18/12/2023

# AUDIT DE SECURITE

## Linux

CONFIDENTIEL

Par
NICOLAS WAILLY

# Fiche de suivi du document

## Historique des modifications

| Version | Date | Redacteur | Modicfication |
|---|---|---|---|
| **1.0** | 18/01/2023 | WAILLY Nicolas | Création du document |
| | | | |
| | | | |
| | | | |

## Liste de diffusion

| Société | Service / Personne | Objet de la Diffusion |
|---|---|---|
| | | |
| | | |
| | | |

# SOMMAIRE

# 01 PRESENTATION DE LA DEMARCHE

## 01.1 RAPPEL DU BESOIN

L'objectif de cet audit est d'évaluer les risques d'une machine Linux, par une démarche présentée ci-dessous. Pour chaque risques identifiés des recommandations seront effectuées afin de limiter le défaut et atteindre un niveau de sécurité acceptable.

## 01.2 PRESENTATION DE LA DEMARCHE

La méthodologie de test d'intrusion se découpe en 4 phases :

- La machine Linux 192.168.72.134 à été analysée et placée dans un réseau isolé
- Une reconnaissance du réseau suivi d'une analyse des services disponible à été réalisé
- Des recherches de vulnérabilités son venus compléter l'analyse précédente

## 01.3 OBJECTIFS VISES

La prestation de test d'intrusion a pour objectif de dresser un état des lieux de la sécurité d'un système d'information ou d'une application à un instant donné. L'objectif est de mettre en lumière les failles de sécurité réellement exploitables par un individu malveillant dans un temps volontairement limité.

## 01.4 MODE OPERATOIRE

Les tests on été réalisé sur une machine Debian 12

Afin de réaliser les tests les outils suivants ont été utilisés :

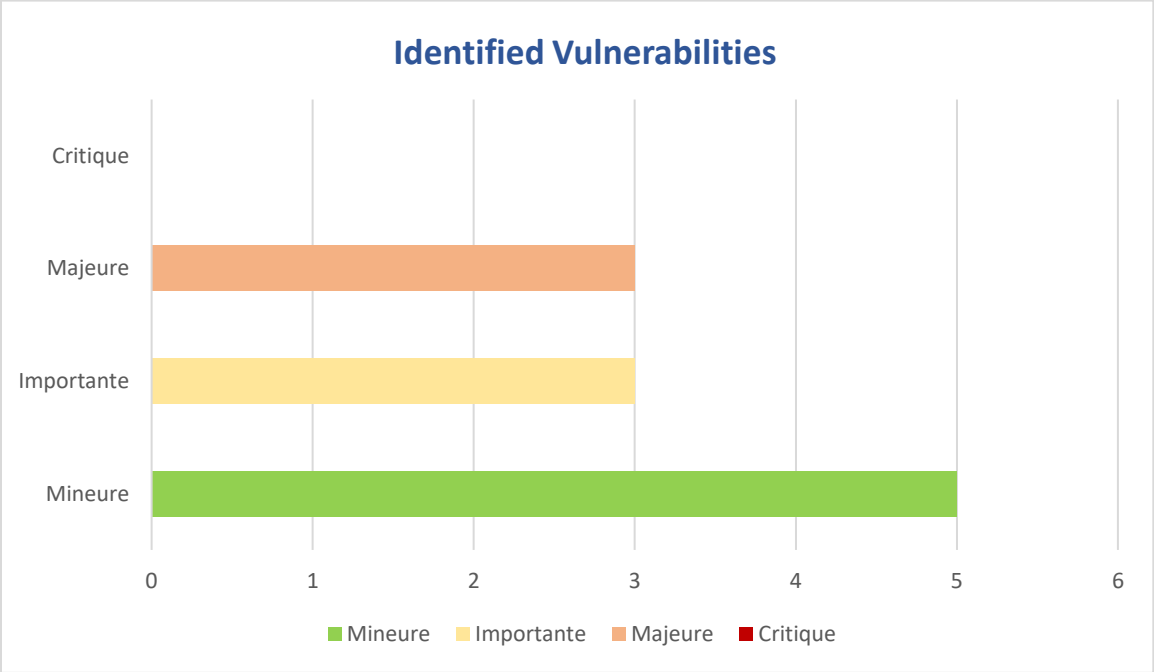
- Lynis

La machine est accessible en dure et ne dispose pas de connexion SSH.

