dépasser les frontières

ANF – Nouvelles Menace Sécurité des Applications Web

Module 3.3 – Analyse des risques et modélisation des menaces
Janvier 2017
45 minutes
Jérémie Boutard

Introduction

« Le bistrot est utile à un dialoguiste, mais il y a un risque : l'alcoolisme. »

- Michel Audiard

Introduction

- Qu'est-ce qui est le plus grave ?
  - (A) Injection SQL (A1) ?
  - (B) Mauvaise configuration sécurité (A5) ?
  - (C) Cross-Site Scripting (XSS) (A3) ?
  - (D) Utilisation de composants avec des vulnérabilités connues (A9) ?

Introduction

- Qu'est-ce qui est le plus grave ?
  - (A) Injection SQL (A1)… sur la page institutionnelle du site du CNRS permettant une défiguration ?
  - (B) Mauvaise configuration sécurité (A5) … en utilisant une clé de chiffrement faible sur le service HTTPS de MyCore permettant de capter des données sensibles ?
  - (C) Cross-Site Scripting (XSS) (A3) … sur le portail d'authentification du CNRS permettant de récupérer les mots de passe des utilisateurs ciblés ?
  - (D) Utilisation de composants avec des vulnérabilités connues (A9) … sur la badgeuse de la cantine permettant de déjeuner gratuitement ?

Introduction

- Conclusion :
  - Le risque ne se réduit pas à des aspects techniques
  - Nous n'avons pas tous la même perception de ce qui est grave, des risques et du « modèle de menace »

- En poussant l'exercice plus loin :
  - Nous ne serions pas du même avis quand aux techniques de « réduction » de ces risques
  - Nous ne serions pas non plus du même avis quand à la « priorisation » liée à ces améliorations

Agenda

- Théorie du risque
- Modèle de menace
- Evil user stories

Définitions

- La plupart disponibles ici : http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(F).zip

- En suivant, proposition de quelques définitions clés

Définitions

- Actif / bien : tout élément (appartenant ou contrôlé par l'organisation) représentant de la valeur pour l'organisation (un bénéfice peut en être obtenu)
  - Actifs primordiaux (principaux, primaires, essentiel) ~ intangibles
    - Processus et activités métiers
    - Informations
  - Actifs de soutien (support, secondaires)
    - Cadre organisationnel
    - Site
    - Personnel
    - Réseau
    - Logiciel
    - Matériel

Définitions

- **Sécurité de l'information** : protection de la *confidentialité*, de *l'intégrité* et de la *disponibilité* de l'information
- **Incident lié à la sécurité de l'information :** un ou plusieurs événements liés à la sécurité de l'information, indésirables ou inattendus, présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information

