Sécurité & Modélisation des menaces

Guillaume Bienkowski — Braincube

Plan

- Introduction
- Présentation de la sécurité
- Gestion des risques de sécurité
- TD

Introduction

Une ou deux petites histoires...

La largeur du domaine de la sécurité

Des myriades de sous domaines:

- sécurité des personnes (physique et mentale)
- sécurité des biens (DAB, stocks, etc.)
- sécurité économique
- sécurité de l'environnement (chimie, nucléaire, etc.)
- sécurité de l'information

Le cas de l'industrie

En industrie plus qu'ailleurs encore, la sécurité importe:

- vies humaines en jeu
- impératifs de production ($$)
- importance du savoir faire et des procédures

La sécurité de l'information

Des normes:

- ISO/IEC 27001-27014 et plus
- IEC 62443, équivalent industriel de la 27001

Des lois:

- RGPD -- vous la connaissez tous
- Loi informatique et libertés

La sécurité de l'information

Des organismes officiels:

- ANSSI (Agence Nationale pour la sécurité des systèmes d'information)
- CNIL
- AESRI (Agence Européenne chargée de la sécurité des réseaux et de l'information)

Des acronymes:

- SCADA Supervisory Control and Data Acquisition
- ICS Industrial Control System
- CIA (CID en Français)

L'objectif de ce cours/TD: la sécurité de l'information

La sécurité est un vaste sujet, nous nous concentrerons sur la sécurité de l'information.

Ce cours présente les méthodologies et un exemple concret de sécurisation d'un ensemble de logiciels de traitement de l'information.

CIA / CID

Modèle qui sous-tend la grande majorité des méthodes de sécurisation. Ce sont les 3 choses considérées comme nécessaires à la sécurité de l'information.

- **Confidentialité**
  La donnée doit être accessible uniquement aux destinataires légitimes.
- **Intégrité**
  La donnée ne doit pouvoir être créée, modifiée ou supprimée seulement par les utilisateurs légitimes
- **Disponibilité** (Availability)
  La donnée doit être consultable à tout moment par les utilisateurs.

La sécurité parfaite n'existe pas

- facteur humain
- course aux armes -- intérêt financier, hackers motivés VS équipe de sécurité
- asymétrie du problème: 1 seule vulnérabilité compromet l'entièreté du système
- évolutions techniques / vétusté
- éléments naturels (*Disponibilité*)

→ insoluble, mais on peut réduire les *risques*

La sécurité (informatique) comme une gestion du risque

Glossaire:

Vulnérabilité: une faiblesse du système étudié. Faiblesse matérielle, logicielle ou de procédure ("*personne ne m'a dit de fermer le coffre fort en partant le soir*").

Menace: L'exploitation d'une *faiblesse* par un agent extérieur pour exfiltrer, altérer ou détruire un *bien* (le bien étant dans notre cas une donnée informatique)

Risque: le potentiel d'une *menace* sur les *biens* de l'entreprise.

La sécurité comme une gestion du risque

De chaque menace découle un risque:

Vulnérabilité: le béton de l'enceinte de confinement de ma centrale résiste à 40 tonnes de pression extérieure

Menace: Un avion de **100T** s'écrase délibérément sur mon enceinte de confinement

Risque: Il est possible que mon confinement soit inadapté à un avion de ligne qui s'écraserait sur mon bâtiment.Le coeur de ma centrale pourrait entrer en fusion.

La sécurité comme une gestion du risque

Exemple plus orienté informatique:

Vulnérabilité: un logiciel exposé sur internet par mon entreprise de production de chocolat souffre d'une vulnérabilité qui permet l'exécution à distance de commandes.

Menace:

Risque:

La sécurité comme une gestion du risque

Exemple plus orienté informatique:

Vulnérabilité: un logiciel exposé sur internet par mon entreprise de production de chocolat souffre d'une vulnérabilité qui permet l'exécution à distance de commandes.

Menace: Une entité intéressé par mes données est capable d'utiliser cette vulnérabilité sans difficulté pour exfiltrer mes recettes à l'extérieur (et les vendre)

Risque:

La sécurité comme une gestion du risque

Exemple plus orienté informatique:

Vulnérabilité: un logiciel exposé sur internet par mon entreprise de production de chocolat souffre d'une vulnérabilité qui permet l'exécution à distance de commandes.

Menace: Un Hacker intéressé par mes données est capable d'utiliser cette vulnérabilité sans difficulté pour exfiltrer mes recettes à l'extérieur (et les vendre)

Risque: Mon entreprise se fait plagier par un concurrent qui exploite mes recettes pour innonder le marché avec un produit similaire au mien. Banqueroute.