## 01.5 EXHAUSTIVITE DES RESULTATS

Les résultats ont été réalisés sur une durée de test prédéfinie et limitée, cette démarche s'appuie sur une durée de test et n'a pas vocations à être exhaustive. Seuls les fonctionnalités accessibles lors de l'audit ont été analysées.

# 02 SYNTHESE MANAGERIALE




The tests conducted on the Linux machine have highlighted a generally good level of security. However, security precautions are either not implemented or applied.

We have identified the presence of vulnerable packages installed on the machine and a lack of recognition of these vulnerable packages.

Some services are applied with a low level of security. No configuration is enabled for the firewall in iptables, although the service is installed and functional.

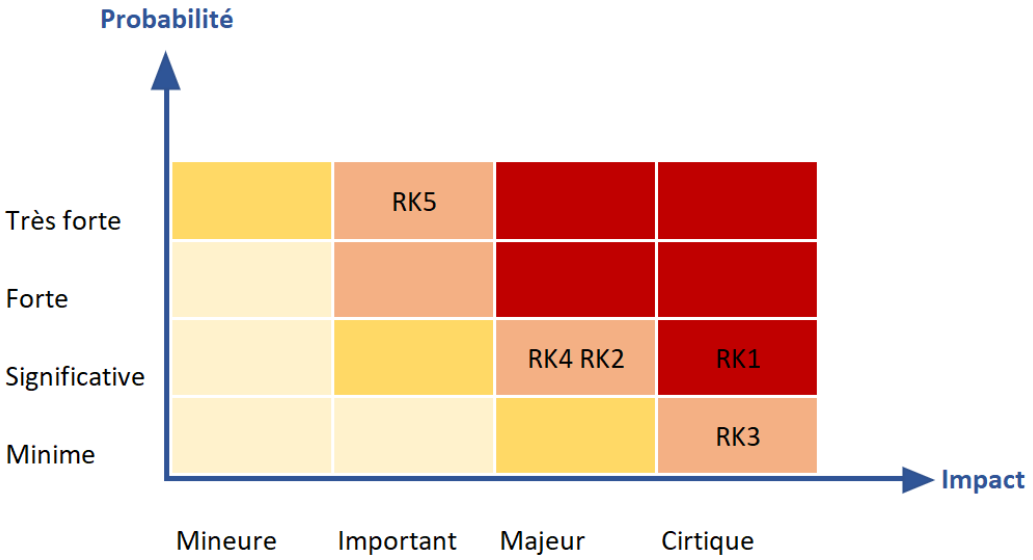
On the other hand, no antivirus has been detected on the machine

# 03 SYNTHESE DES RISQUES

Voici ci-dessous la liste des vulnérabilités identifiées :

### Synthèse des risques

- **RK1 :** Un utilisateur prend le contrôle physique ou à distance de la machine
- **RK2 :** Installation de paquets malveillant
- **RK3 :** Un attaquant accède à des données techniques et exploite des défauts dans les composants logiciels de l'environnement
- **RK4 :** Un utilisateur laisse fuiter des informations critiques
- **RK5 :** l'infrastructure est victime d'une campagne de ransomware où de phishing




Cette matrice des risques pourra être adaptée vis-à-vis de votre éventuel référentiel interne de gestion des risques.

# 04 SYNTHESE DES VULNERABILITES IDENTIFEES

## 04.1 SYNTHESE TECHNIQUE

Les tests réalisé sur a machine Linux, ont permis de mettre en évidence plusieurs problèmes :

- **Au niveau de la sécurisation des sessions :**
  - Aucun mot de passe n'est configuré pour au GRUB.
  - La session utilisateur et la session ROOT ont des mots de passe qui n'expire jamais.

