Ségur - 75007 Paris
www.numerique.gouv.fr / communication.dinsic@modernisation.gouv.fr