Comment addresser ces risques

Il existe une myriade de méthodes: EBIOS, MEHARI, OCTAVE, ...

Toutes se valent.

La plupart utilisent les mêmes prémisses:

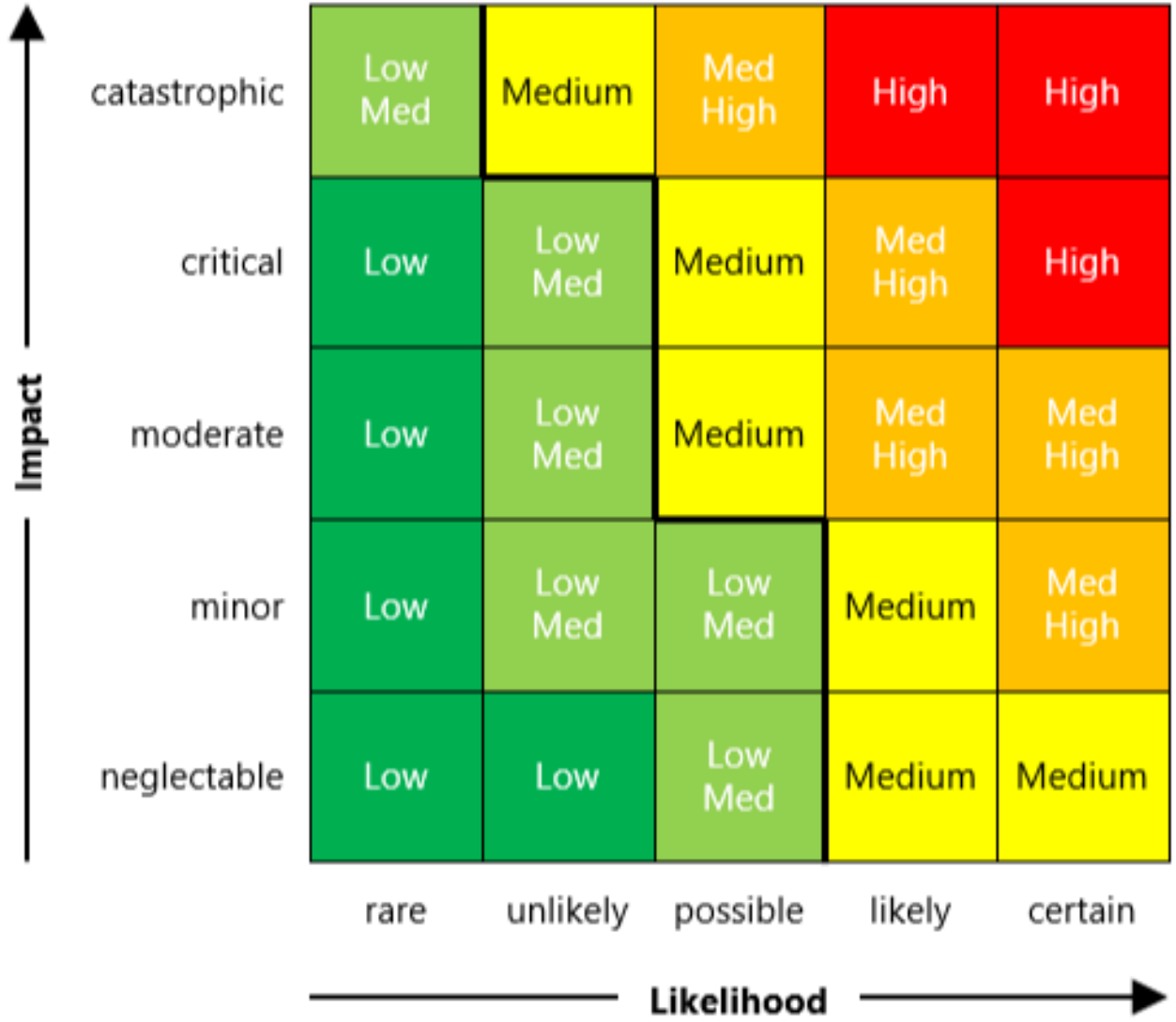
- Assurer le CIA/CID
- Échelonner les réponses en accord avec les risques
- Suivi long terme des actions, et ré-évaluation régulière