- **Des services de ne sont pas configurés ou sécurisés :**
  - Iptable est installées sans règles ou configuration et ne fonctionne donc pas.
  - De nombreux services sont fonctionnels mais pas sécurisées.
  - Aucune mesure n'est mise en place pour qu'un utilisateur classique de la machine ne puisse pas voir la configuration deamon-Cups pour les imprimantes

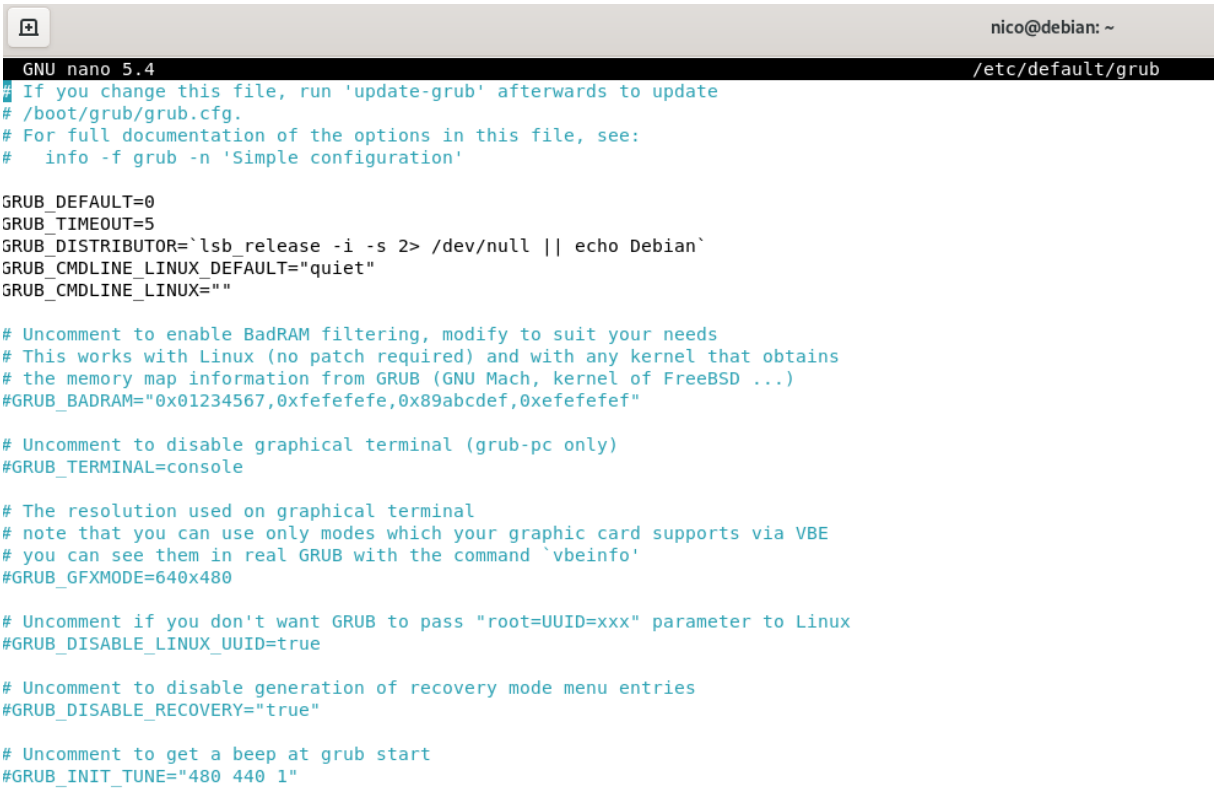
- **Séparation des partitions:**
  - Le partitionnement est établi sur les disques mais n'est pas sécurisé.

## 04.2 LISTES DES VULNERABILITES IDENTIFIEES

| ID | DESCRIPTION | RISQUE AVERE | PERIMETRE | Risque |
|---|---|---|---|---|
| V1 | Pas de mot de passe pour le GRUB | Oui | 192.168.72.134 | important |
| V2 | Aucune configuration parefeu | Oui | 192.168.72.134 | important |
| V3 | Pas d'antivirus configuré | Oui | 192.168.72.134 | majeur |
| V4 | Plusieurs services installés ne sont pas sécurisés | Oui | 192.168.72.134 | majeur |
| V5 | Partitionnement des disques, tout dans une partition | Oui | 192.168.72.134 | Important |
| V6 | Port SSH et Telnet ouvert | Oui | 192.168.72.134 | important |
| V7 | Utilisation de paquet vulnérable | Oui | 192.168.72.134 | critique |

