Territoir+ Prod

# Cybersécurité : accompagner votre mise en conformité NIS2 #3

29 janvier 2026

By Les interconnectés

# Programme du jour

## Protection – Sécuriser les systèmes et formaliser les plans (partie 2)

- 9h : Accueil et tour de table
- 9h20 : Intervention de Hugo Longuespe, délégué à la sécurité numérique dans les Hauts-de-France, ANSSI
- 10h : définir et mettre en œuvre un PCA/PRA adapté à la taille et à la maturité de sa collectivité
- 10h30 : retour d'expérience de Lionel Pérès, DGS de la commune de Vaison-la-Romaine
- 11h : Pause
- 11h10 : Sécuriser ses relations contractuelles avec les prestataires
- 11h30 : Retour d'expérience de Paul-André Pincemin, délégué à la cybersécurité de Rennes ville et métropole
- 11h55 : Conclusion

# Les objectifs de ce cycle TP Cyber

## Un accompagnement pour préparer et faciliter sa mise en conformité

1. Comprendre le cadre réglementaire de la directive NIS2
2. Capitaliser sur des retours d'expérience terrain
3. Partager et découvrir des ressources techniques
4. Qualifier collectivement des bonnes pratiques pour renforcer sa politique cyber

Territoir+ Prod

By Les interconnectés

# Calendrier des travaux cyber

| T3 2025 | T4 2025 | JANVIER 2026 | T1 2026 |
| --- | --- | --- | --- |
| Animation du groupe miroir (3 rencontres avec l'ANSSI)<br><br>Animation de la Journée Expert Cyber à Bordeaux<br><br>Publication du baromètre avec un focus cyber | Lancement et animation du cycle Territoir'Prod Cyber (2 rencontres) | Examen et vote de la loi Résilience en séance publique à l'Assemblée nationale | Poursuite du travail du Territoir'Prod Cyber<br><br>Concertations possibles avec l'ANSSI pour travailler sur le cadre réglementaire<br><br>Élaboration d'un guide de bonnes pratiques |

Territoir+ Prod

By Les interconnectés

# Tour de table

| Prénom | Nom | Fonction | Collectivité |
|---|---|---|---|
| **Benjamin** | **MOSDALE** | RSSI | Grenoble-Alpes Métropole |
| **Sabrina** | **BANSE** | DPO/RSSI | CA Ventoux Comtat Venaissin |
| **Hélène** | **ETCHEGOYEN** | Responsable du service informatique | CC Lacq-Orthez |
| **Éric** | **ALABERT** | RSSI | Montpellier Métropole |
| **Sébastien** | **JAMES** | Responsable informatique de l'offre aux communes | Saint-Etienne Métropole |
| **Julien** | **GUYON** | RSSI | Eurométropole de Metz |
| **Frédéric** | **BALEYE** | Chef du Service SI | CC Terres des Confluences |
| **Corinne** | **TREBOSC** | Directrice DSI | CA Sicoval |
| **Christophe** | **BOVIO** | RSSI | CA Pau |
| **Lionel** | **PÉRÈS** | DGS | Vaison-la-Romaine |
| **Damien** | **CHRISMENT** | Responsable Service Infrastructure | Ville et Métropole de Rennes |
| **Paul-André** | **PINCEMIN** | Délégué à la cybersécurité | Ville et Métropole de Rennes |
| **Bruno** | **COLONNA** | Ingénieur sécurité des SI | Montpellier Métropole |
| **Manuel** | **SAINT-SERNIN** | Chef de projet technique DSIN | Saint-Étienne Métropole |

# Intervention de Hugo Longuespe

Délégué à la sécurité numérique de la région des Hauts-de-France (ANSSI)

Territoir+ Prod

By Les interconnectés

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

# ANSSI

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

# LES INTERCONNECTÉS

## ATELIER TERRITOIR'PROD CYBER – 29/01/2026

[Diffusion limitée à l'atelier Territoir'Prod Cyber]

# Les principales missions de l'Agence Nationale de Sécurité des Systèmes d'information (ANSSI)

Qualifier et certifier des produits et des services de cybersécurité
Promouvoir le « *Secure by design* »
Agir sur les dispositifs normatifs et réglementaires et contrôler leur bonne application

CERT-FR

**DÉFENDRE** les systèmes d'information critiques et les victimes de cyberattaques d'ampleur et la nation en structurant le niveau national d'assistance aux victimes