Comment addresser ces risques

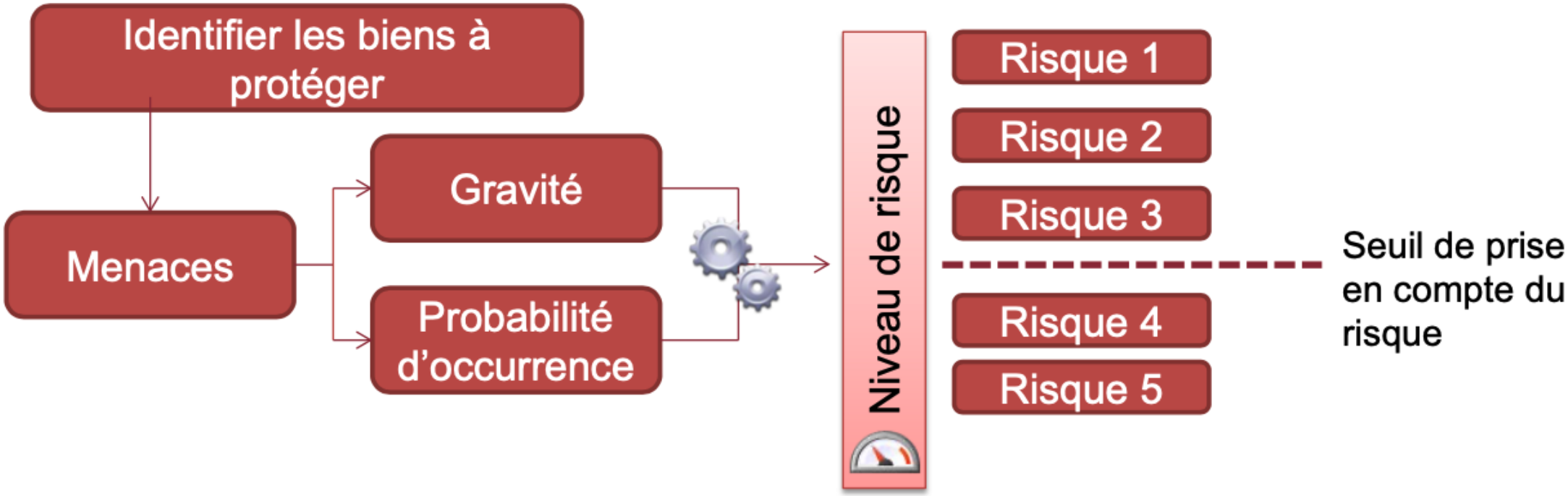
À partir de ce constat, on échelonne les mesures de sécurité selon 2 axes:

- la probabilité de la menace
- les conséquences, l'impact, la gravité de la menace

L'évaluation est subjective: elle va permettre d'ordonner les mesures selon leur impact.



La méthode d'analyse



C'est celle qui est recommandée par l'ANSSI.

Plusieurs types de solutions à une menace de sécurité

- **Techniques**
  La conception du logiciel ou sa mise en oeuvre réduisent voire empêchent carrément le souci de sécurité. Poka Yoke.
  Exemples:
  - logiciel qui tourne avec un utilisateur dédié sur la machine, et non pas en *root*.
  - Authentification déléguée OpenID ou SAML: plus besoin de stocker de mot de passe.
  - Publication d'une nouvelle version impossible si des vulnérabilités sont détectées via scanning automatique

Plusieurs types de solutions à une menace de sécurité

- **Organisationnelles**
  La structure de l'entreprise et du travail rend insignifiante ou inopérable la vulnérabilité
  Exemples:
    - Accès aux salles des machines via badge, autorisé seulement aux admin systèmes
    - Impossible de faire entrer du code sans relecture
    - Rituels de revue des risques (réunion de sécurité, ...)

La méthode d'analyse

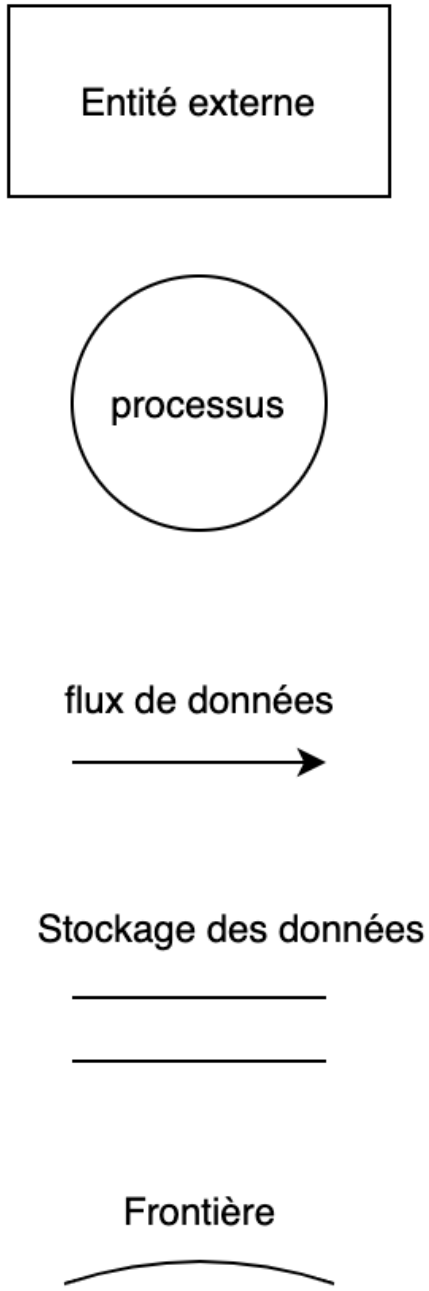
4 étapes:

