# STI – Analyse de menace

1. Description du système
   1. Objectifs du système

* Permettre aux utilisateurs de communiquer par message
* Réputation : les messages doivent arriver au destinataire voulu et être visibles uniquement par le/les destinataires.
  1. Hypothèses de sécurité
* Réseau interne et administrateurs de confiance
* Système d'exploitation et serveur Web de confiance
  1. Exigences de sécurité :
* Le site Web doit être disponible à 99% du temps (disponibilité)
* Les informations des utilisateurs doivent être scrupuleusement protégées (privacy)
* Les informations accédées par les utilisateurs ne doivent pas pouvoir être tracées (privacy)
* Seul un administrateur doit pouvoir ajouter/modifier/supprimer un utilisateur
* Les mails reçus par un utilisateur ne doivent être visibles que pour lui (privacy)
  1. Eléments du système :
* Base de données des utilisateurs
* Base de données des messages
* Application Web
  1. Rôles des utilisateurs :
* Collaborateur
* Administrateur (même droits que collaborateurs + options administrateur)
* Webmasters (gestion du site)
  1. Actifs à haute valeur :
* Base de données des utilisateurs (données)
  + Confidentialité, sphère privée
  + Un incident nuirait à la réputation du site
* Base de données des messages (données)
  + Confidentialité (messages privés entre collaborateur)
  + Intégrité (une modification impliquerait une baisse de réputation)
* Base de données des logs (données)
  + Confidentialité, sphère privée (possibilité de connaître la liste des accès)
  + Intégrité (prouver les actions des utilisateurs)
  + En cas d'incident les utilisateurs ne peuvent répudier leurs actions
* Infrastructure
  + Intégrité, disponibilité
  + Un incident serait critique et nuirait à la disponibilité/réputation
  1. DFD

Une image contenant texte, carte, ciel, divers

Description générée automatiquement

1. Identification des sources de menaces
   1. Sources de menace

* Hackers, script-kiddies
  + Motivation : s'amuser, gloire
  + Cible : n'importe quel élément / actif
  + Potentialité : haute
* Cybercrime (spam, maliciels)
  + Motivation : récupération d’information / nuire aux utilisateurs
  + Cible : vol de credentials des utilisateurs, spam des utilisateur, modification / récupération d'informations
  + Potentialité : haute
* Concurrent
  + Motivation : détruire la réputation du site
  + Cible : base de données des utilisateurs / base de données des messages
  + Potentialité : faible

1. Identification des scénarios d’attaque