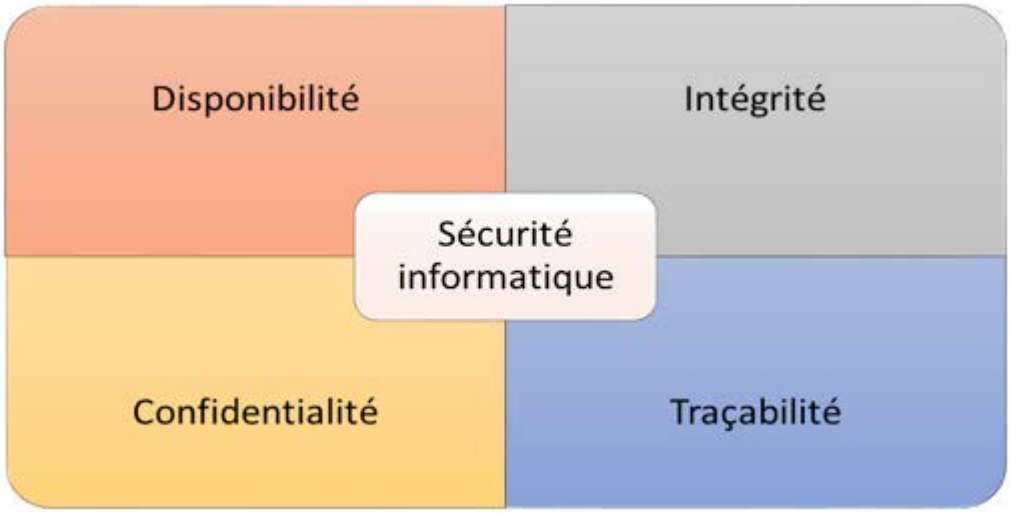
Cyber-sécurité

pierre-yves.tanniou@cerema.fr

Sommaire

- Les composantes de la sécurité
- Références ANSSI
- Illustrations sur quelques thèmes
  - Accès physiques
  - Vidéo-protection
  - Mises à jour
  - Obscurité
- Evaluation de la sécurité