**CONNAÎTRE** l'état de l'art de la cybersécurité et les menaces du cyberespace et les tendances

**PARTAGER** de la connaissance, des recommandations et de l'expertise en sécurité numérique

**ACCOMPAGNER** l'écosystème national et international

**REGULER**


InterCERT FRANCE


Une menace systémique

- Lucrativité
- Déstabilisation
- Espionnage

**Aux origines diverses**

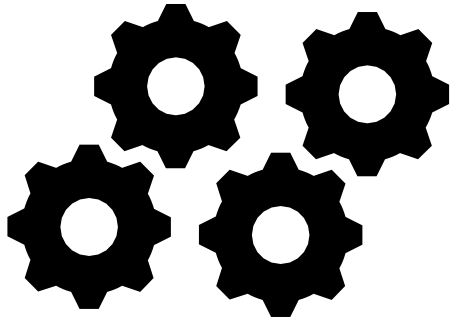
Cybercriminels

Attaquants réputés à un Etat dont Russie et Chine

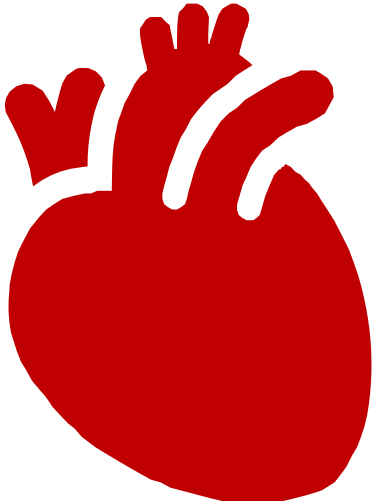
**Qui n'épargne personne**

**« Pas besoin d'être une cible pour être une victime »**

# LE RISQUE CYBER : UN CHANGEMENT DE PARADIGME



Hier
panne informatique =
risque technique



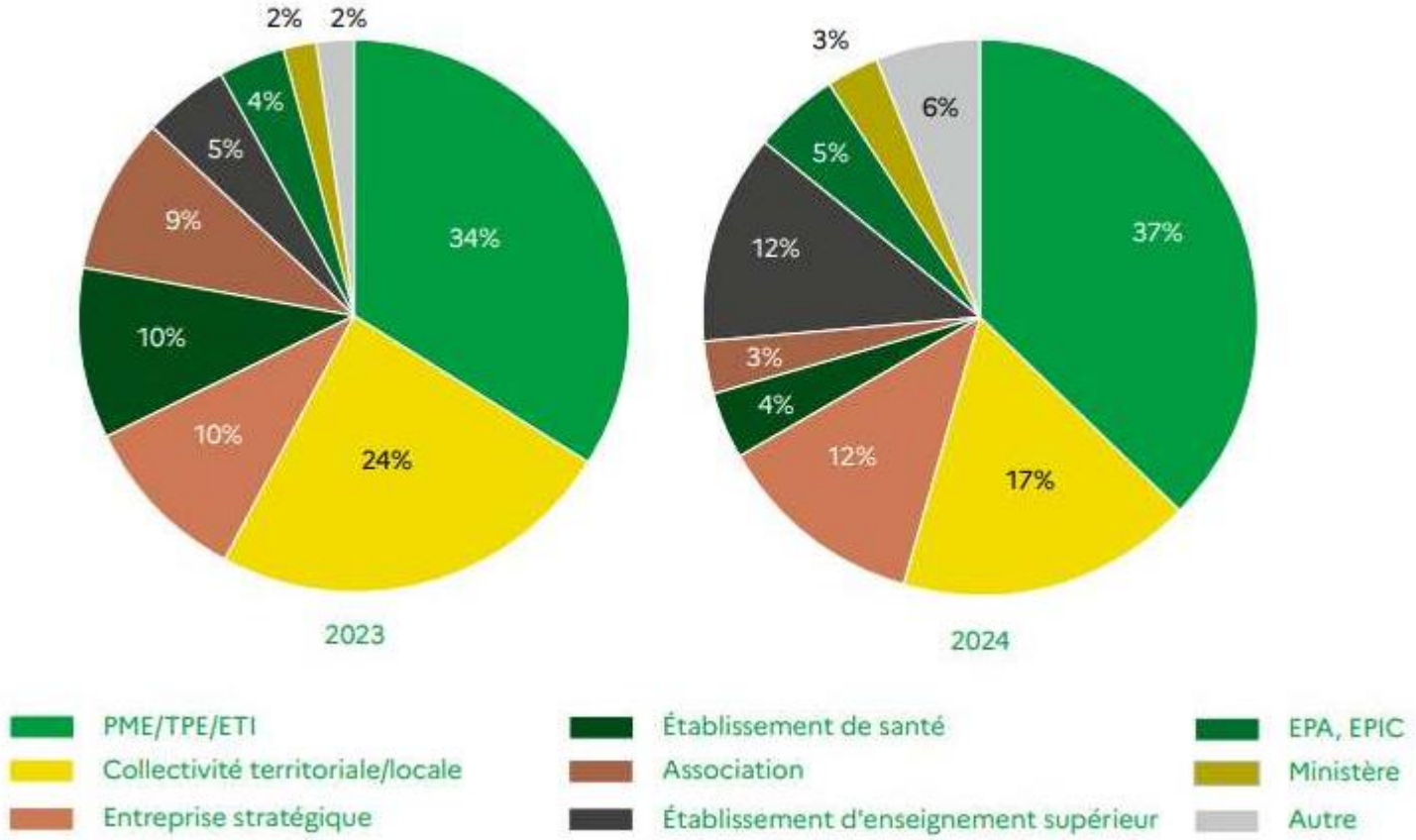
Aujourd'hui
cyber attaque =
risque stratégique
potentiellement vital

# Finalité lucrative

## Évolution des attaques par rançongiciel suivies par l'ANSSI

En 2024, 144 compromissions par rançongiciel ont été portées à la connaissance de l'ANSSI. Le nombre d'attaques se maintient à un niveau équivalent à 2023, et la menace associée demeure particulièrement importante pour la France.

## Répartition des victimes d'attaques par le biais de rançongiciels




[Diffusion limitée à l'atelier Territoir'Prod Cyber]

