Quelques moyens de sécurité mis en place

- Ne pas utiliser n'importe quelle image du docker hub
    - prendre des images vérifiées et certifiées par docker
    - créer une base de données d'images sécurisées en remodelant des images vérifiées ou entièrement crées par nous-même.

- Utilisation de docker secret pour la sécurisation de data et de mots de passe/clés à transmettre
  echo "ceci est un secret" | docker secret create my_secret_data

- Ne mapper que les ports utiles grâce à l'argument -p
  docker run -p 80:80 pour traefik
  docker run -p 6379:6379 pour redis
  docker run -p 9000:9000 pour portainer

- Utilisation d'un reverse proxy avec traefik.

- Utilisation de clés privées pour accéder aux serveurs et mots de passes complexes min/maj/chiffres/caractères spéciaux.

- Utilisation de SE-linux, nous nous y sommes adaptés.

- Aucun fichier importé sur les serveurs, nous les avons créés directement.

- Avoir des snapshots de secours.

- Éviter de lancer les containers et les process en tant que root mais utiliser un user dédié.