## V1. Pas de mot de passe sur le GRUB

<table>
<tr><td rowspan="4">V1<br><br>Important</td><td colspan="3">Aucun mot de passe n’a été défini pour accéder au GRUB</td></tr>
<tr><td colspan="3"><u>Vulnérabilité :</u><br>L'absence de mot de passe pour GRUB expose le système à des attaques potentielles au niveau du gestionnaire de démarrage.<br><u>Recommandation :</u><br>Configurer un mot de passe pour GRUB pour renforcer la sécurité du démarrage.<br>Mettre en œuvre des restrictions d'accès physique au serveur pour prévenir l'accès non autorisé au gestionnaire de démarrage.</td></tr>
<tr><td colspan="3"><u>Périmètre concernés :</u> 192.168.72.134</td></tr>
<tr><td>Impact</td><td>Difficulté d’exploitation</td><td>Risque avéré</td></tr>
<tr><td>Faible</td><td>Moyenne</td><td>Oui</td></tr>
</table>



## V2. Aucune configuration IPtables

<table>
<tr><td rowspan="4">V2<br><br>Important</td><td colspan="3">Aucune configuration IPtables</td></tr>
<tr><td colspan="3"><u>Vulnérabilité :</u><br>Le pare-feu est activé mais aucune configuration n’est appliquée<br>Un pare-feu non configuré expose le serveur à des attaques réseau non autorisées<br><u>Recommandation :</u><br>Configurer le pare-feu pour filtrer le trafic réseau entrant et sortant.<br>Autoriser uniquement les ports nécessaires pour les services essentiels.<br>Bloquer le trafic non autorisé ou non nécessaire.</td></tr>
<tr><td colspan="3"><u>Périmètre concernés :</u> 192.168.72.134</td></tr>
<tr><td>Impact</td><td>Difficulté d’exploitation</td><td>Risque avéré</td></tr>
<tr><td></td><td>Important</td><td>Elevée</td><td>Oui</td></tr>
</table>

```
root@debian:~/lynis# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

## V3.Pas d’antivirus configuré

<table>
<tr><td rowspan="4">V3<br><br>majeur</td><td colspan="3">Pas d’antivirus configuré</td></tr>
<tr><td colspan="3"><u>Vulnérabilité :</u><br>L'absence d'un antivirus expose le serveur à des risques liés aux malwares et aux attaques par logiciels malveillants.<br><u>Recommandation :</u><br>Installer et configurer un logiciel antivirus adapté au système d'exploitation Debian 12.<br>Effectuer des analyses régulières pour détecter et éliminer les menaces potentielles.</td></tr>
<tr><td colspan="3"><u>Périmètre concernés :</u> 192.168.72.134</td></tr>
<tr><td>Impact</td><td>Difficulté d’exploitation</td><td>Risque avéré</td></tr>
<tr><td>Majeur</td><td>Important</td><td>Oui</td></tr>
</table>

## V4.Plusieurs services installés ne sont pas sécurisés

| | | | |
|---|---|---|---|
| **V4**<br><br>**Majeure** | Plusieurs services installés ne sont pas sécurisés | | |
| | **Vulnérabilité :**<br>Plusieurs services sont configurés sans mesure préalable de sécurité ou une sécurité faible<br><br>**Recommandation :**<br>Vérifier la configuration de ses services et adaptés pour chacun les bonnes pratiques | | |
| | **Périmètre concernés :** 192.168.72.134 | | |
| | Impact | Difficulté d'exploitation | Risque avéré |
| | FORT | Faible | Oui |