# Quelle cybermenace pèse sur les collectivités ?

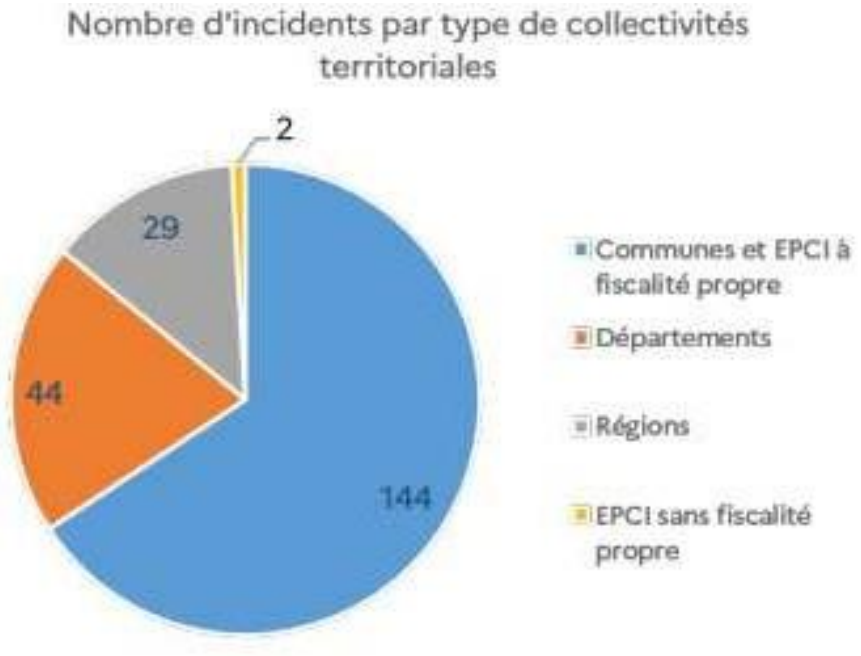


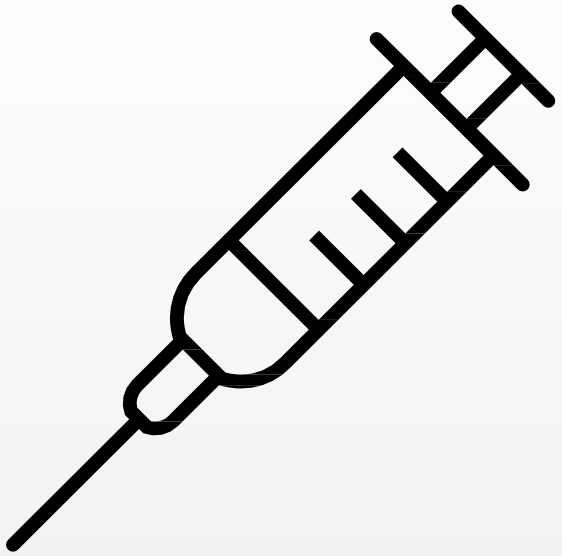

FIGURE 1 – Répartition des incidents portés à la connaissance de l'ANSSI en 2024

- Les types d'incidents ayant impactés les CT :

- Compromission de comptes de messagerie
- Attaques pas déni de service distribué (DDoS)
- Intrusions sur les SI : connexions illégitimes réussies avec dépôt de code malveillance / exploitation de vulnérabilités
- Chiffrement par rançongiciel
- Fuite des données personnelles des agents et des administrés avec publication
- Défiguration de suites Internet
- Effets de bord constatés sur d'autres CT en raison de l'interconnexion des SI

https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-002/

# LES VECTEURS DE COMPROMISSION



hameçonnage

vulnérabilités logicielles

liens numériques avec ses fournisseurs

# 5 mesures cyber préventives prioritaires

1. Renforcer l'authentification sur les systèmes d'information (double facteur)
2. Accroître la supervision de sécurité
3. Sauvegarder hors-ligne les données et les applications critiques
4. Etablir une liste priorisée des services numériques critiques de l'entité
5. S'assurer de l'existence d'un dispositif de gestion de crise adapté à une cyberattaque


# Anticiper et réagir





**Ressources gestion de crise**

**Kit d'exercice pour les collectivités territoriales**

# Découvrez comment progresser avec MesServicesCyber

## La plateforme publique des services et ressources cyber pour aider, proposée par l'ANSSI



**Accédez gratuitement à un catalogue complet de services et ressources**

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

# MERCI DE VOTRE ATTENTION

HAUTS-DE-FRANCE@SSI.GOUV.FR

**Ressources**

https://cyber.gouv.fr/
https://cert.ssi.gouv.fr/

# Définir et mettre en œuvre un PCA/PRA adapté à la taille et à la maturité de sa collectivité

Territoir+ Prod

By Les interconnectés

# Comprendre vos obligations

## 3 objectifs de sécurité communs

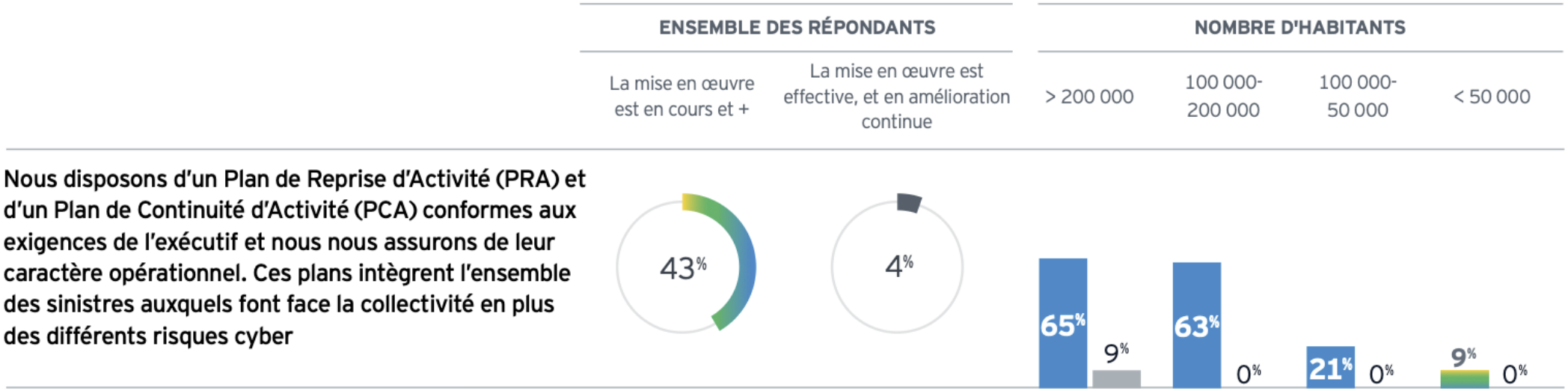
| Pilier | Objectif de sécurité (OS) |
|---|---|
| **RÉSILIENCE** | OS13. Continuité et reprise d'activité |
| | OS14. Réaction aux crises d'origine cyber |
| | OS15. Exercices, tests et entraînements |