1. identification des biens à protéger
2. énumération des manières d'enfreindre le *CID* sur ces biens
3. détermination de l'impact et la probabilité d'occurrence, hierarchisation des risques
4. élaboration de contre mesures techniques ou organisationnelle pour réduire ces risques

Identification des biens à protéger

On utilise la méthode du Data Flow Diagram.

Modélisation via un diagramme énumérant tous les flux de données, et les frontières de changement de droits.



Identification des biens à protéger

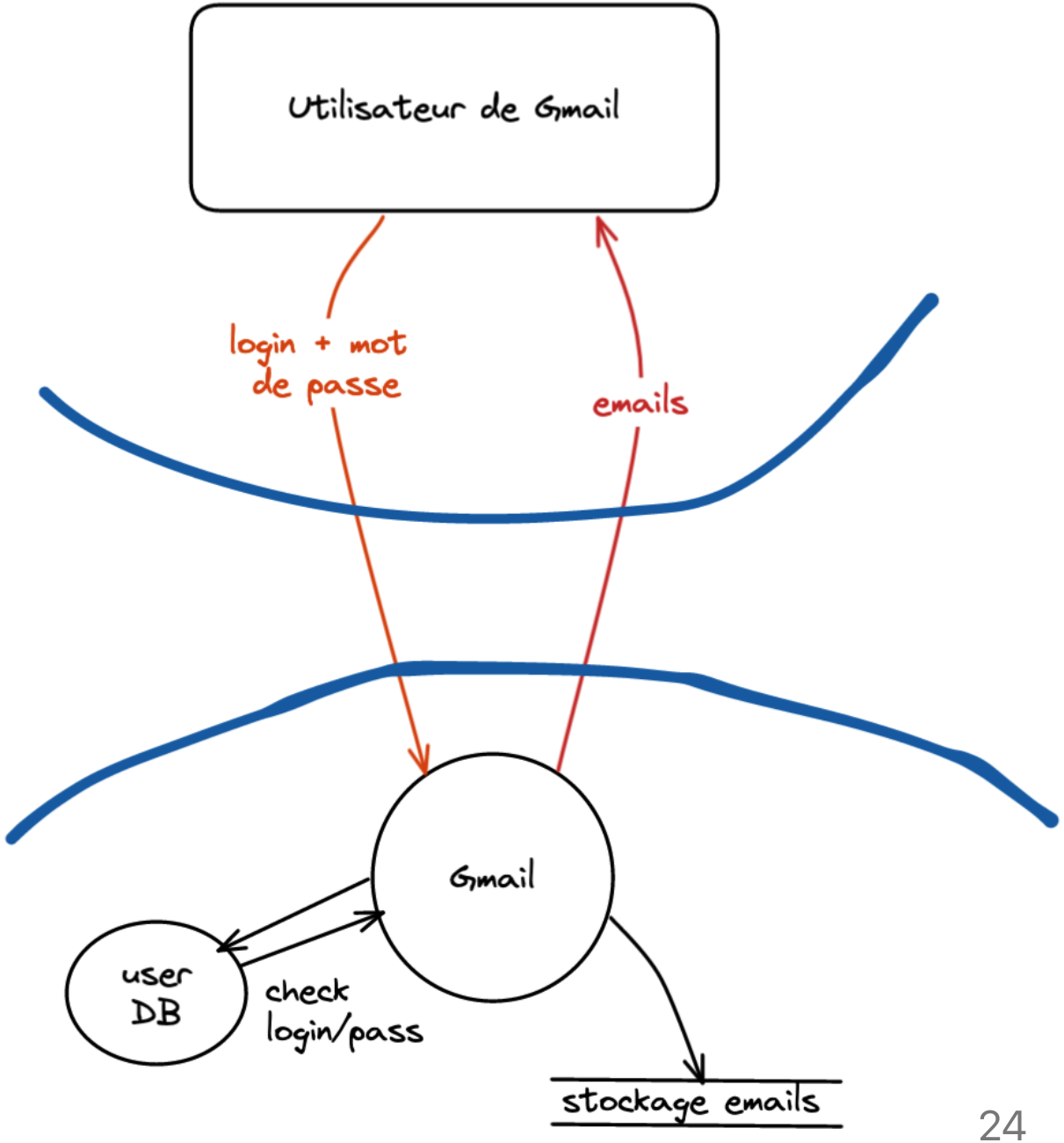
La liste des biens est constituées des choses en lesquelles un attaquant est intéressé.

