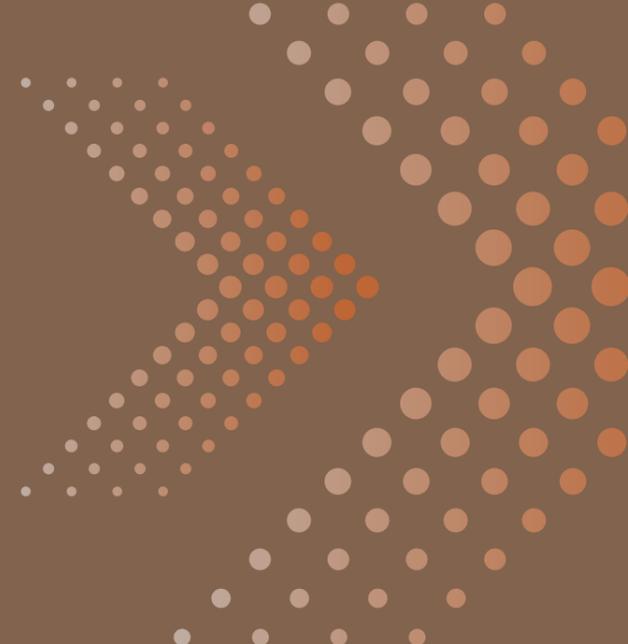


Cet été, offrez-vous  
une vue panoramique  
**de votre Système**  
**d'Information OT**



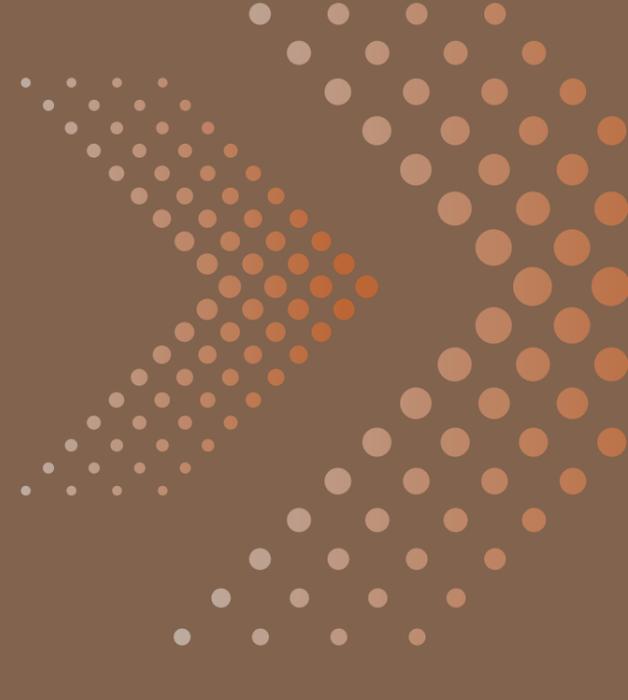


# + 250%

de cyberattaques industrielles  
entre 2021 et 2023

**Et vous, avez-vous  
une vraie visibilité ?**

# Sans visibilité, il n'y a pas de protection

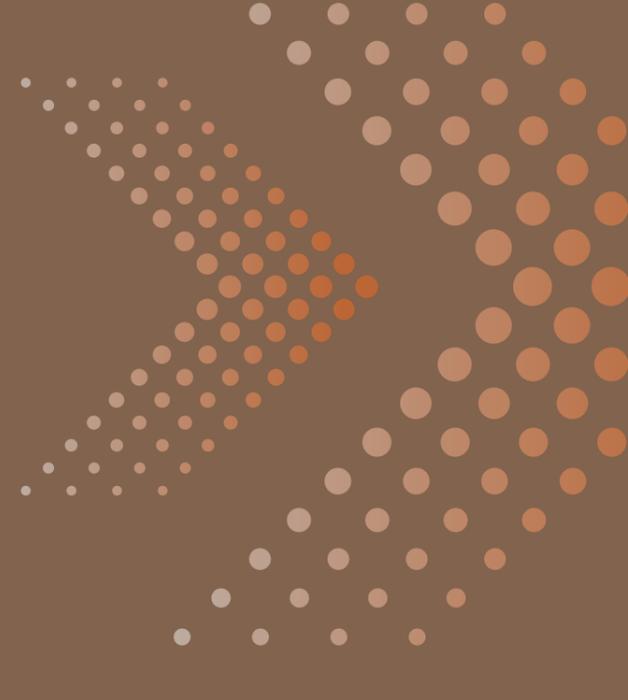


Les risques se cachent dans les zones d'ombre :

- ❌ Équipements non identifiés
- ❌ Connexions oubliées
- ❌ Assets mal documentés
- ❌ Mises à jour de logiciels non maîtrisées