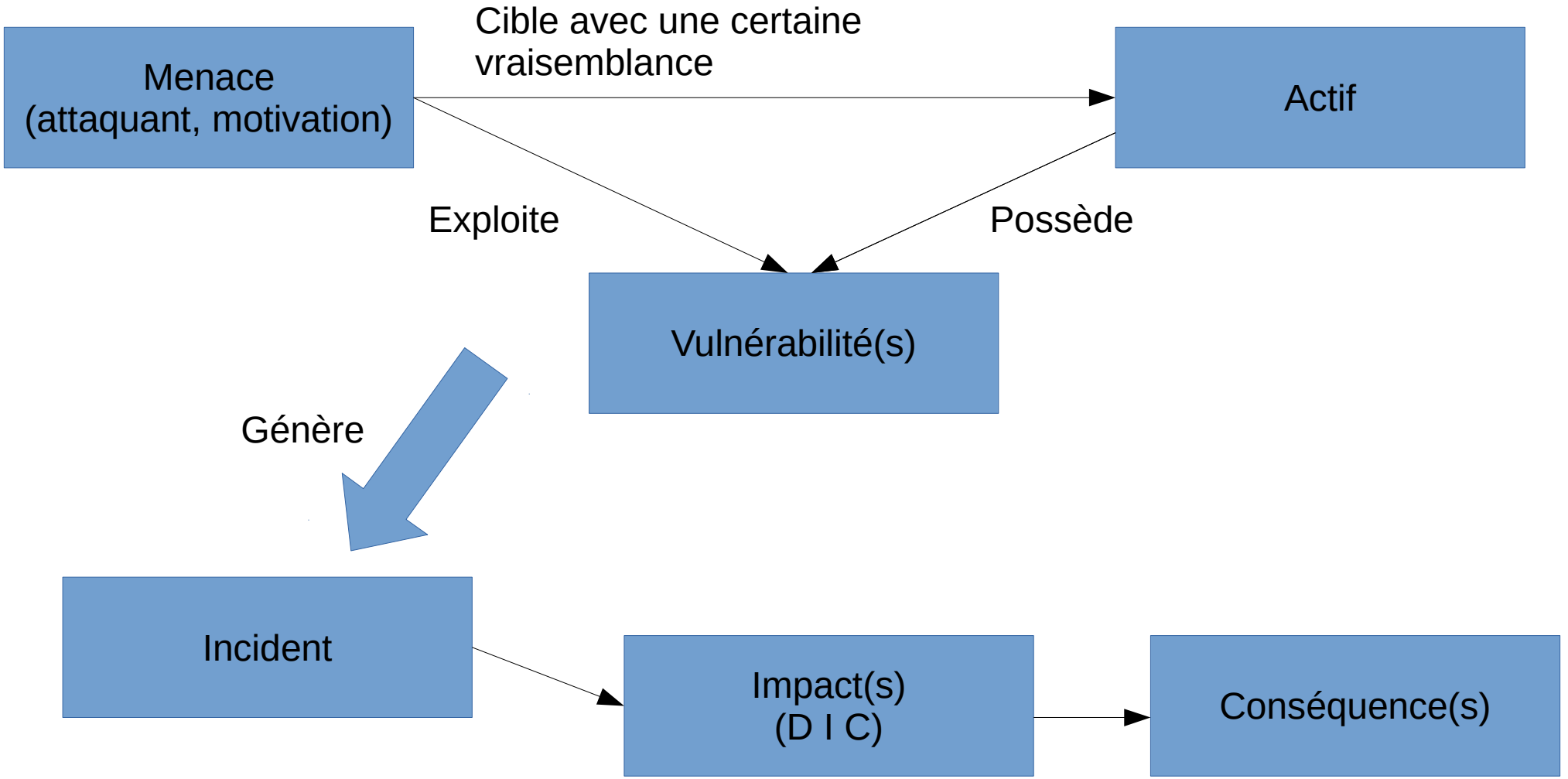
Définitions

- **Conséquence** : effet d'un événement affectant les objectifs
- **Vulnérabilité** : faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces
- **Vraisemblance (probabilité d'occurrence)** : possibilité que quelque chose se produise
- **Menace** : cause potentielle d'un incident indésirable qui peut nuire à un système ou un organisme
- **Scénario de menace** : Enchaînement spécifique d'actions par un ou plusieurs agents de menace menant à l'atteinte, intentionnelle ou accidentelle, d'un état ou d'un événement indésirable pour l'organisation

Définitions

- **Risque** : effet de l'incertitude sur l'atteinte des objectifs
- **Niveau de risque** : importance d'un risque exprimé en terme de combinaison des conséquences et de leur vraisemblance
- **Mesure de sécurité** : mesure qui modifie un risque
- **Risque résiduel** : risque subsistant après le traitement du risque

Scénario de risque



Scénario de risque

- Un scénario de risque en une phrase :
  - Une menace cible un actif en exploitant une vulnérabilité selon une certaine vraisemblance ce qui génère un incident de sécurité qui aura un impact sur la sécurité et aura des conséquences pour l'organisme

  - Exemple :

    Un utilisateur mécontent, possédant des compétences informatiques et du matériel simple, utilise une injection SQL sur le site institutionnel du CNRS. Ceci aura pour impact de défigurer le site (perte d'intégrité) et aura pour conséquence une perte d'image de l'unité et une charge de personnel pour remettre le site en place.

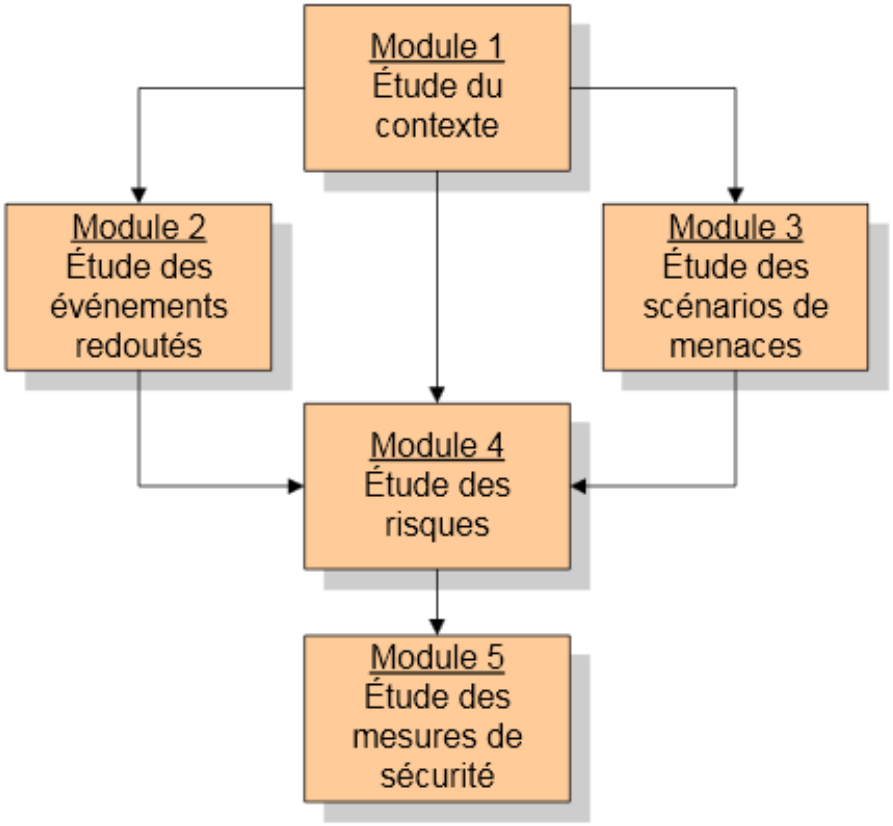
Scénario de risque

- Dans un tableau « d'analyse de risque » :

Actif	Menace	Vraisemblance	Vulnérabilité	Impact (DIC)	Conséquence	Niveau de risque
Web institutionnel du CNRS	Utilisateur mécontent	Moyenne (connaissance et matériel simple	Injection SQL	Défiguration (intégrité)	- Perte d'image - Charge de restauration	Moyen