Dans le diagramme de flow, les flux de données et les endroits de stockages sont généralement les endroits intéressants.

Exemple de Data Flow Diagram

Exemple avec un flow simple d'utilisateur Gmail.

On explore pas ici les utilisateurs admin ou le processus de création d'utilisateur ou de changement de mot de passe.



On démarre le TD

Choisissez un binôme, vous allez travailler à 2 (ou 3 si nombre impair)

Ouvrez le document support et faites-en une copie (ou téléchargez-le sur votre ordinateur)

Le code se trouve ici: https://masterind4.github.io

Le sujet

Nous allons réaliser une étude des menaces sur une entreprise dont vous êtes un des architectes logiciel.

Le composant que nous allons étudier est le système d'ingestion de données d'Assurance Qualité de vos prestataires.

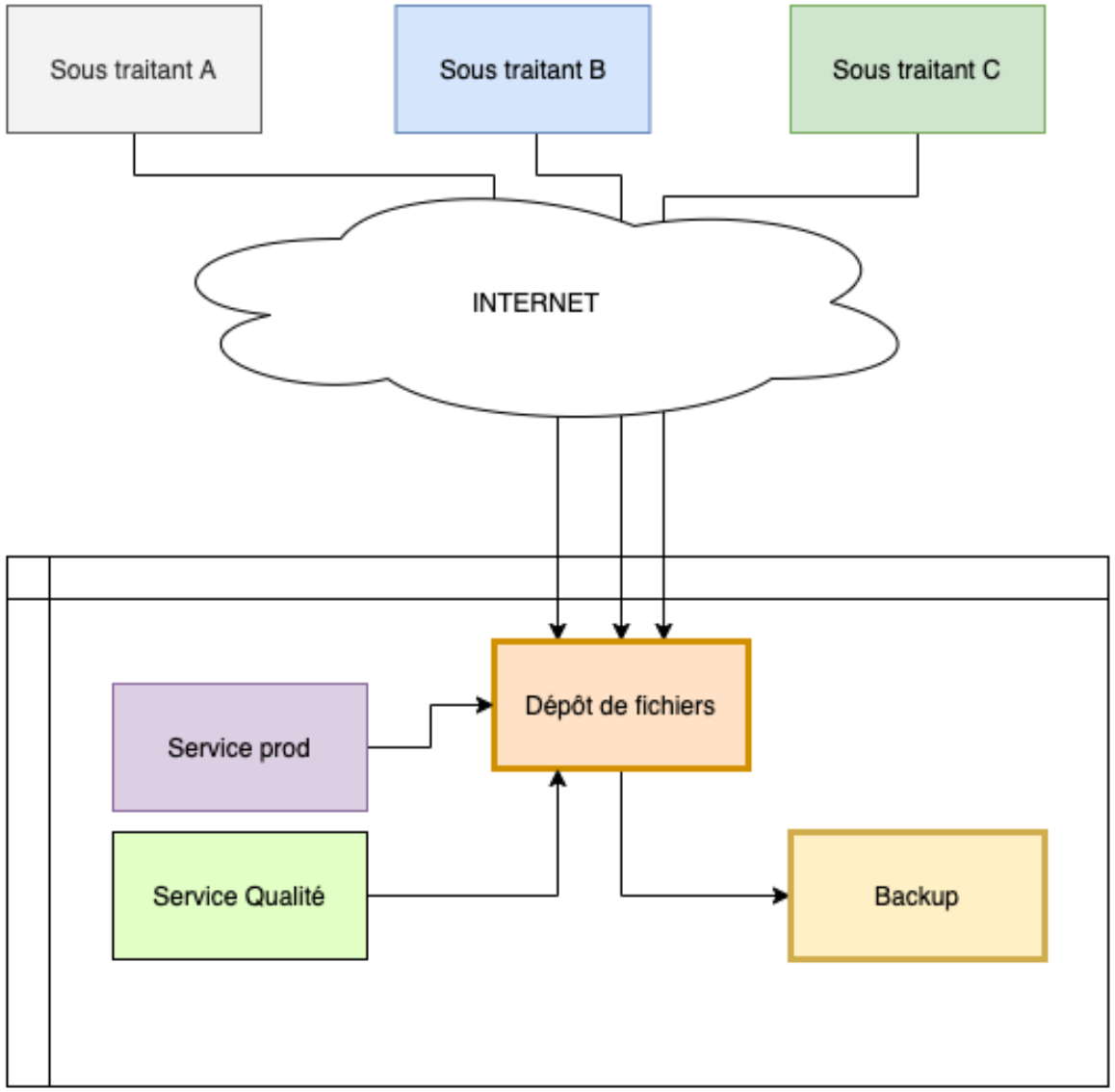
Il faudra utiliser l'analyse de risques que l'on vient de voir en cours, afin d'identifier les vulnérabilités, échelonner les risques associés, proposer des mesures de réduction de ces risques, et implémenter les parties techniques.