```
ModemManager.service                       5.9 MEDIUM    😐
NetworkManager.service                     7.8 EXPOSED   😕
accounts-daemon.service                    9.6 UNSAFE    😨
alsa-state.service                         9.6 UNSAFE    😨
anacron.service                            9.6 UNSAFE    😨
avahi-daemon.service                       9.6 UNSAFE    😨
bluetooth.service                          6.9 MEDIUM    😐
colord.service                             8.8 EXPOSED   😕
cron.service                               9.6 UNSAFE    😨
cups-browsed.service                       9.6 UNSAFE    😨
cups.service                               9.6 UNSAFE    😨
dbus.service                               9.6 UNSAFE    😨
emergency.service                          9.5 UNSAFE    😨
fwupd.service                              7.4 MEDIUM    😐
gdm.service                                9.8 UNSAFE    😨
getty@tty1.service                         9.6 UNSAFE    😨
open-vm-tools.service                      9.5 UNSAFE    😨
packagekit.service                         9.6 UNSAFE    😨
plymouth-start.service                     9.5 UNSAFE    😨
polkit.service                             9.6 UNSAFE    😨
rc-local.service                           9.6 UNSAFE    😨
rescue.service                             9.5 UNSAFE    😨
rsyslog.service                            9.6 UNSAFE    😨
rtkit-daemon.service                       7.2 MEDIUM    😐
switcheroo-control.service                 7.6 EXPOSED   😕
systemd-ask-password-console.service       9.4 UNSAFE    😨
systemd-ask-password-plymouth.service      9.5 UNSAFE    😨
systemd-ask-password-wall.service          9.4 UNSAFE    😨
systemd-fsckd.service                      9.5 UNSAFE    😨
systemd-initctl.service                    9.4 UNSAFE    😨
systemd-journald.service                   4.3 OK        🙂
systemd-logind.service                     2.6 OK        🙂
systemd-networkd.service                   2.9 OK        🙂
systemd-rfkill.service                     9.4 UNSAFE    😨
systemd-timesyncd.service                  2.1 OK        🙂
systemd-udevd.service                      8.0 EXPOSED   😕
udisks2.service                            9.6 UNSAFE    😨
unattended-upgrades.service                9.6 UNSAFE    😨
upower.service                             2.4 OK        🙂
user@1000.service                          9.4 UNSAFE    😨
vgauth.service                             9.5 UNSAFE    😨
wpa_supplicant.service                     9.6 UNSAFE    😨
```

## V5. Partitionnement des disques, tout dans une partition