- Étape suivante, définir des échelles pour rendre cartésien le niveau de risque :
  - risque = (vraisemblance x impact x conséquence)
  - Permettra d'objectiver la priorisation des actions de réduction de risque (seuil d'acceptation du risque, responsabilité hiérarchique de la prise de risque)

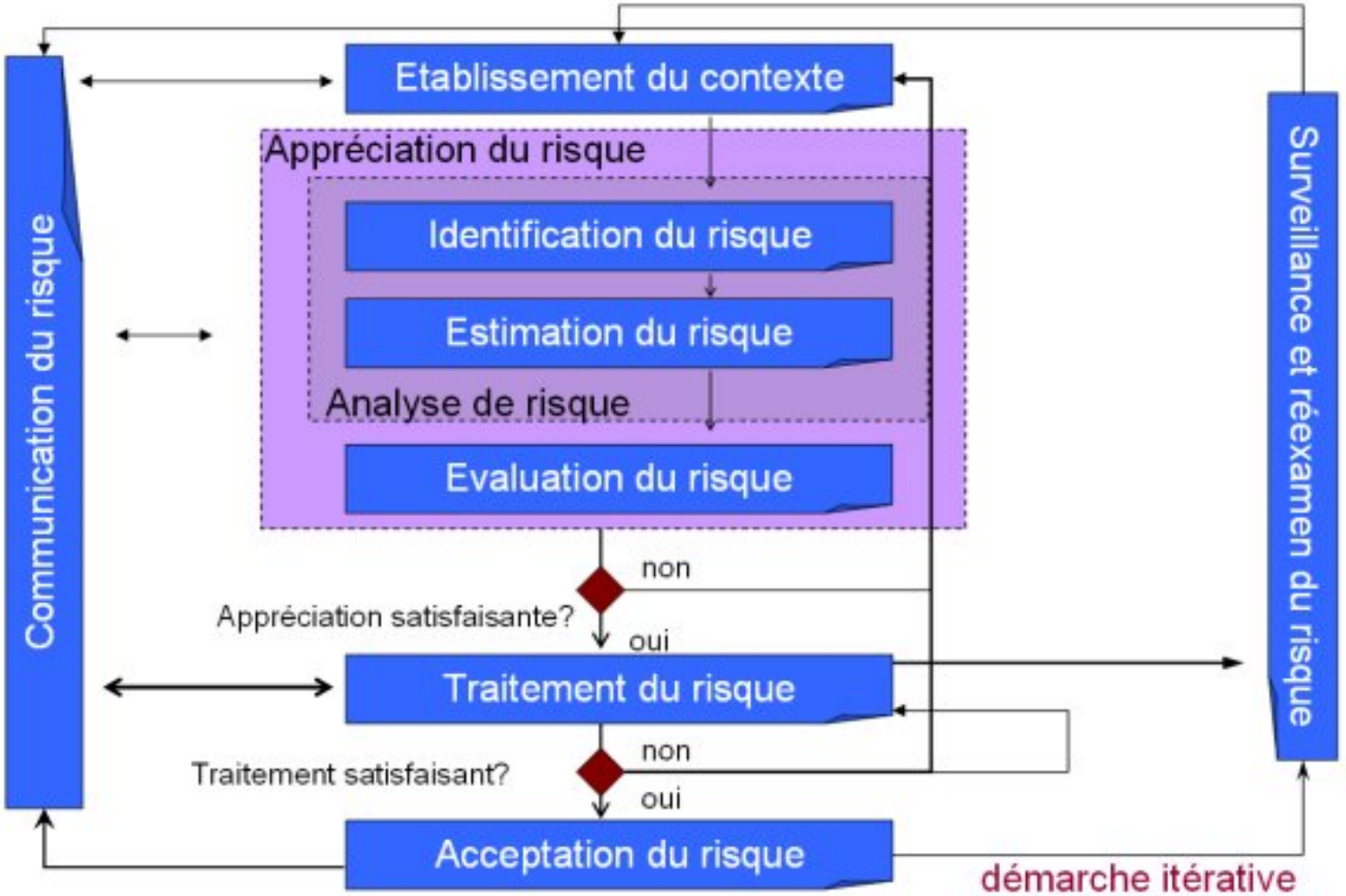
Méthode d'analyse de risque EBIOS2010



https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

Méthode de management du risque ISO27005

- https://fr.wikipedia.org/wiki/ISO/CEI_27005



Plus proche du développeur : Le Modèle de Menace

Définition :

- Un processus pour identifier et documenter les menaces auxquelles un système est exposé et les mesures à mettre en œuvre pour les contrer, les détecter ou les atténuer

- Processus améliorable et répétable
- Activité à réaliser tôt dans le cycle de développement
  - Durant la conception, optimise le traitement du risque et optimise les coûts en limitant les corrections/ajustement et limite les investissements disproportionnés
- Simple
  - Crayon, pizza, café

Le Modèle de Menace

Le processus vise à définir :

- Des menaces s'exerçant sur l'application
- Des scénarios d'incident
- Des mesures pour réduire l'impact et les conséquences des scénarios de menace (bloquer, détecter, atténuer)
- Aide à prioriser les efforts de sécurité