**La cartographie OT est la base  
d'une cybersécurité solide**

# Pourquoi la cartographie OT est cruciale ?



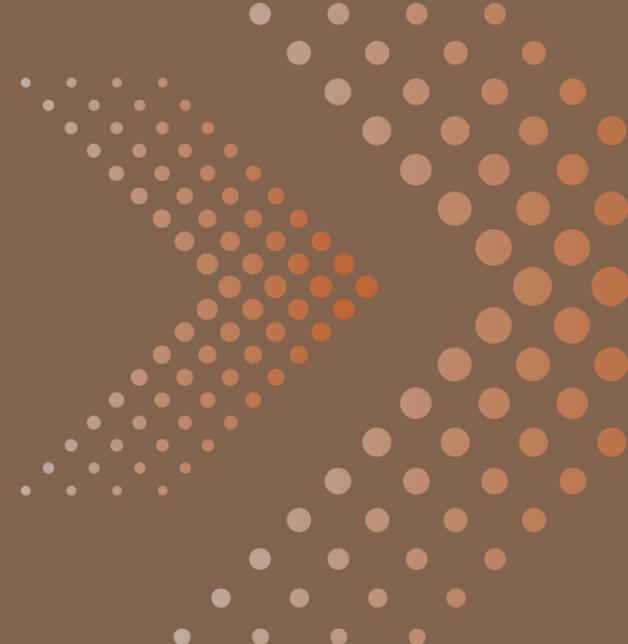
Elle vous permet de :

-  Identifier tous vos assets
-  Comprendre vos flux
-  Révéler les failles
-  Concevoir / Renforcer votre architecture OT sécurisée

**Un prérequis  
de la directive NIS 2 !**

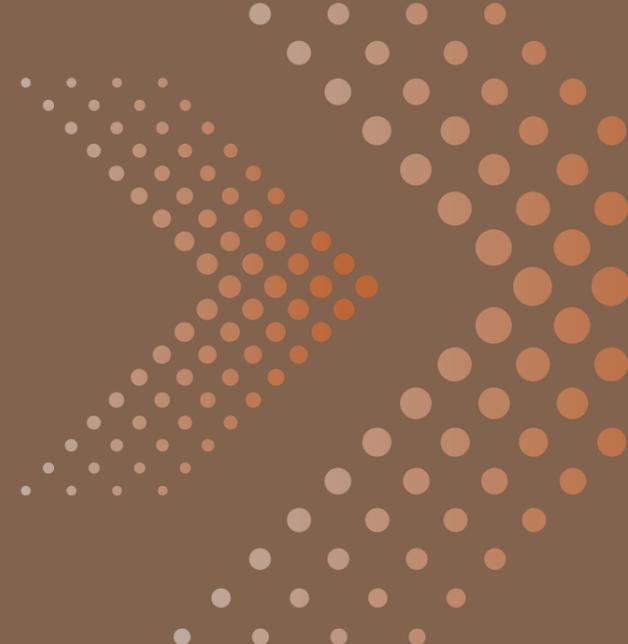


# Les 5 étapes d'une cartographie OT



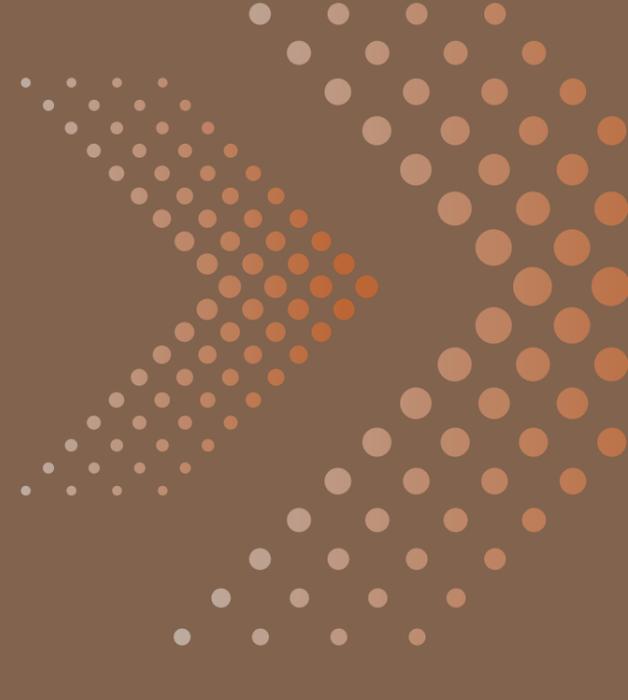
- 1** Spécification du besoin
  - 2** Recueil des informations existantes et échange avec les équipes
  - 3** Collecte des données sur site pour relever les assets et les flux via les solutions Seckiot
  - 4** Création des 6 vues recommandées par l'ANSSI
  - 5** Suivi et mise à jour selon la PSSI et recommandations
- 

# Construire une architecture OT sécurisée



Après la cartographie, on renforce son architecture OT pour protéger, segmenter et contrôler chaque asset identifié et chaque flux découvert.

# Des outils de protection indispensables



Déployer des outils comme les firewalls Stormshield et les switches Siemens sont essentiels pour :

-  Prévenir les intrusions
-  Limiter la propagation des attaques
-  Garantir la continuité opérationnelle

**Ces équipements forment  
un socle robuste pour  
sécuriser son SI OT**

# Cet été, on reste mobilisé

Nos équipes restent disponibles tout l'été pour vous accompagner dans vos projets de cybersécurité des réseaux OT :

-  Architecture
-  Cartographie
-  Audit & Diagnostic
-  Formation spécialisée
-  Assistance à distance