Composantes de la sécurité : DICT

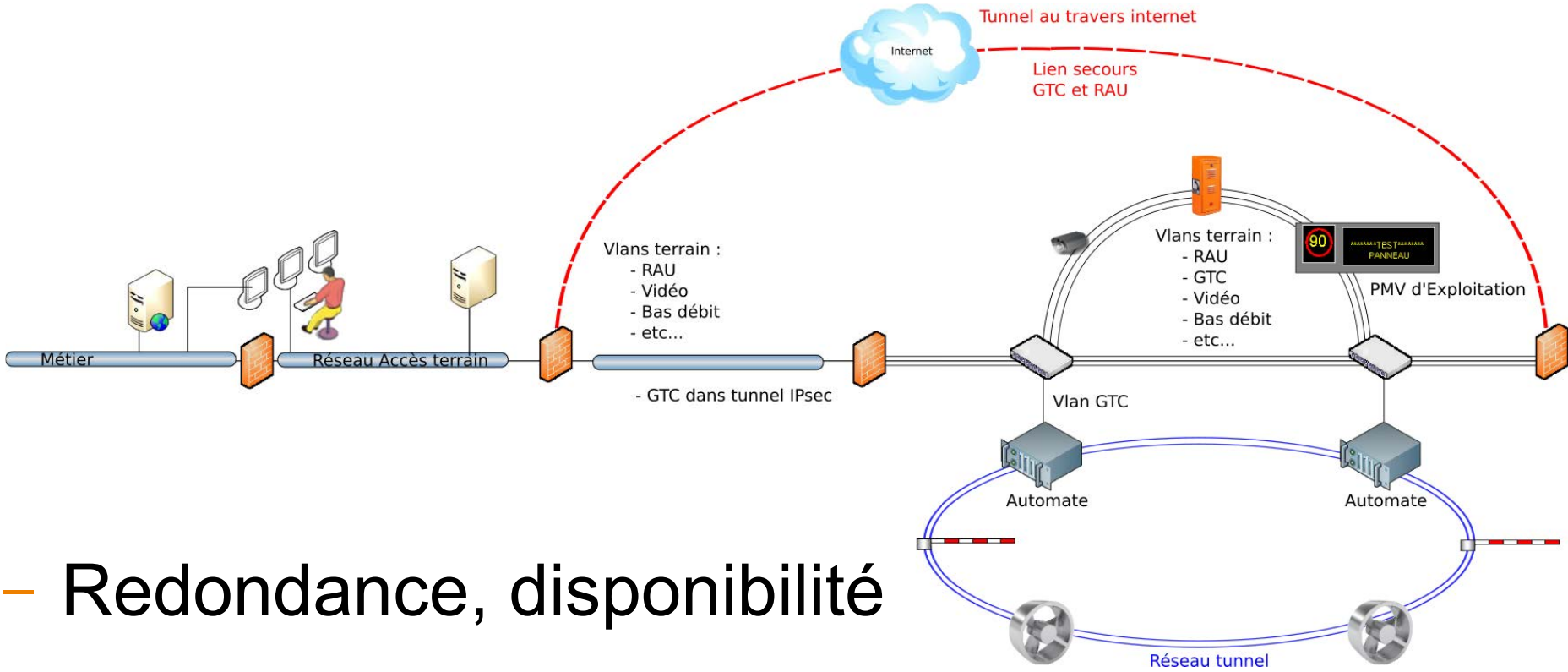


- **Disponibilité** : garantir l'accès aux ressources, au moment voulu
- **Intégrité** : garantir que les données échangées sont exactes et complète
- **Confidentialité** : garantir que seules les personnes autorisées peuvent avoir accès aux données et aux ressources
- **Traçabilité**, authentification, non-répudiation : garantir la traçabilité des accès et des tentatives d'accès ; tracer le fonctionnement ; conservation de ces traces comme preuves exploitables.

Guides ANSSI

- Maîtriser la SSI pour les systèmes industriels
- La cybersécurité des systèmes industriels – Méthode de classification et mesures principales.
- La cybersécurité des systèmes industriels – Mesures détaillées
- Cas pratique
- Cas pratique d'un tunnel routier – Partie 1 : classification
- Cas pratique d'un tunnel routier – partie 2 : mesures

Architecture



- Redondance, disponibilité
- Et les autres composantes de la sécurité ? Maîtrise ?

Accès physique

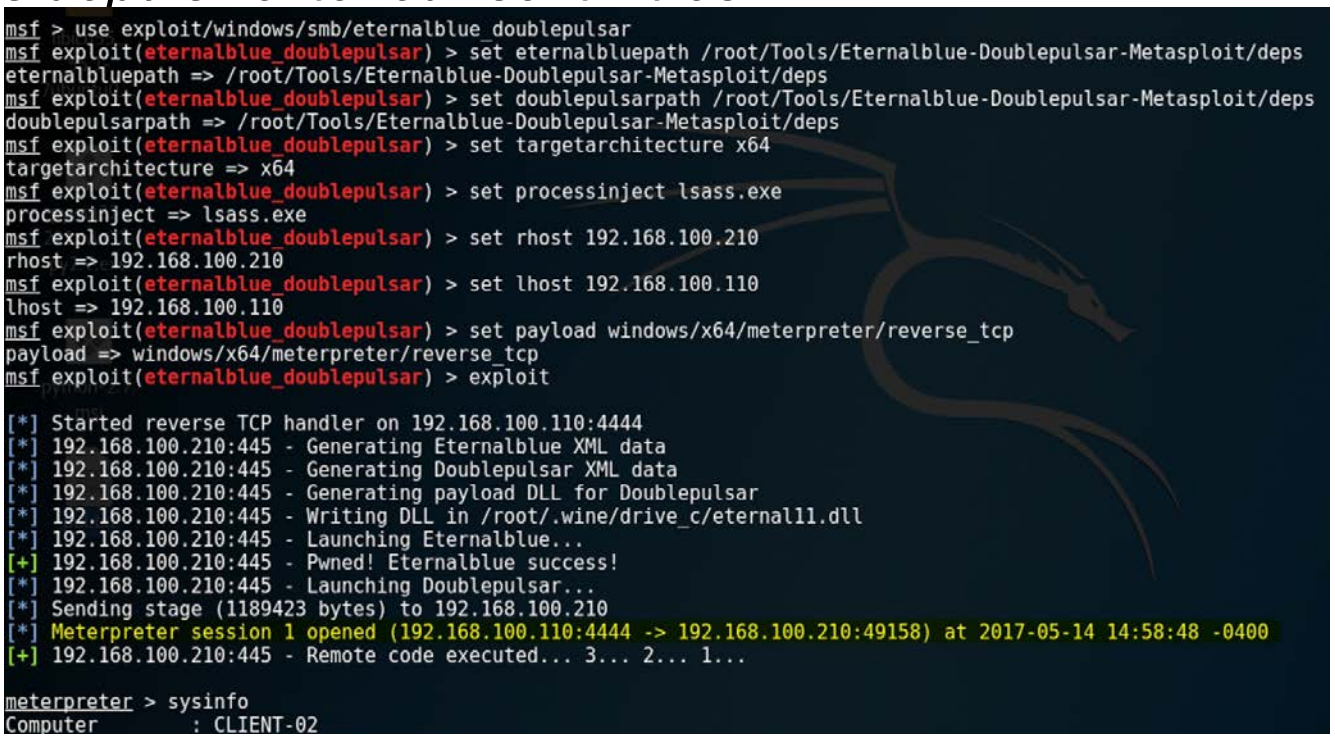
- Eviter qu'un attaquant externe puis être interne
- Pas de protection infaillible
- Le système peut alerter l'exploitant mais seul l'exploitant peut réagir.