Territoir+ Prod

By Les interconnectés

# Développer de bonnes pratiques

## Élaborer un plan de continuité d'activité (PCA)/plan de reprise d'activité (PRA)




[Lien vers le baromètre 2025]

Territoir+ Prod

By Les interconnectés

# Développer de bonnes pratiques

## Anticiper et gérer une crise cyber



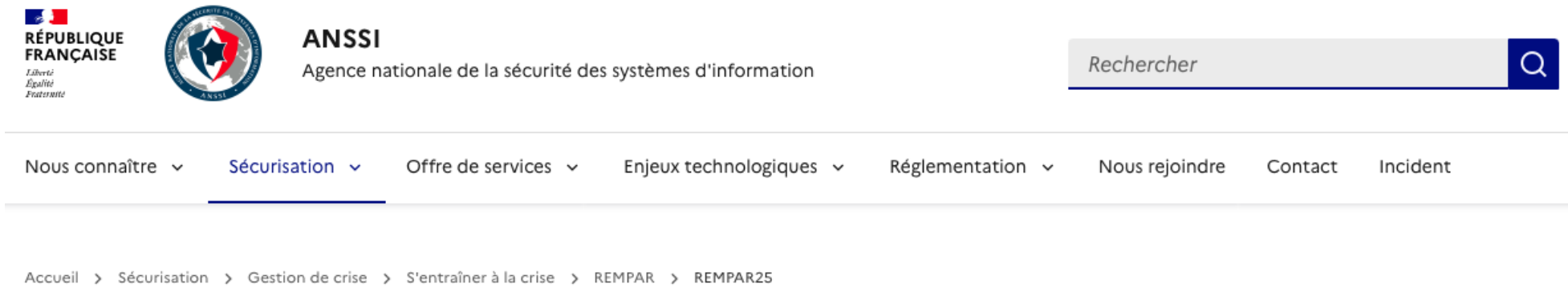

[Lien vers les guides]

Territoir+ Prod

By Les interconnectés

# Développer de bonnes pratiques

## Anticiper et gérer une crise cyber



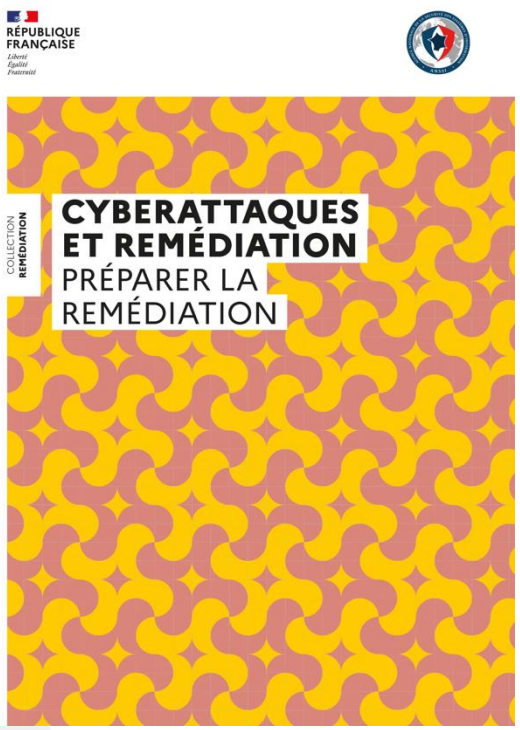

[Lien vers le RETEX]