⇒Pas si différent des concepts vu auparavant

Le Modèle de Menace

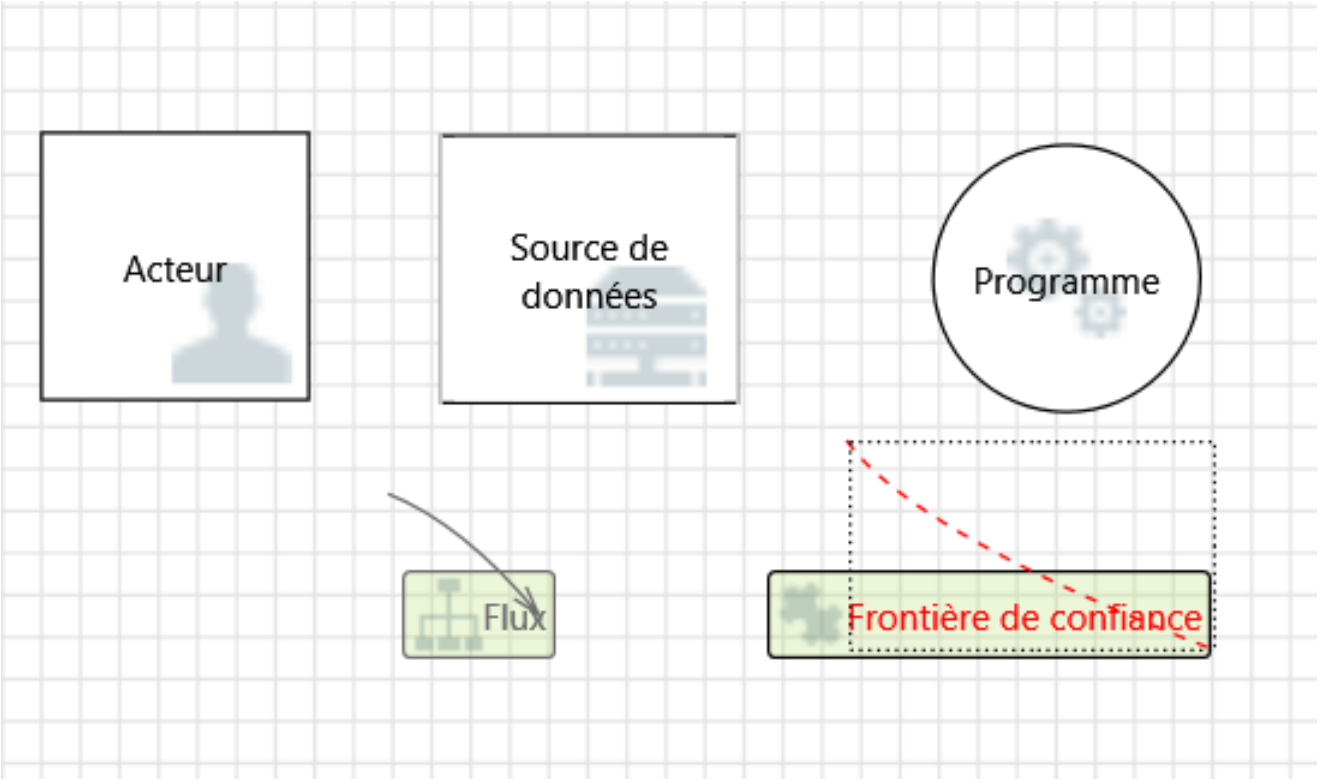
- 3 étapes de haut niveau :
  - Décomposer l'application
  - Déterminer et évaluer les menaces
  - Déterminer les mesures de sécurité

Le Modèle de Menace : Décomposer l'application

- Objectifs :
  - Comprendre le fonctionnement de l'application
    - Actifs
  - Déterminer les différentes interactions avec l'extérieur
    - Dépendances externes
    - Points d'entrée
    - Niveaux de confiance
- Sources :
  - Revue documentaire
  - Collecte d'information

