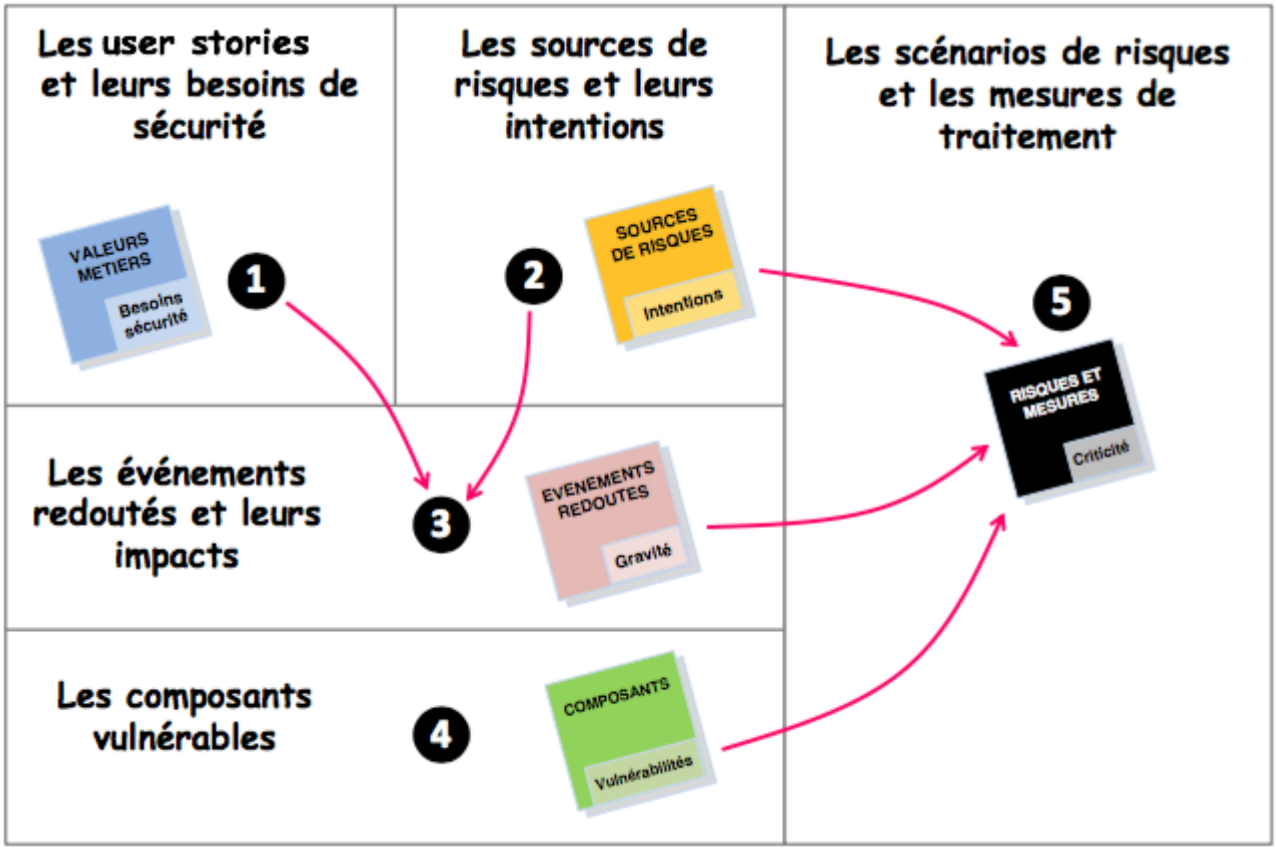
Conception Agile et sécurité

Inspiré du guide “Conception Agile et sécurité” pulié par l'ANSSI.

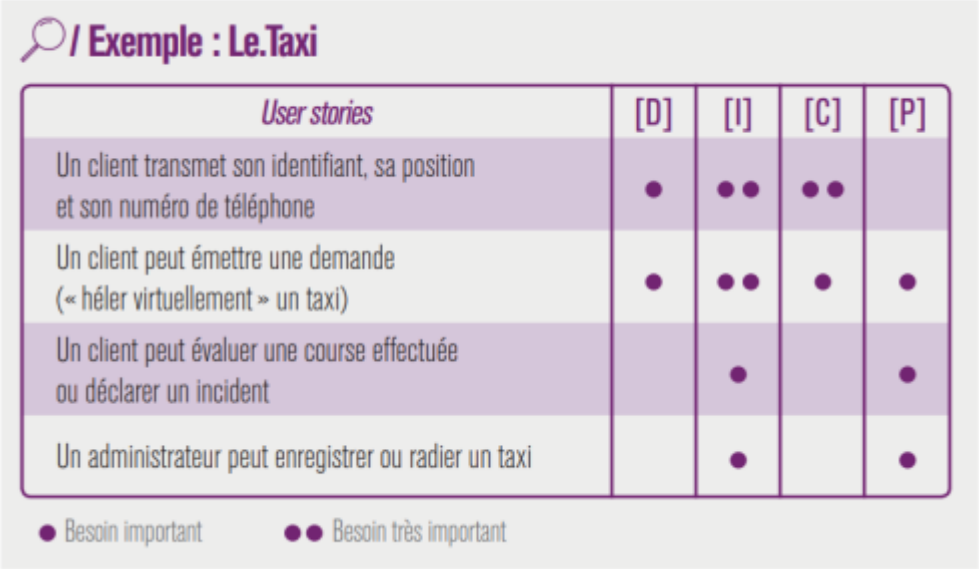
Démarche d'identification et de traitement des risques dans un contexte AGILE.