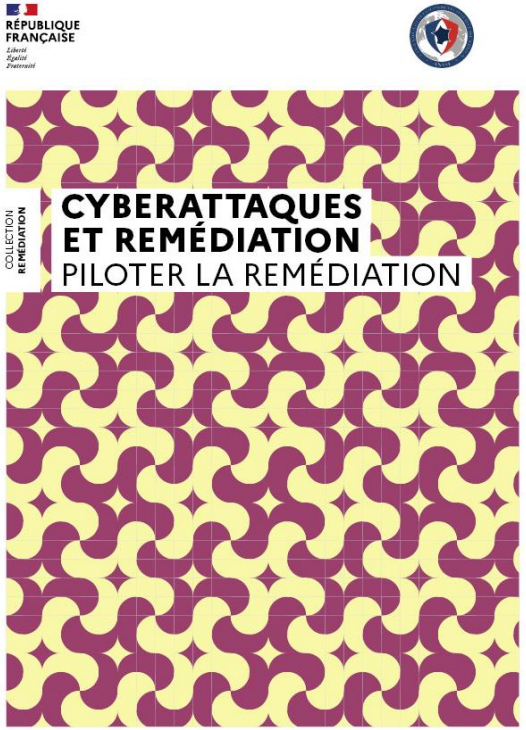
Territoir+ Prod

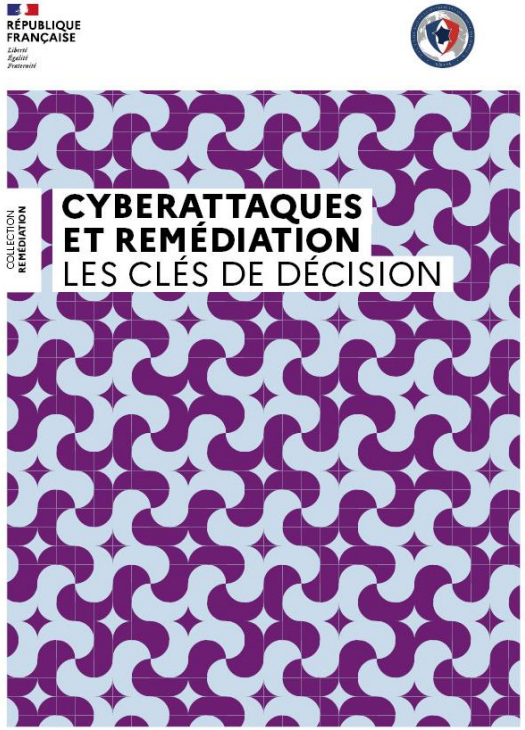
By Les interconnectés

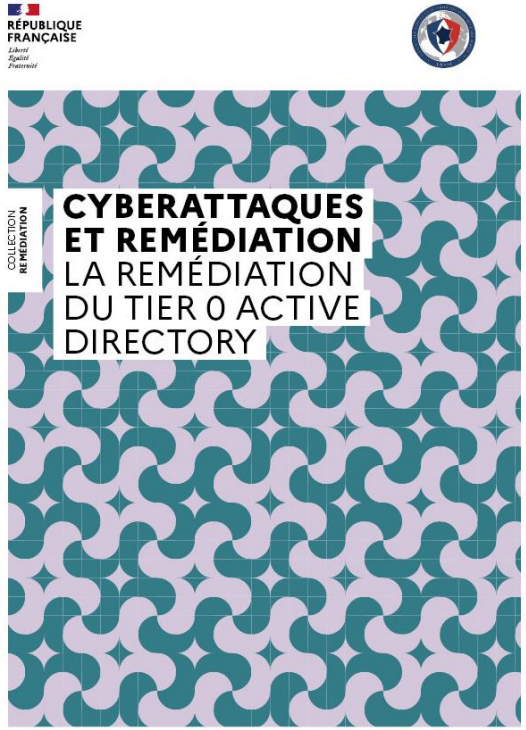
# Développer de bonnes pratiques

## Préparer la rémédiation : projet de reprise de contrôle d’un système d’information compromis et du rétablissement d'un état de fonctionnement suffisant




Lien vers les guides

Territoir+ Prod

By Les interconnectés

# Retour d’expérience de Lionel Pérès : préparer et mettre en œuvre son PCA

DGS de la commune de Vaison-la-Romaine

Territoir+ Prod

By Les interconnectés

# Pause

Territoir+ Prod

By Les interconnectés

# Sécuriser ses relations contractuelles avec les prestataires

Territoir+ Prod

By Les interconnectés

# Sécuriser ses relations contractuelles

## Les prestataires qualifiés par l'ANSSI


Lien vers le catalogue

Territoir+ Prod

By Les interconnectés

# Se rapprocher de ses interlocuteurs locaux

## Les CSIRT Territoriaux

| Territoire | CSIRT |
|---|---|
| Bourgogne-Franche-Comté | CSIRT Bourgogne-Franche-Comté |
| Bretagne | Breizh Cyber |
| Corse | CSIRT CyberCorsica \| Centre de cybersécurité de Corse |
| Centre-Val de Loire | CybeRéponse |
| Grand Est | Grand Est Cybersécurité |
| Hauts-de-France | CSIRT Hauts-de-France |
| Île-de-France | Urgence Cyber Île-de-France |
| Normandie | Normandie Cyber |
| Nouvelle-Aquitaine | Campus régional de Cybersécurité et de Confiance numérique |
| Occitanie | Cyber'Occ |
| Pays de la Loire | Pays de la Loire Cyber Assistance |
| Provence-Alpes-Côte d'Azur | Urgence Cyber région Sud |

| Territoires | CSIRT |
|---|---|
| Guadeloupe, Guyane, Martinique, Saint-Barthélémy, Saint-Martin, Saint-Pierre-et-Miquelon | CSIRT-ATLANTIC |
| Nouvelle-Calédonie | Centre Cyber du Pacifique |
| Réunion | CSIRT LA RÉUNION |