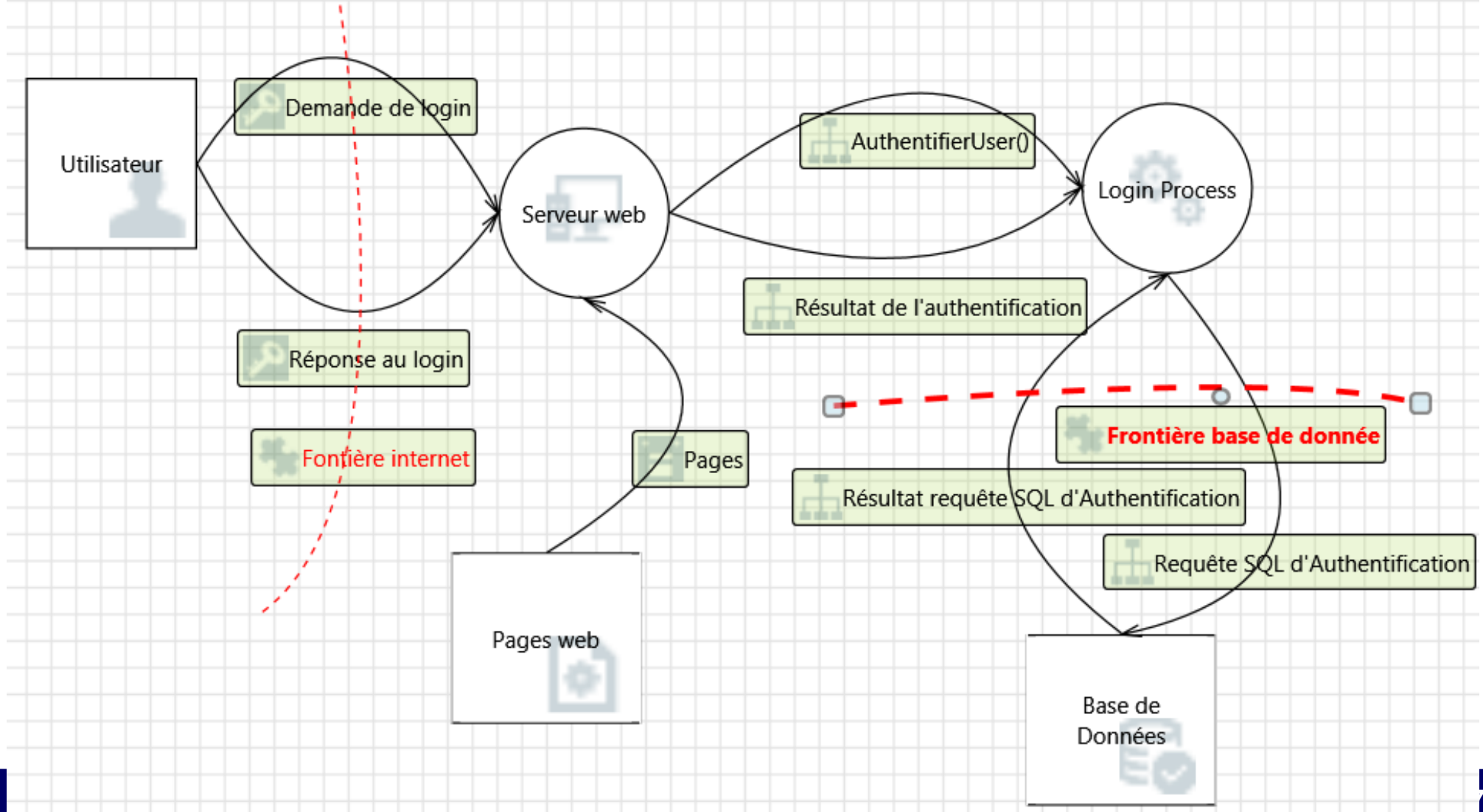
Le Modèle de Menace : Décomposer l'application

- Outil : Data Flow Diagram
  - Simple, compréhensible



Le Modèle de Menace : Décomposer l'application

- Exemple (Microsoft Threat Modeling Tool 2016) :



Le Modèle de Menace : Déterminer et évaluer les menaces

- Objectifs
  - Catégoriser les menaces
  - Évaluer les menaces

Le Modèle de Menace : Déterminer et évaluer les menaces : Catégoriser les menaces

- STRIDE
  - Utilisation sur le DFD de catégorie de menace « standard »
    - Spoofing identity : usurpation d'identité
    - Tampering with data : altération des données
    - Repudiation : Répudiation ;-)
    - Information disclosure : divulgation d'informations
    - Denial of service : Déni de service
    - Elevation of privilège : Élévation de privilège

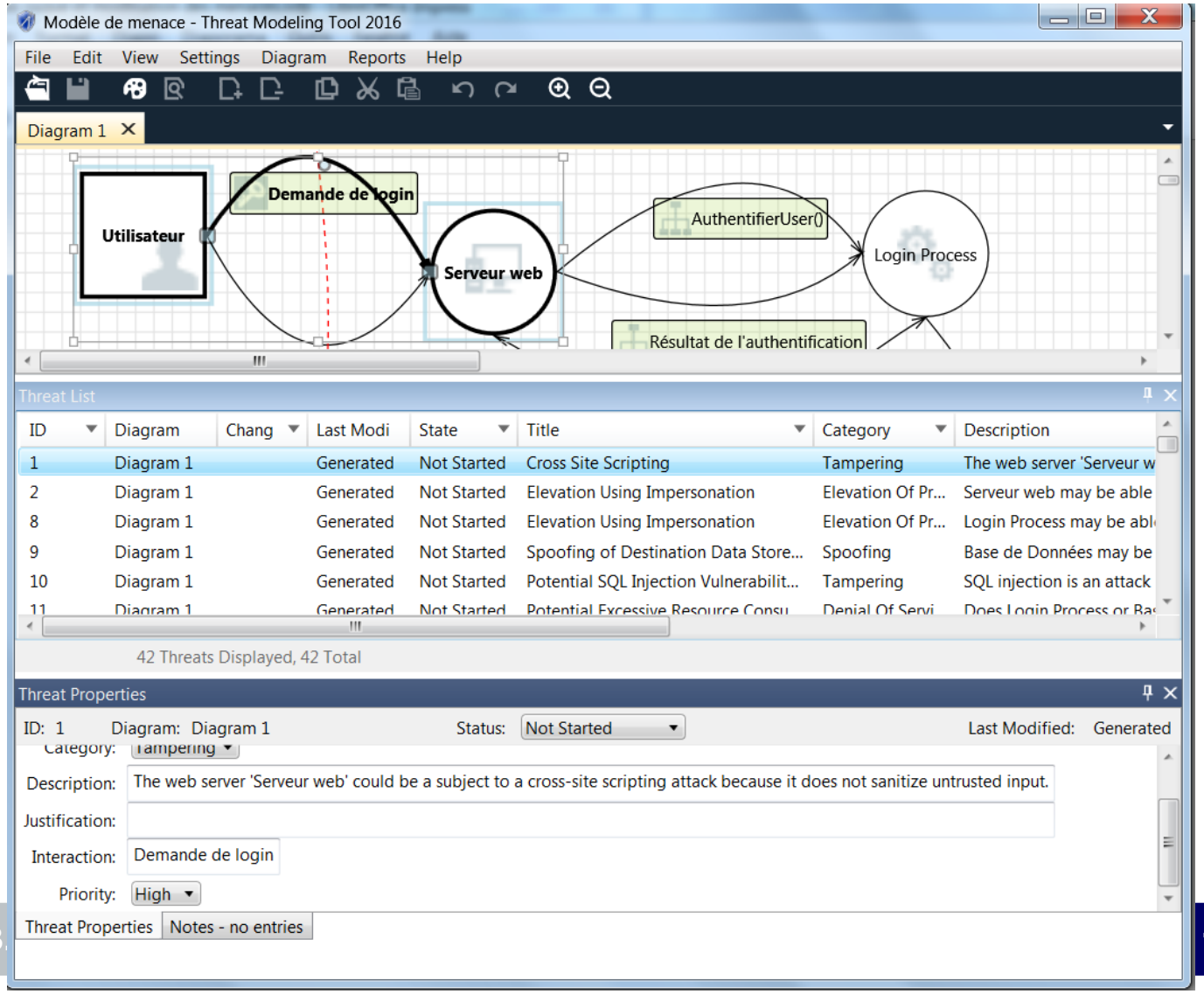
Le Modèle de Menace : Déterminer et évaluer les menaces : Catégoriser les menaces