```
root@debian:~/lynis# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@debian:~/lynis# df -H
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
udev                990M       0  990M   0% /dev
tmpfs               203M    1,5M  202M   1% /run
/dev/sda1            31G    5,4G   24G  19% /
tmpfs               1,1G       0  1,1G   0% /dev/shm
tmpfs               5,3M    4,1k  5,3M   1% /run/lock
tmpfs               203M    934k  202M   1% /run/user/1000
```

| | | | |
|---|---|---|---|
| V5<br><br>Important | Partitionnement des disques, tout dans une partition | | |
| | **Vulnérabilité :**<br>L'isolement insuffisant des partitions, en particulier pour /home, /tmp et /var, peut entraîner une propagation de l'infection en cas de compromission.<br>**Recommandation :**<br>Partition /home :<br><br>Isoler /home /tmp et /var sur des partitions distinctes.<br>Appliquer des restrictions d'accès strictes, limitant l'accès aux utilisateurs autorisés.<br>Utiliser l'option noexec pour empêcher l'exécution de fichiers binaires dans /tmp. | | |
| | **Périmètre concernés :** 192.168.72.134 | | |
| | Impact | Difficulté d'exploitation | Risque avéré |
| | FORT | Moyenne | Oui |

## V6. Port SSH et Telnet ouvert

<table>
<tr><td rowspan="4">V6<br><br>Important</td><td colspan="3">Partitionnement des disques, tout dans une partition</td></tr>
<tr><td colspan="3"><u>Vulnérabilité :</u><br>La configuration actuelle de SSH comporte des éléments suggérant des améliorations pour renforcer la sécurité du service.<br>Telnet transmet les informations, y compris les mots de passe, de manière non cryptée, présentant des risques de sécurité importants.<br><br><u>Recommandation :</u><br>Désactiver Telnet</td></tr>
<tr><td colspan="3"><u>Périmètre concernés :</u> 192.168.72.134</td></tr>
<tr><td>Impact</td><td>Difficulté d’exploitation</td><td>Risque avéré</td></tr>
<tr><td>FORT</td><td>Faible</td><td>Oui</td></tr>
</table>

## V7. Utilisation de paquet vulnérable

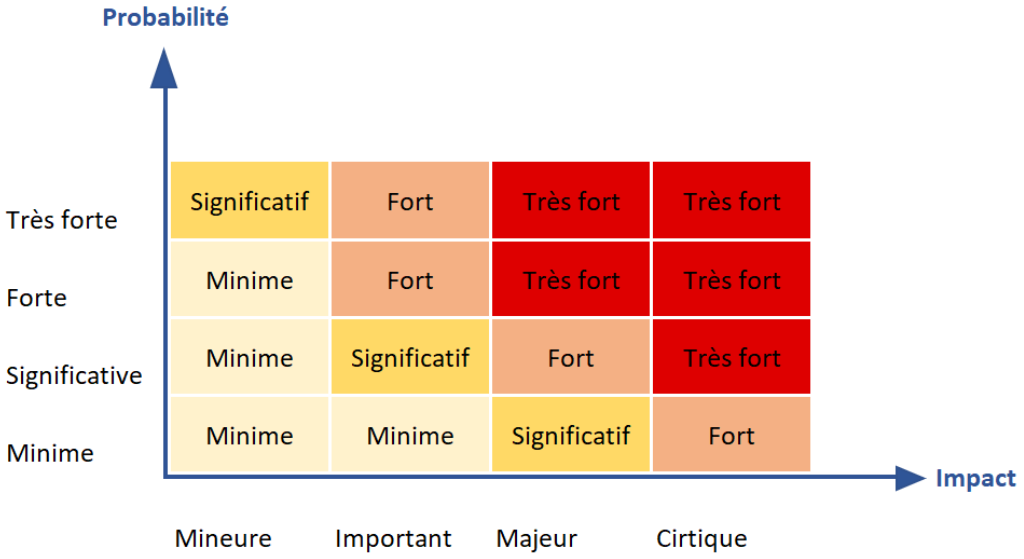
<table>
<tr><td rowspan="4">V7<br><br>Important</td><td colspan="3">Utilisation de paquet vulnérable</td></tr>
<tr><td colspan="3"><u>Vulnérabilité :</u><br>Des paquets installée sur la machine sont des paquets vulnérable est non pas été supprimé ou modifié<br><br><u>Recommandation :</u><br>Appliquer les recommandation pour ces paquets. Supprimer les paquets si nécessaire.</td></tr>
<tr><td colspan="3"><u>Périmètre concernés :</u> 192.168.72.134</td></tr>
<tr><td>Impact</td><td>Difficulté d’exploitation</td><td>Risque avéré</td></tr>
<tr><td>FORT</td><td>FORT</td><td>Oui</td></tr>
</table>