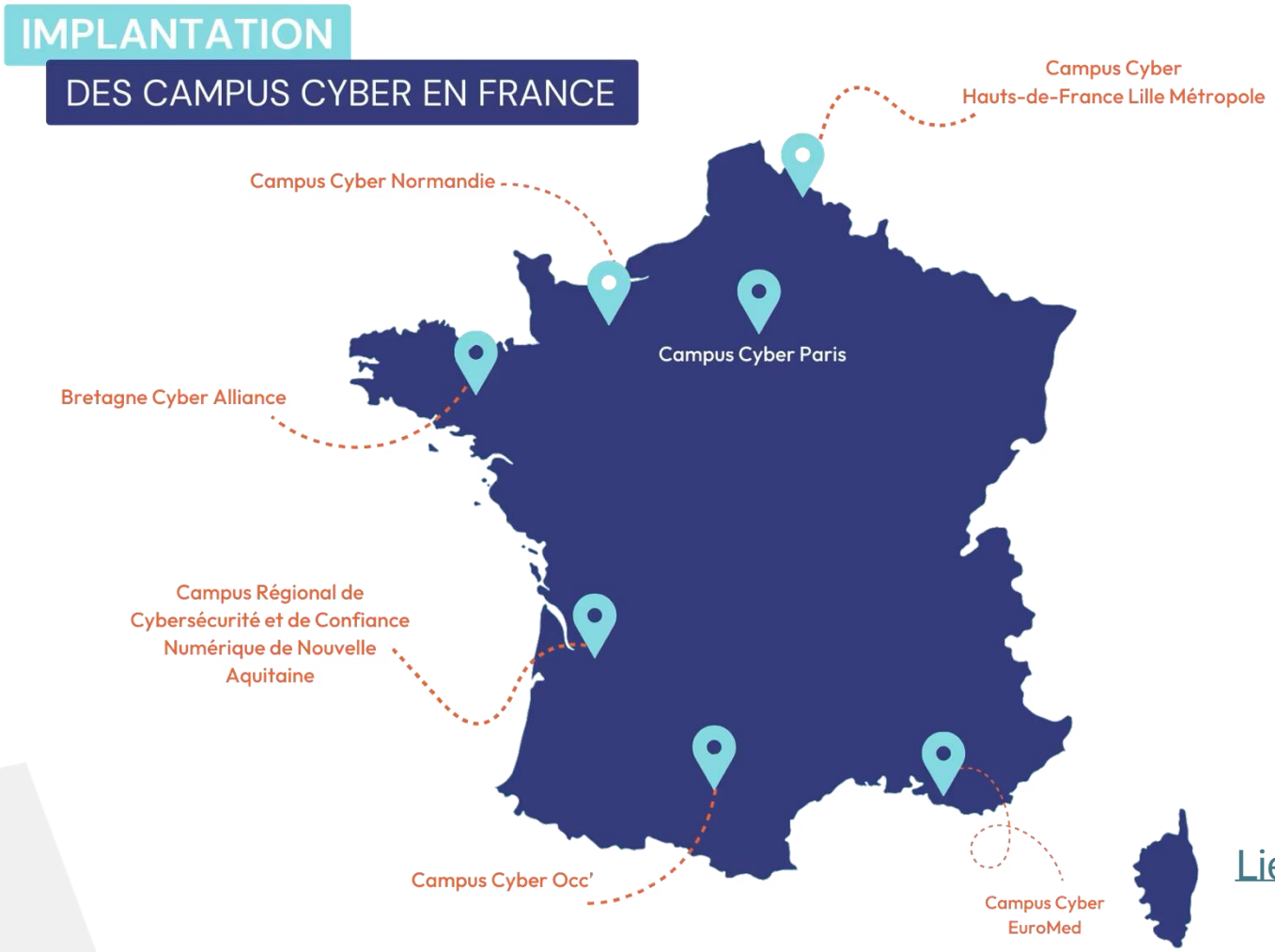
Lien vers la liste des CSIRT

Territoir+ Prod

By Les interconnectés

# Se rapprocher de ses interlocuteurs locaux

## Les Campus Cyber




[Lien vers la liste des Campus Cyber]

Territoir+ Prod

By Les interconnectés

# Retour d’expérience de Paul-André Pincemin

Délégué à la cybersécurité de Rennes ville et métropole

Territoir+ Prod

By Les interconnectés

# 4. Présentation du guide Cyber à destination des collectivités


**GUIDE**

Intégration du risque cyber au plan communal de sauvegarde des petites communes

Novembre 2024

Région Bretagne

Ministère des Armées et des Anciens Combattants

Rennes Métropole

# Quelques éléments de contexte 1/2

- La feuille de route cyber de Rennes Métropole s'articule autour de 4 axes :

1. Développement économique (RH, startups, locaux sécurisé, plate-forme) ;
2. L'attractivité, en particulier de talents ;
3. La cybersécurité des territoires ;
4. La diffusion des bonnes pratiques cyber au plus grand nombre.

- Concernant l'axe 3, RM est partenaire du CSF des industries de sécurité et membre du PEC.
- Elle y porte le sujet de la cyber protection des territoires.

# Quelques éléments de contexte 2/2

- Deux constats partagés dans ces deux instances :

- Beaucoup d'acteurs publics ou parapublics en appui de la cybersécurité ;
- Un angle mort dans le soutien à la cybersécurité des territoires : les petites communes.

- Une double opportunité identifiée dans le cadre de ces instances :

- La mise à jour des PCS en 2026 ;
- Travail de concert pour réaliser un guide pour accompagner la prise en compte de la cyber dans les PCS des petites communes

# Objectif fixé en novembre 2023

- Réaliser une première version du guide pragmatique pour l'ECW 2024
- En embarquant un maximum d'acteurs en soutien de la cyberprotection des territoires :

- Des élus de petites communes ;
- le réseau des RSSI des collectivités ;
- le réseau des DPO des grande villes et métropole ;
- ANSSI ;
- Préfecture ;
- Les CSIRT ;
- Cybermalveillance.gouv.fr ;

- Pour qu'il devienne le document de référence pour cette communauté
- Avec cette préoccupation d'améliorations incrémentale au regard des retours

# Structuration du document

- Rappel de quoi on parle, en l'occurrence les missions qui peuvent être impactées *(page 6 et annexe C page 40)* ;
- Les bonnes pratiques / les bons réflexes en cas de suspicion d'attaque *(page 8 annexe B page 30)* ;
- Quelques recommandations qui nous semblaient utiles pour :
    - la mise en place de la cellule de gestion de crise *(page 11)* ;
    - L'élaboration du PCA *(page 12 annexes D et E pages 40)* ;
- Quelques pistes complémentaires concernant :
    - Les bonnes pratiques en amont *(page 14)* ;
    - Les impacts physiques et psychologiques des crises cyber sur les agents *(p16)* ;
    - La prise en compte du risque cyber dans les achats *(page 19)* ;
    - Des pistes pour en savoir plus sur son niveau de risque cyber en l'état *(page 23)* ;
    - Et pour ceux qui souhaiteraient aller plus loin, quelles ressources *(page 25)* .

• Avec une logique de poupée gigogne.

# Limite du document

- C’est une seconde version réalisée en un temps contraint :
  - Qui a pris en compte des demandes spécifiques (facteur humain, assurance) ;
  - D’autres sans doute à prendre en compte pour l’ECW 2026 ;
  - L’occasion d’identifier des chantiers à traiter à part entière (mutualisation…).

- Surtout c’est un document qui ne demande qu’a être complété :
  - Pour le rendre encore plus « clé en main » pour l’élaboration des PCS ;
  - Une nouvelle version tous les ans ;
  - Avec une limite due aux spécificités de chaque commune (ex PCA).

