



AGILITÉ & CYBERSÉCURITÉ

MÉTHODE ET OUTILS À L'USAGE DES
ÉQUIPES PROJET

Philippe Menut
Co-Gérant SITALIS
Gérant PSL-SI

PRESENTATION



✓ **Notre objectif : accompagner les TPE/PME de la région dans leurs démarches de sécurisation et de protection de leur patrimoine numérique**

✓ **Formations**

- **Hygiène numérique**
- **Analyse de risque**
- **Accompagnement de projet agile**

Née des constats suivants :

- La numérisation des activités professionnelles est grandissante, quelque soit le métier.
- Les TPE/PME ne sont pas suffisamment « armées » face aux risques, qui eux sont bien réels.
- Les impacts trop souvent sous-évalués et il est généralement trop tard quand un incident survient.

- ✓ Le risque cyber est un risque grandissant.
- ✓ Sa prise en compte doit être réelle et totale.
- ✓ La cybersécurité, n'est pas une surcouche d'un projet.
- ✓ La sécurité doit être intégrées, au plus tôt et en permanence, dans la conduite de projets agile
- ✓ L'objectif est de nourrir efficacement :
 - la prévention des risques numériques
 - la détection des cyberattaques.
- ✓ devoir de conseil des acteurs du numérique



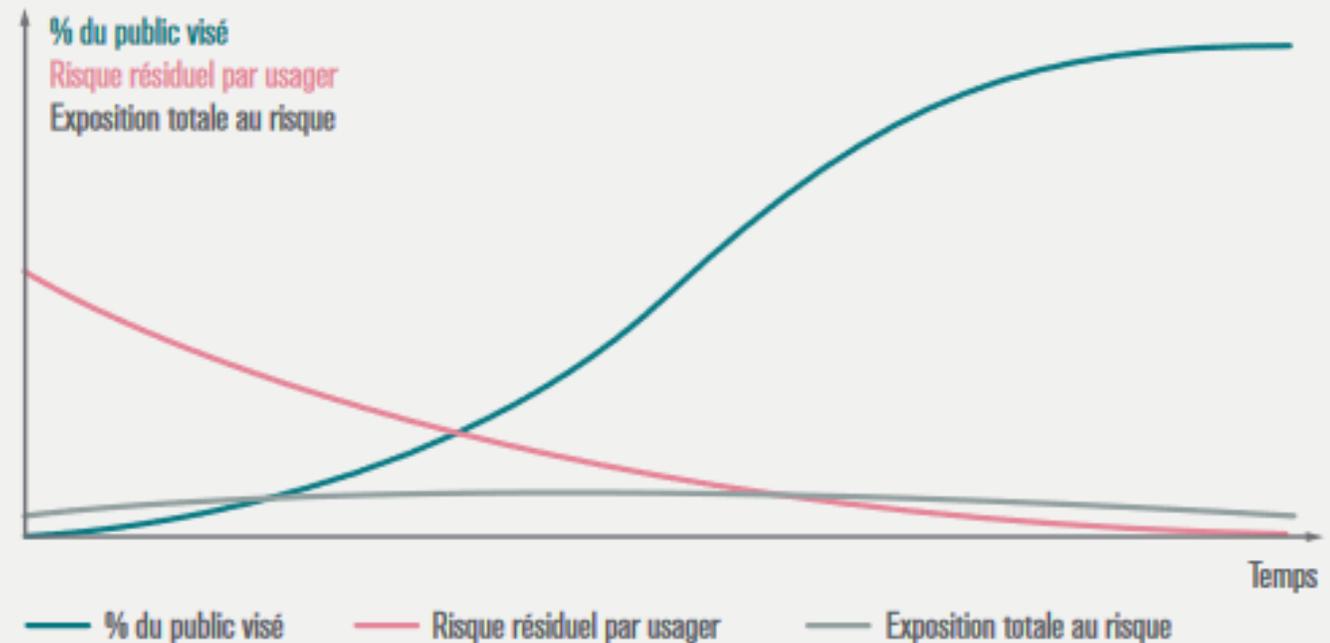
Introduction

Le Coeur de la démarche
repose sur l'organisation
d'ateliers d'appréciation des
risques

LA CLÉ DE LA COMPATIBILITÉ AGILE

- ✓ **Prise en compte incrémentale du risque**
 - Considérer simultanément le nombre d'usagers et le risque encouru par chacun
- ✓ **prise en compte des enjeux de sécurité**
 - Continue
 - pragmatique

Exposition au risque résiduel d'un produit



- ✓ L'atelier d'analyse de risque vu comme un nouvel « rituel » agile
- ✓ Le premier atelier :
 - cadrer le périmètre
 - analyser de risque global
- ✓ Formaliser les résultats à l'issue de chaque atelier
- ✓ Itération après itération, actualiser et affiner



CONCRÈTEMENT, LE CŒUR DE LA DÉMARCHE

L'ATELIER D'ANALYSE DE RISQUE



L'APPRÉCIATION DES RISQUES

RISQUES

LES BASES À CONNAITRE ET À TRANSMETTRE

✓ Les users stories revêtent un enjeu de sécurité vis-à-vis de l'un ou l'autre des critères DICP

- [D] Disponibilité
- [I] Intégrité
- [C] Confidentialité
- [P] Preuve

✓ Définir les besoins de sécurité



L'APPRÉCIATION DES RISQUES

LES ÉTAPES

User stories	[D]	[I]	[C]	[P]
Un client transmet son identifiant, sa position et son téléphone	○	○○	○○	
Un client peut émettre une demande	○	○○	○	○
Un client peut évaluer un service ou déclarer un incident		○		○

○ besoin important ○○ Besoin très important

✓ Définir les événements redoutés

Événement redoutés	Impacts métier	Gravité
Le système ne répond pas	Expérience utilisateur dégradée Perte de client	○
Un opérateur émet de fausses informations	Qualité de service dégradée Perte de client	○○

○ modéré ○○ très élevé

✓ Les risques résultent de la combinaison des éléments de l'analyse et sont décrits par un scénario de menace intentionnel ou accidentel

- ✓ Ateliers d'appréciation des risques
 - abuser story
 - scénario accidentel
- ✓ Gérer les abuser story et scénario accidentel dans le backlog
- ✓ Se concentrer sur les risques numériques liés aux cas d'usage du produit
- ✓ Privilégier les abuser stories (scénarios intentionnels)



L'APPRÉCIATION DES RISQUES

SYNTHÈSE : L'AGILITÉ &
CYBERSÉCURITÉ



SITALIS

MERCI DE
VOTRE
ATTENTION

Philippe Menut



06 72 76 30 38



pmenut@sitalis.fr



www.sitalis.fr