# 05 ANNEXES

## 05.1 ECHELLE DES RISQUES

Les scénarios de risques sont évalués selon les échelles suivantes :

- Les impacts (sur une échelle de 1 à 4)
- Les probabilités d'occurrence du risque associé.




Pour une approche risques, la dimension probabilité est appréciée selon l'échelle suivante

- **Minime :** Le risque résulte d'une attaque complexe, difficile à réaliser ou ne permettant pas d'obtenir d'informations sensibles. Les conditions préalables à la réalisation de ce mode opératoire sont très difficilement réunies par la source de la menace. La motivation de la source pour mener l'attaque reste faible.
- **Significatif :** Le risque résulte d'une vulnérabilité exploitable mais complexe. Elle est exploitée par une source motivée disposant d'informations confidentielles ou profitant de complicité interne. La probabilité de survenance est significative.
- **Forte :** La risque résulte de l'exploitation d'une vulnérabilité connue qui peut être complexe. Un minimum de connaissances de l'application est requis pour conduire l'attaque mais l'attractivité du gain est forte. Elle a une forte probabilité de se produire.
- **Très forte :** Le risque surviendra si aucune mesure de sécurité n'est prise. Les vulnérabilités associées sont triviales et ne nécessitent pas forcement d'authentification préalable.

## 05.2 ECHELLE DE CLASSIFICATION DES MESURES CORRECTIVES

Pour chaque mesure, les critères suivants sont évalués :

• Indication de complexité :

- Action de complexité élevée nécessitant de nombreuses interactions entre les équipes et une prise de décision de la part du management.
- Action de complexité moyenne nécessitant des interactions entre les équipes.
- Action de complexité faible pouvant être menée de manière autonome par l'équipe en charge.

• Indication de coûts et de charge, à définir en fonction du contexte client :

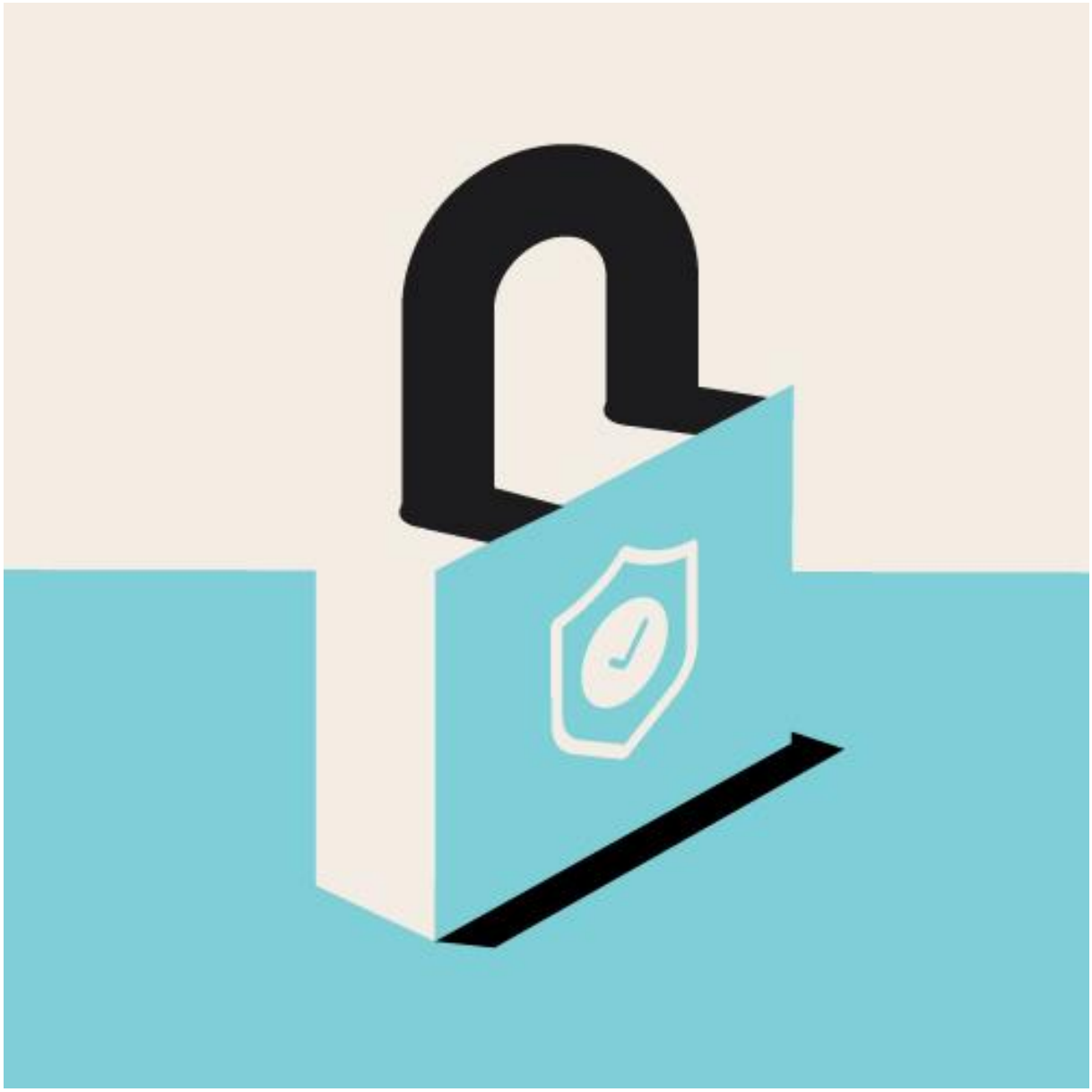
- Coût important.
- Coût modéré
- Coût faible.

• Indication de gain en sécurité par rapport à l'état des lieux, une fois l'action complètement terminée :

- Gain important (contribue de manière importante à la réduction des risques).
- Gain modéré (contribue correctement à la réduction des risques).
- Gain faible (contribue peu à la réduction des risques).

• Les mesures sont classées par priorité :

- Priorité 1 : action court terme, à mettre en place rapidement.
- Priorité 2 : action à mettre en œuvre à moyen terme, corrigeant des faiblesses non négligeables.
- Priorité 3 : action pouvant être mise en œuvre à plus long terme pour accroître le niveau de sécurité.



Par WAILLY Nicolas

@ : nicolaswailly7@gmail.com

Tel : 00 00 00 00 00