- Exemple 1

Catégorie	Scénario de la menace
Usurpation d'identité	L'attaquant va accéder aux login et mot de passe d'un autre utilisateur pour les utiliser « illégalement » en écoutant sur un canal faiblement chiffré
Altération des données	L'attaquant va modifier les authentifiants des utilisateurs dans la base de données ou sur le flux internet en utilisant une injection SQL
Répudiation	L'attaquant va nier avoir utilisé ses informations d'authentification en utilisant le fait qu'il n'existe pas de système de trace
Divulgation d'information	L'attaquant va lire les informations d'authentification (dans le cache du navigateur par exemple) en utilisant un XSS
Deni de service	L'attaquant va saturer le formulaire d'authentification et d'empêcher l'accès au service
Élévation de privilège	Après authentification, l'attaquant va obtenir plus de privilège en endossant les droits d'un autre utilisateur en utilisant une référence directe aux objets

Le Modèle de Menace : Déterminer et évaluer les menaces : Catégoriser les menaces

- Exemple 2 (Microsoft Threat Modeling Tool 2016)



Le Modèle de Menace : Déterminer et évaluer les menaces : Évaluer les menaces

- DREAD
  - Utilisation sur le STRIDE d'une méthode d'évaluation des menaces
    - Damage potential : Potentiel de dommages: Quelle est la gravité des dommages si la vulnérabilité est exploitée?
    - Reproductibility : Reproductibilité: Comment est-il facile de reproduire l'attaque?
    - Exploitability : Exploitabilité: Comment est-il facile de lancer une attaque?
    - Affected users : Utilisateurs concernés: En pourcentage, combien d'utilisateurs sont touchés?
    - Discoverability : Découvrir: Comment est-il facile de trouver la vulnérabilité ?
  - Calcul du score : avec chaque critère sur 10 : (D + R + E + A + D) / 5

Le Modèle de Menace : Déterminer et évaluer les menaces : Évaluer les menaces

- Exemple

Catégorie de menace	Scénario de la menace	DREAD	Niveau de risque
Usurpation d'identité	L'attaquant va accéder aux login et mot de passe d'un autre utilisateur pour les utiliser « illégalement » en écoutant sur un canal faiblement chiffré	Damage : données de valorisation : 10	9
		Reproductibility : très facile : 10	
		Exploitability : être sur le même réseau : 5	
		Affected users : tous : 10	
		Discoverability : facile : 10	
Altération des données	L'attaquant va modifier les authentifiant des utilisateurs dans la base de données en utilisant une injection SQL	Damage : perte d'accès, temps de travail : 7	7
		Reproductibility : compliqué : 5	
		Exploitability : exposition internet : 10	
		Affected users : tous : 10	
		Discoverability : il faut être authentfié : 3	

Le Modèle de Menace : Déterminer les mesures de sécurité

- Pour chaque type de menace, déterminer si des mesures de sécurité sont déjà implémentées pour réduire les vulnérabilités

- Et estimer si ces mesures :
  - Ne réduisent pas le risque (mesures inutiles dans ce contexte?)
  - Réduisent partiellement ces risques
  - Réduisent totalement ces risques

Le Modèle de Menace : Déterminer les mesures de sécurité

- Selon le niveau de risque, estimer si une action est à envisager (selon l'ISO27005) :
  - Le refus ou évitement : le risque considéré est trop élevé, l'activité amenant le risque doit être supprimée
  - Le transfert : le risque sera transféré à une autre entité (un assureur, un sous-traitant) capable de le gérer
  - La réduction : le risque doit être diminué. Il s'agit de réduire l'impact du risque de manière que le risque soit acceptable. Implémentation d'une nouvelle mesure
  - Conservation du risque : le risque est maintenu tel quel.

