


Conception Agile et sécurité

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

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

 / 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		●		●

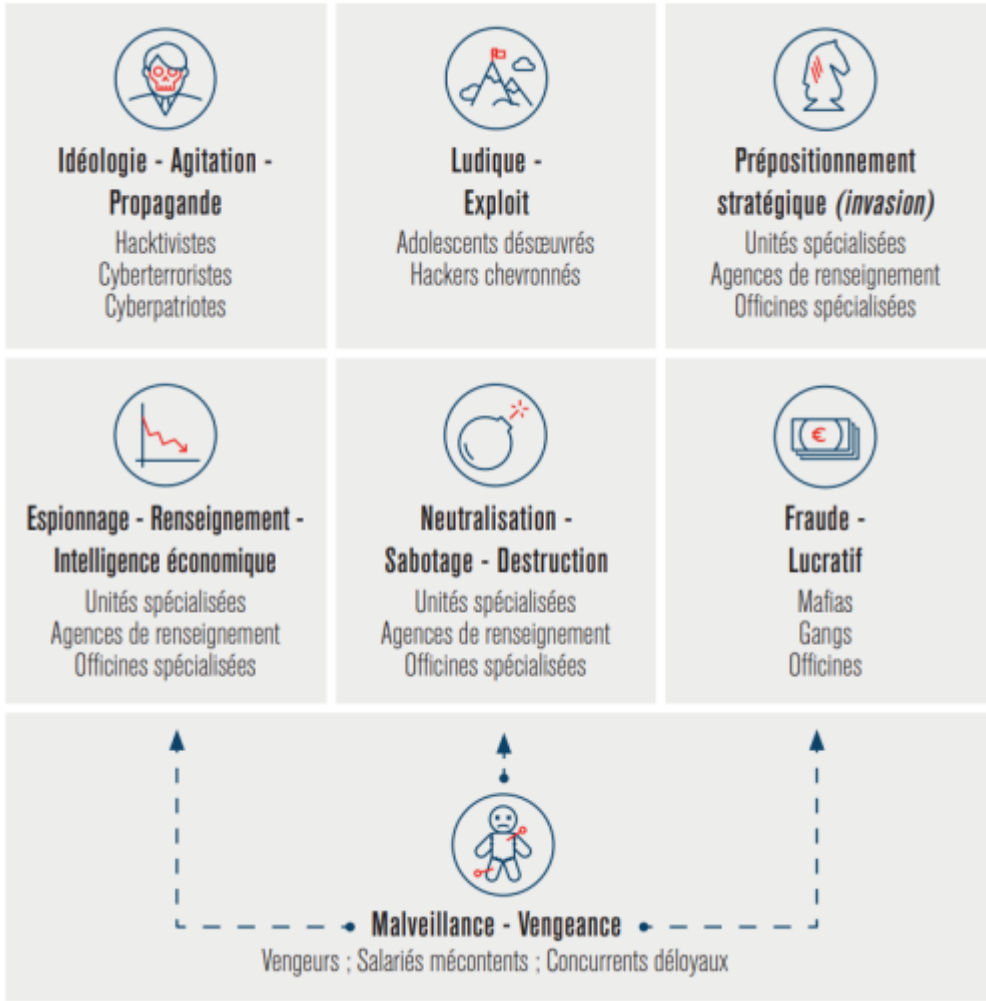
● Besoin important ●● Besoin très important

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

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 évènement redouté (ER) correspond au non-respect d'un besoin de sécurité. Il peut être exprimé sous la forme d'une expression courte qui permet 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



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.

From:

<http://slamwiki2.kobject.net/> - **Broken SlamWiki 2.0**

Permanent link:

http://slamwiki2.kobject.net/sio/bloc3/agile_security?rev=1697756981

Last update: **2023/10/20 01:09**