Fonctionnement théorique

Votre société fait appel à plusieurs sous traitants qui vous fournissent en pièces diverses pour votre production.
Leur contrat de fourniture stipule qu'ils doivent régulièrement vous fournir des rapports de contrôle qualité, ainsi que des rapports de production via un système d'échange de fichiers, de manière automatisée.

Une fois les fichiers déposés, vos collègues affectés à la production peuvent les consulter. *Ils n'ont pas besoin de les modifier par contre*. Vous avez déjà anticipé des pertes éventuelles de fichiers et avez mis en place une sauvegarde régulière de ces fichiers.

Schéma


Sous traitant A
Sous traitant B
Sous traitant C
INTERNET
Service prod
Service Qualité
Dépôt de fichiers
Backup

Comment démarrer

Clonez le dépôt, et rendez-vous dans le dossier `./tp_securite` dans un terminal.

À cet endroit, lancez la commande `docker-compose up` dans le terminal. Laisser le temps à docker-compose de faire son affaire, et ouvrez un navigateur sur http://localhost:8080

`Ctrl + C` pour arrêter le serveur dans le terminal, et `docker-compose up` pour relancer. `docker-compose down` pour complètement supprimer les logiciels.

Les fichiers manipulés par le site sont disponibles dans le dossier `./tp_securite/run/{stockage,backup}`

Si docker-compose n'est pas installé

Consulter le fichhier `README.md` dans le dossier `tp_securite` pour trouver comment installer l'executable.

Fonctionnement pratique

Les fournisseurs ont un login/mot de passe pour envoyer leurs fichiers sur l'interface web http://localhost:8080

`fournisseur:SomeThinGh4sToGive`

L'admin a un login/mot de passe:

`admin:An0tHerPassW0rd`

Les utilisateurs internes ont un mot de passe dédié:

`userinterne:SomeThinGh4sToGive`

Prise en main du TD

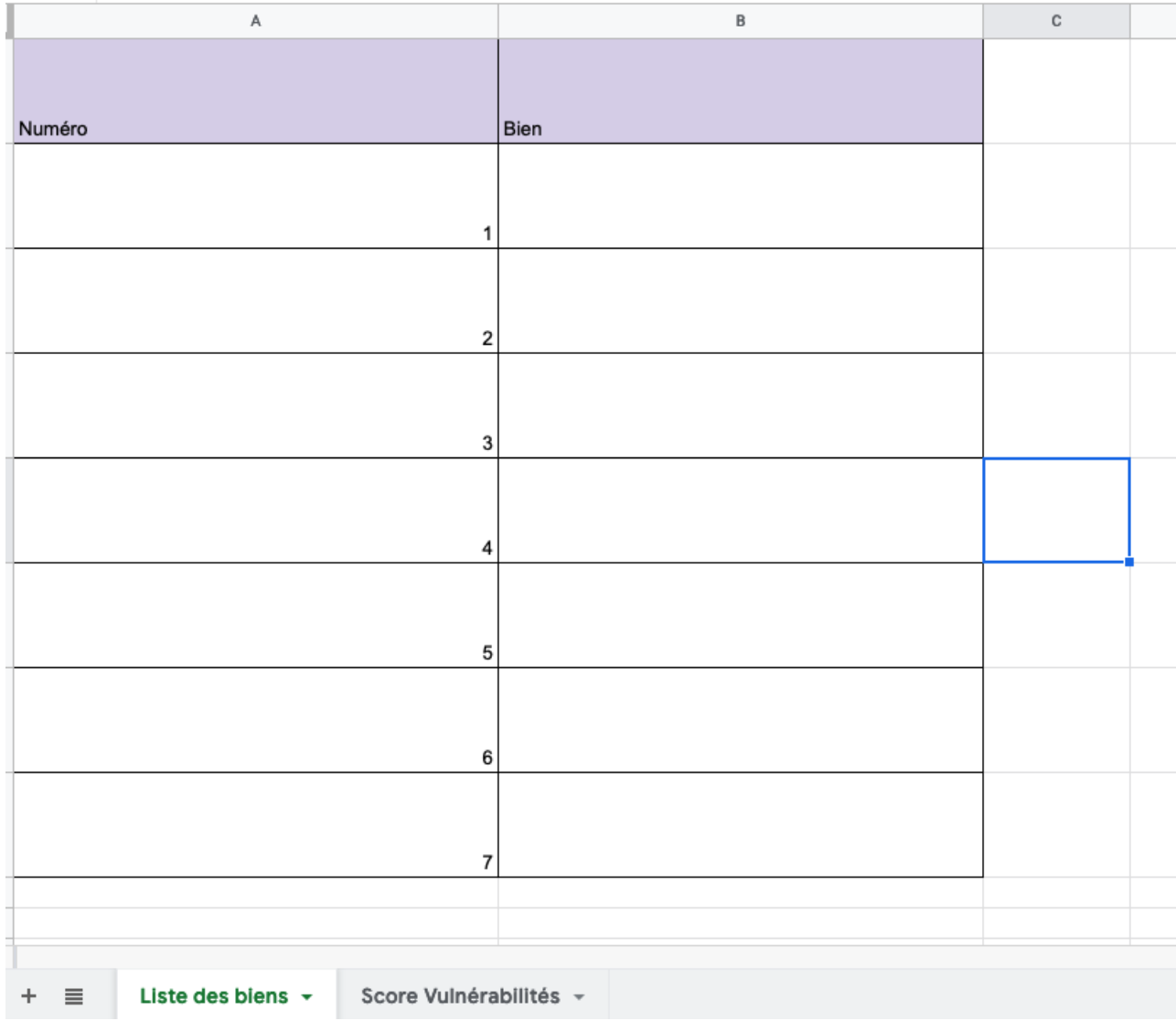
Amusez-vous quelques minutes avec le portail. Constatez que les fonctionnalités attendues sont présentes:

- les fournisseurs peuvent envoyer des fichiers
- les fichiers sont stockés à la fois dans le dossier `stockage` ET le dossier `backup`
- Les utilisateurs standards peuvent consulter ces fichiers

Nous allons procéder avec les 4 étapes de l'analyse de risques.