Le Modèle de Menace : Déterminer les mesures de sécurité

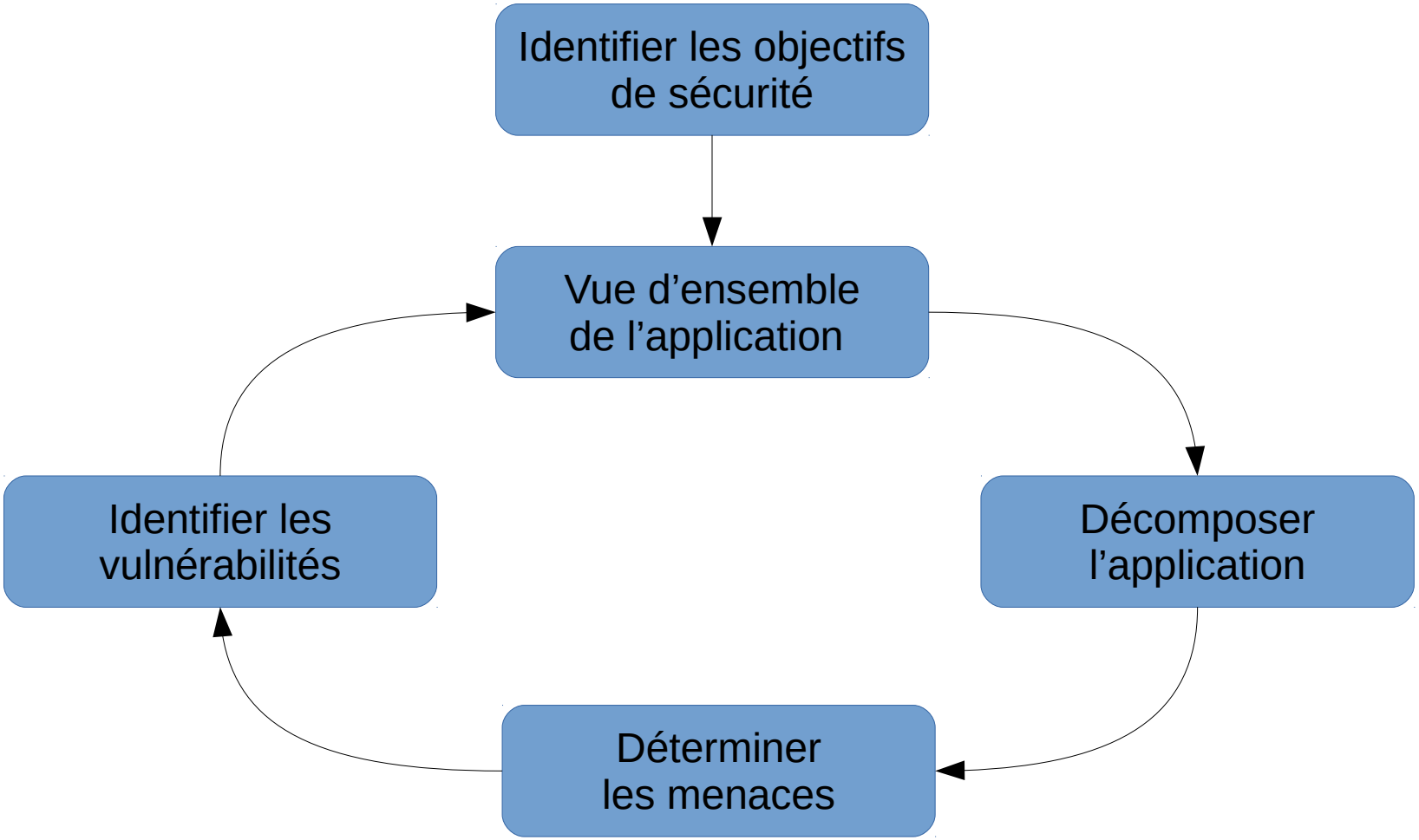
- Exemple

Catégorie de menace	Scénario de la menace	Niveau de risque	Mesure déja implémentée	Traitement du risque	Niveau de risque résiduel
Usurpation d'identité	L'attaquant va accéder aux login et mot de passe d'un autre utilisateur pour les utiliser « illégalement » en écoutant sur un canal faiblement chiffré	9	Aucune	Réduction : Implémenter mise en place HTTPS	2
Altération des données	L'attaquant va modifier les authentifiant des utilisateurs dans la base de données en utilisant une injection SQL	7 (2 avec la mesure déjà implémentée)	Contrôle des entrées	Conservation	2