- Pour communiquer de vos remarques, demandes de complément ou commentaires => pa.pincemin@rennesmetropole.fr

- Lien vers le doc : www.pole-excellence-cyber.org/publications/

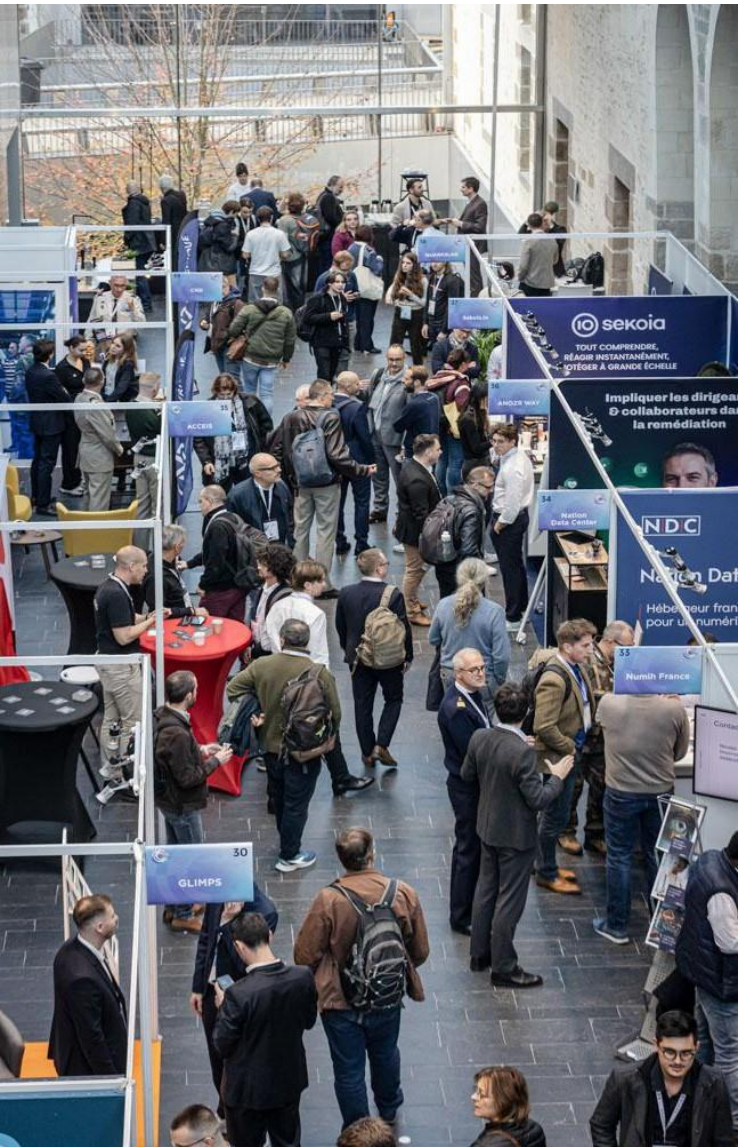
HOPSCOTCH

PÔLE D'EXCELLENCE CYBER

# EUROPEAN CYBER WEEK

Le rendez-vous européen de la cyber au service des territoires

# Qu’est ce que l’European Cyber Week ?




**C’est un congrès européen majeur dédié à la cybersécurité, à la cyberdéfense et à l’intelligence artificielle** appliquée à ces domaines. C’est **un rendez-vous professionnel et stratégique**, organisé chaque année par le *Pôle d’excellence cyber* et ses membres avec le soutien du ministère des Armées, de la Région Bretagne et de Rennes métropole, qui réunit **les principaux acteurs civils et militaires**, entreprises, institutions, chercheurs, startups, et experts du secteur numérique.

- **Un congrès professionnel**, avec des **conférences, tables rondes, ateliers, démonstrations technologiques et sessions de networking** autour des enjeux actuels et futurs du numérique sécurisé (cybersécurité, cyberdéfense, souveraineté numérique, IA, etc.).

- **Un lieu d’échanges et de coopération** entre acteurs publics et privés pour renforcer l’autonomie européenne face aux menaces cyber.

- **Un événement orienté vers l’innovation**, la formation, le recrutement et le développement industriel et économique dans le domaine de la sécurité numérique.

**L'European Cyber Week (ECW), ne traite pas la cybersécurité comme un sujet uniquement technique, mais comme un enjeu stratégique, régalien et européen, au croisement de la défense, de l'industrie, de la recherche et des politiques publiques.**