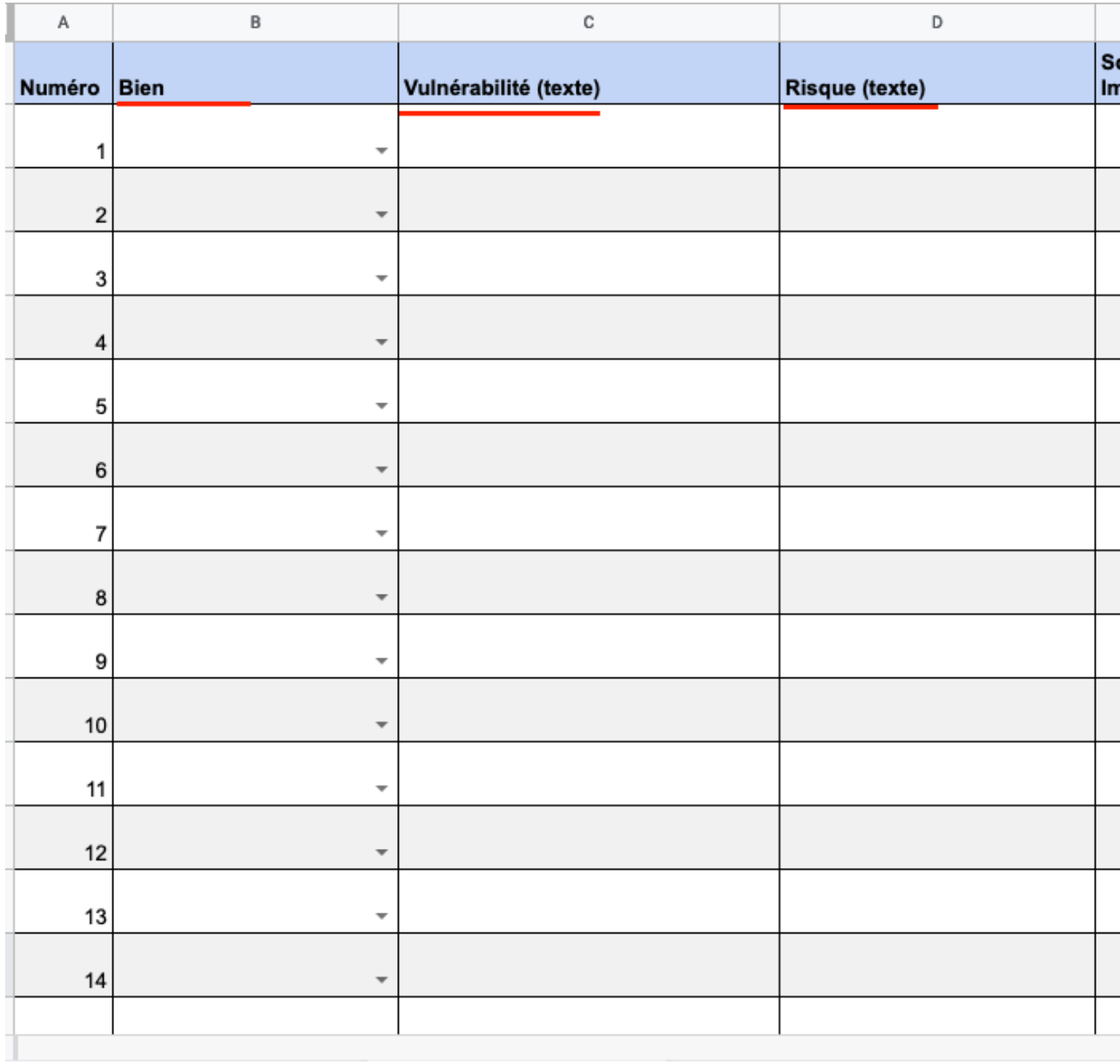
Étape 1: Détermination des biens

Lister les données manipulées par l'ensemble du système. Pour cela, on crée ensemble un schéma de flow de données. Ensuite, utiliser la première feuille du document Drive fourni.



Étape 2: Énumération des manières d'enfreindre le CID sur ces biens

Laissez votre imagination parler. Pour cela utiliser la 2ème feuille du document Drive fourni, en remplissant les colonnes "Vulnérabilité" et "Risque". Sélectionner le bien à gauche dans la liste déroulante.



A	B	C	D
Numéro	Bien	Vulnérabilité (texte)	Risque (texte)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			

Étape 2 bis: On scanne les images

Utiliser l'executable trivy que vous avez dans le dossier `./tp_securite` :

```
# liste les images docker présentes
docker images
# scanne une image et produit un rapport
# exemple: ./trivy i mariadb:10.7
./trivy image <nom image>
```

Évaluation du rapport pour l'image `tp_securite_depot`

Étape 3: Notation des menaces

On retourne tous ensemble pour faire une revue des vulnérabilités trouvées. On applique un score à ces risques et on liste ceux qu'on souhaite corriger.

Étape 4: Mesures correctives

Énumération des mesures correctives, et on passe à l'action.

Mise à jour de l'image docker de base pour le service de fichier

- Utiliser une version plus récente de PHP (voir hub.docker.com, utiliser le semver)
- Utiliser la dernière version de filegator disponible sur internet

Attention: bien reconstruire l'image avant de relancer: `docker-compose build`

Constater que ça fonctionne encore, et que trivy est bien plus heureux.

Utilisation d'un utilisateur dédié pour la base MariaDB

Modifier les variables d'environnement passées au container mariadb pour créer un utilisateur dédié à la base d'authentification

Modifier la configuration du dépôt de fichier pour utiliser cet utilisateur.

Bien supprimer les données dans `./run/db/*` et redémarrer la DB.

Utilisateurs dédiés à chaque prestataire

Utiliser l'UI de Filegator ou alors modifier le script `init.sql` pour créer des utilisateurs dédiés

Autres améliorations possibles

- Implémenter un filtrage IP sur les prestataires
- Passer le frontal en HTTPS (très important, mais hors du scope ici)
- Rendre le frontal hautement disponible en ayant 2 frontaux
- Rendre le stockage hautement disponible via un stockage partagé
- Changer le frontal pour une authentification par certificats ou clés SSH
- Passer le backup à une authentification forte via clé SSH plutôt qu'un login/pass
- Faire tourner trivy régulièrement et remonter une alerte lorsque les images sont vulnérables

Questions?