Vidéo protection

- Analogique :
  - évite de créer des accès IP vers le reste du système
  - néanmoins piratable
  - Devient coûteux
- Numérique
  - éventuellement protégée

Maintien à jour de la sécurité

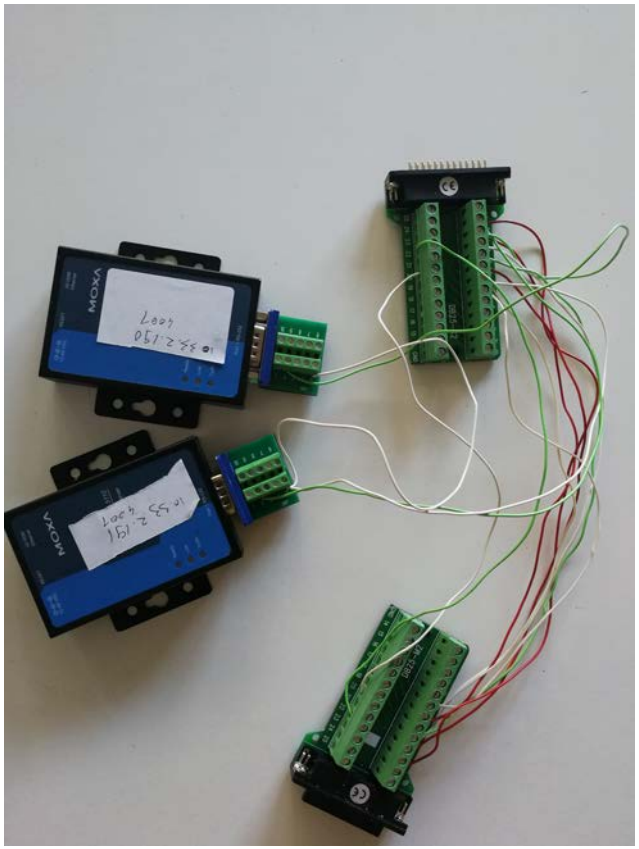
- Je n'en ai pas besoin «*Mon système est stable et figé* » ou « *les accès depuis l'extérieur sont filtrés* »