**01** Défense

**02** Sécurité Intérieure

**03** Protection des infrastructures critiques

**04** Résilience des services publics

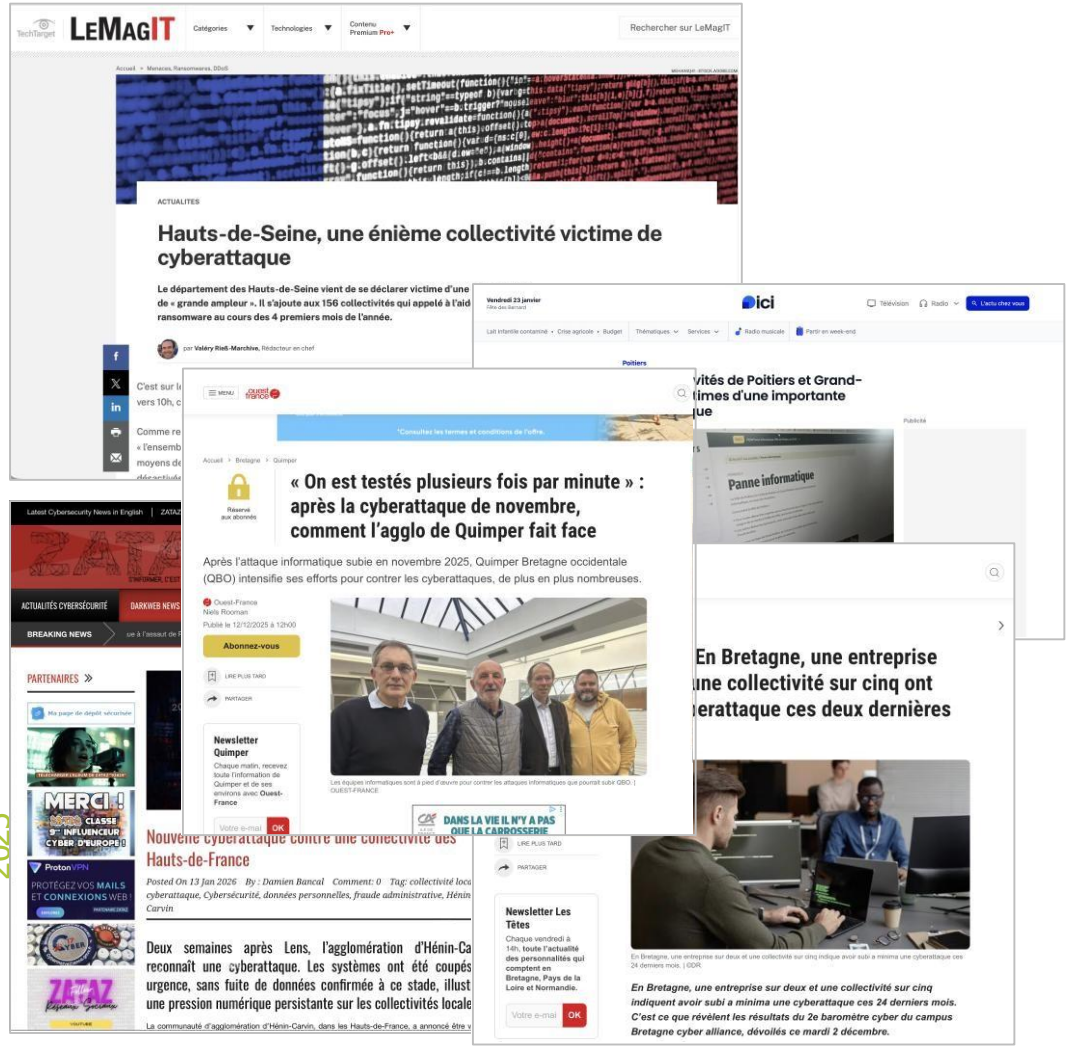
**05** IA de Défense

**06** Lutte informationnelle

## Avec un écosystème unique

- État : ANSSI, DGA, COMCYBER, DGSE, AMIAD, DRSD…
- Collectivités & territoires
- Industriels
- Startups
- Universités & recherche
- Europe & partenaires internationaux

# l’ECW, un évènement phare pour les collectivités




1 / **Les collectivités sont en première ligne (eau, transports, hôpitaux, mairies, écoles…)**

2/ **Elles sont les cibles prioritaires des attaques**

3/ **Elles ont besoin de solutions, compétences et réseaux**

**L’ECW est un point d’entrée unique vers tout l’écosystème cyber**

# ECW : Pourquoi est-elle utile aux collectivités ?

- Comprendre les menaces réelles
- Identifier des solutions souveraines
- Rencontrer les bons acteurs
- Anticiper NIS2, résilience, continuité d'activité
- Former élus et DSI

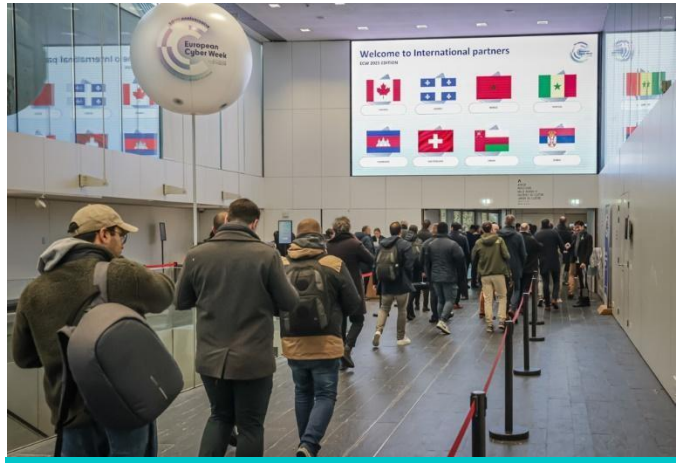
# ECW : Ce que les collectivités viennent y chercher ?

- Vision stratégique
- Solutions concrètes
- Retours d'expérience
- Partenariats

# ECW : Place de marché cyber pour les territoires

- Pairs
- fournisseurs
- experts
- formations
- diagnostics
- projets européens
- financement

# CHIFFRES CLÉS « ÉVÉNEMENT »




**8 500 inscriptions**

**3,5 jours**


**130 partenaires**

**+35 conférences**

**1 keynote Ministérielle**

**11 ateliers Industriels**

MERCI À TOUS

# ET RENDEZ-VOUS POUR L'ECW 2026 DU 16 AU 19 NOVEMBRE 2026

À vos agendas :

*Vos prochains rendez-vous à ne pas manquer !*

Territoir+ Prod

By Les interconnectés

# Vos rendez-vous à ne pas manquer !

**5 février 2026**
TP IA #4

**26 mars 2026**
TP Inclusion #4

**2 avril 2026**
TP Territoires connectés responsables #2 conjoint au TP Data

**Territoir' Prod**

Territoir+ Prod

Territoir+ Prod

By Les interconnectés


forum.interconnectes.fr

1ER ET 2 JUIN 2026
**STATION F**

Les interconnectés
RÉSEAU DES TERRITOIRES INNOVANTS

- 1 et 2 juin 2026 - **Station F**, Paris
- <u>Enjeux de cette édition</u> :
  - Lancement du nouveau mandat avec les élus et les agents ;
  - L'indépendance numérique des territoires.

Territoir+ Prod

By Les interconnectés