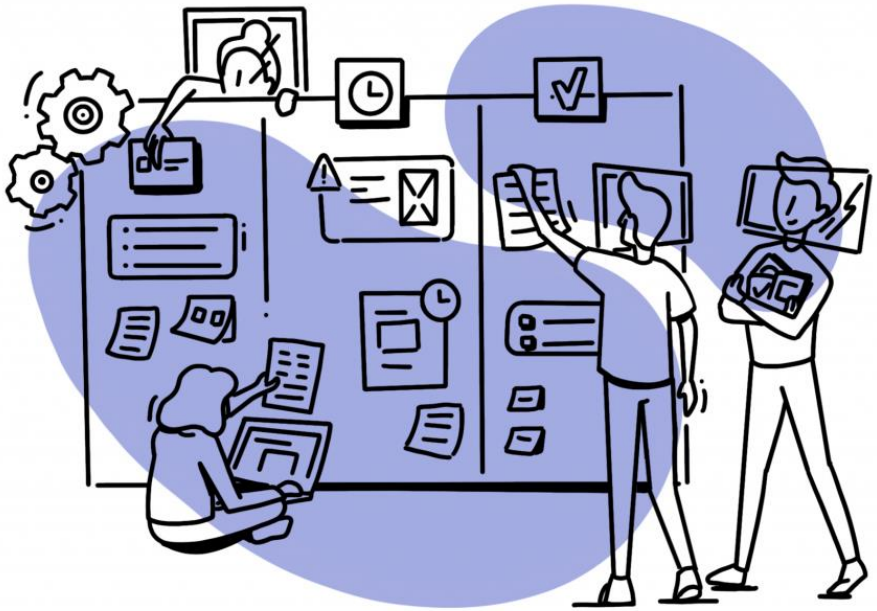


Projet GED'IMAGINATION
Approche agile / Security By Design

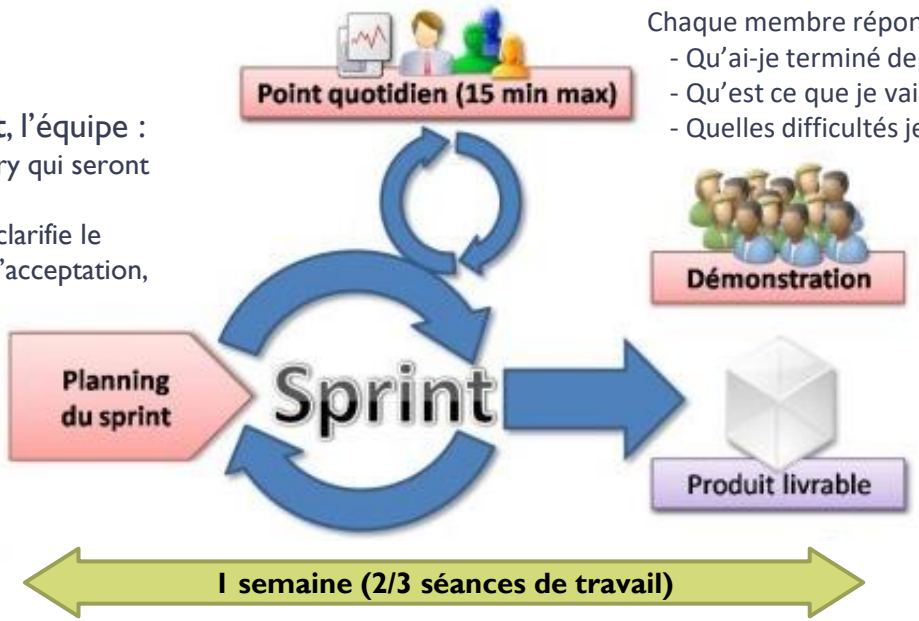
BTS SIO2 SLAM

Notre gestion de projet agile

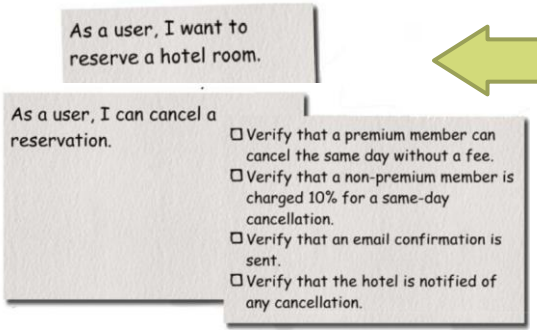
- Déroulement d'un sprint

Une mêlée au début de chaque séance
Chaque membre répond à 3 questions :
- Qu'ai-je terminé depuis la dernière mêlée ?
- Qu'est ce que je vais faire d'ici la prochaine mêlée ?
- Quelles difficultés je rencontre ou je pense rencontrer ?

Au début d'un sprint, l'équipe :
- sélectionne la/les user story qui seront développées
- affine chaque user story : clarifie le besoin, définit les critères d'acceptation, ajuste l'estimation, découpe en tâches
- réfléchit à la solution d'implémentation (conception fonctionnelle et technique)



Revue en fin de sprint
- Démo des fonctionnalités développées
- Feedback de l'équipe et du PO
- Améliorations possibles pour le prochain sprint



Sprint 1

User Story	Scénario / Critères d'acceptation
[*AppWeb*] **User Story N°4** **En tant que** participant, **je souhaite** poster ma réalisation	**Etant donné** que je suis connecté à l'application web, **lorsque** je demande de participer au concours **alors** je peux saisir les caractéristiques de ma réalisation et poster la photo correspondante ✓ : ma participation est confirmée ✘ : ma photo est trop volumineuse ✘ : j'ai déjà participé (posté une photo), je ne peux plus participer ✘ : je suis hors période de participation, je ne peux pas participer

Evil User Stories	Security User Story - ***Mesures de sécurité à mettre en place***
En tant qu'attaquant , **je veux** injecter du code malveillant (injections SQL / XSS) dans les champs de saisie non sécurisés	**En tant que** développeur, **je veux** m'assurer que les attaques par injection de code sont évitées • *Filtrer les entrées utilisateurs, échapper tous les caractères spéciaux avant d'insérer les données dans une requête* • *Utiliser des requêtes préparées ou des procédures stockées*
En tant qu'attaquant, **je veux** prendre le contrôle du serveur en envoyant un fichier infecté	**En tant que** développeur, **je veux** m'assurer que les fichiers téléchargés sont sains • *Définir une liste blanche des extensions de fichier autorisées et refuser tout autre type de fichier* • *Réaliser un scan antivirus du fichier avant de l'envoyer sur le serveur*

Sprint 1

- User Story N°4 - Découpage en tâches
  - Modéliser la base de données (tables utiles)
  - Créer les tables et insérer un jeu de données
  - Maquetter la page / le formulaire
  - Créer le formulaire et coder les traitements en mettant en place les mesures de sécurité
  - Tester (couverture des tests d'acceptation)
  - Préparer la démo
  - Actualiser la documentation