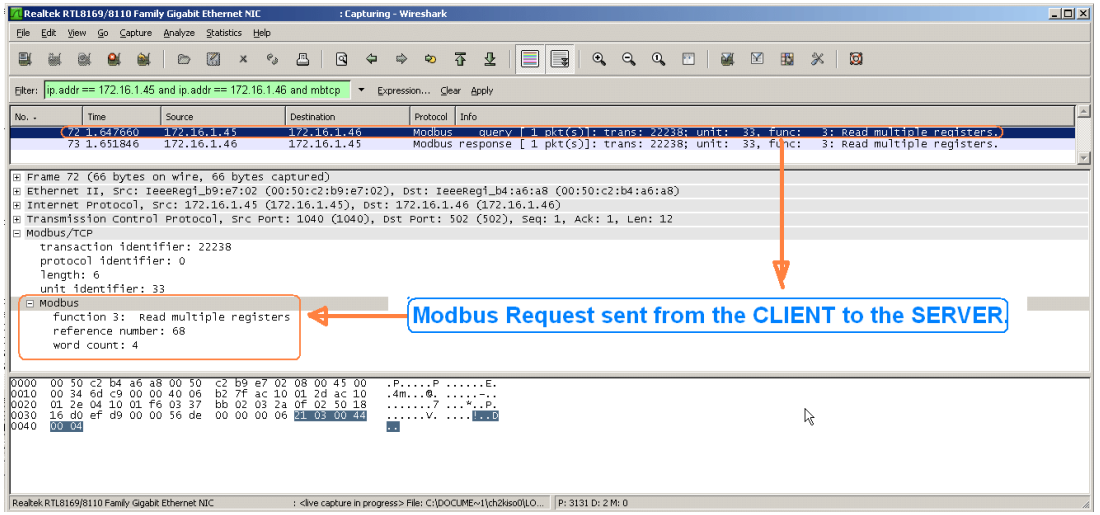
- Un malveillant peut exploiter des vulnérabilités depuis l'intérieur et éventuellement créer un accès vers l'extérieur
- Restent les 0-days

Sécurité par l'obscurité ?

- Mon système n'est pas IP

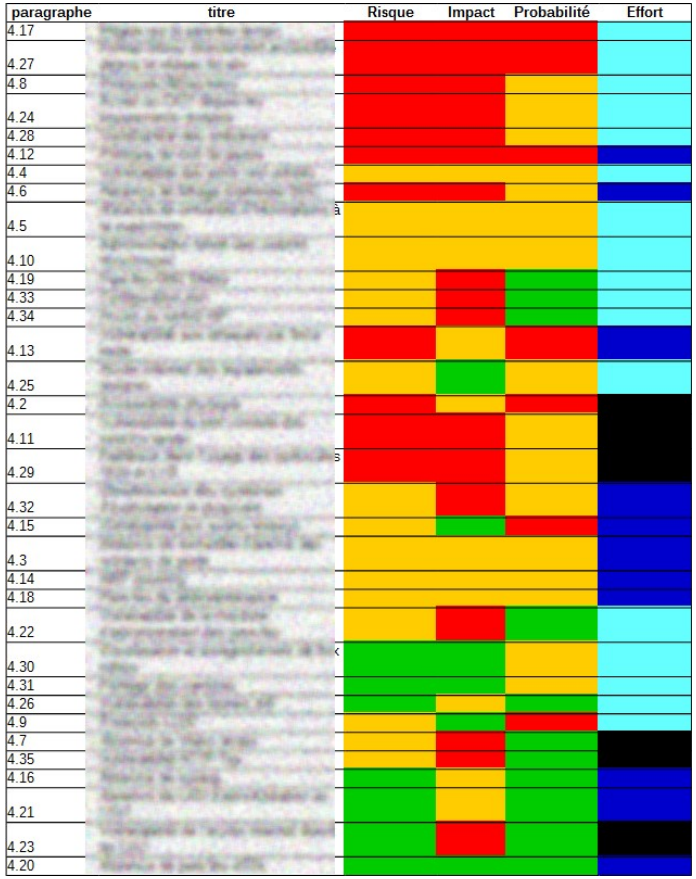


- Mon système utilise un protocole spécifique



Evaluations et tests de sécurité

- Audit de sécurité
  - démarche commune entre l'expert et l'exploitant
  - envisager les vulnérabilité sur différents composants
- Attaque red team
  - l'équipe rouge cherche une vulnérabilité exploitable
  - tester les procédures
  - Impact psychologique : facilite l'adhésion



Merci de votre attention