1- Besoins de sécurité

Pour chaque US, identifier les besoins de sécurité en utilisant la matrice DICP :

- **[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

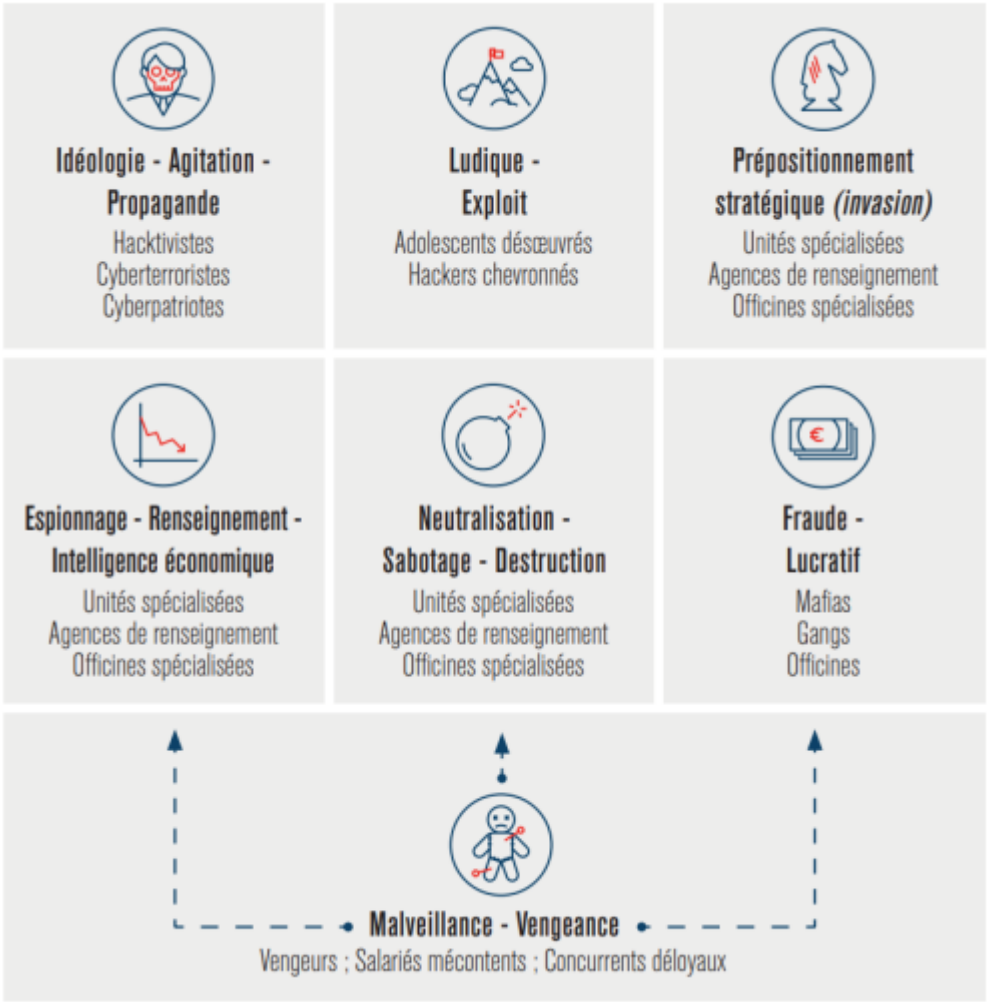


Il est également possible de partir d'un besoin (DICP), et de déterminer les US qui sont concernées par lui.

2 - Sources de risque

Recensement des 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 :



Evènements redoutés et conséquences

Un événement redouté (ER) correspond au non-respect d'un besoin de sécurité. Il peut être exprimé sous la forme d'une expression courte permettant de comprendre facilement le préjudice lié à la user story concernée.

Exemple :

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	●

Ecosystème et composants vulnérables

Identification des composants du produit :

- 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.

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

Scénarii de risque : abuser stories

Consiste à 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 , les événements redoutés et les composants vulnérables.

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

Pour chaque abuser story répertoriée, définir si besoin l'option de traitement du risque la plus appropriée

- Eviter,
- Réduire,
- Transférer
- Accepter