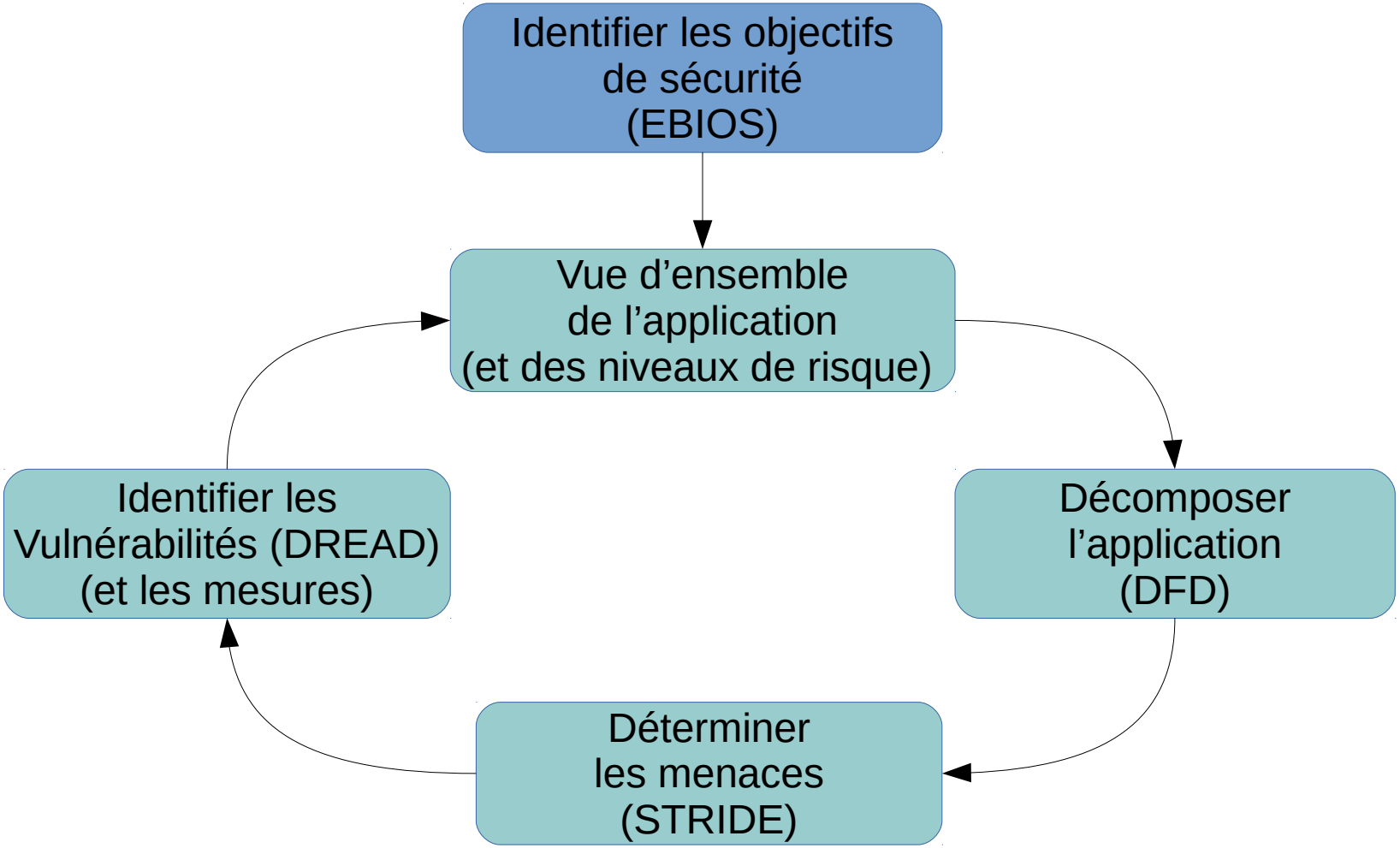
Le Modèle de Menace : Déterminer les mesures de sécurité

- Quelques points organisationnels :
  - Partager le modèle de menaces avec tous les acteurs du projet :
    - Équipe de développement
    - Direction
    - Hiérarchie
    - Maîtrise d'ouvrage
    - Adminsys
    - Partenaire
    - Etc.
  - Faire valider la priorisation par les parties prenantes (cf. ci-dessus)
  - Échanger avec ses homologues dans l'unité et dans les réseaux métiers

Le Modèle de Menace : processus complet d'amélioration continue



Le Modèle de Menace : processus complet d'amélioration continue



Le Modèle de Menace : pour aller plus loin

- Quelques références documentaires :
  - https://msdn.microsoft.com/fr-fr/library/f13d73y6(v=vs.100).aspx
  - https://msdn.microsoft.com/library/ms978516.aspx
  - https://msdn.microsoft.com/library/ms954176.aspx
  - https://www.owasp.org/index.php/Application_Threat_Modeling
  - https://www.owasp.org/index.php/Threat_Risk_Modeling

Complément de méthode : Evil User Stories

- Pour s'adapter aux backlog des méthodes agiles
  - Réduire le temps de développement sans nuire à la sécurité
- Sur chaque sprint définir et appliquer des histoires d'usages malicieux du code :
  - Spécifiques aux fonctions implémentées
  - Communs au projet, comme :
    - Authentification
    - Gestion des sessions
    - Contrôle d'accès
    - Validation d'entrée
    - Codage / échappement de sortie
    - Cryptographie
    - Gestion des erreurs et journalisation
    - Protection des données
    - Sécurité de la communication
    - Fonctionnalités de sécurité HTTP

Complément de méthode : Evil User Stories

- Exemple :
  - En tant que méchant, je peut écouter un canal insuffisamment chiffré pour accéder aux login et mot de passe des utilisateurs et les utiliser illégalement
  - En tant que méchant, je peut utiliser un injection SQL pour modifier les identifiants des utilisateurs dans la base de données
  - En tant que méchant, je peux saturer le formulaire d'authentification et empêcher l'accès au service par les utilisateurs légitimes
  - En tant que méchant, je peux lire et même modifier toutes les données qui sont entrées et sorties par votre application