



Les

interconnectés

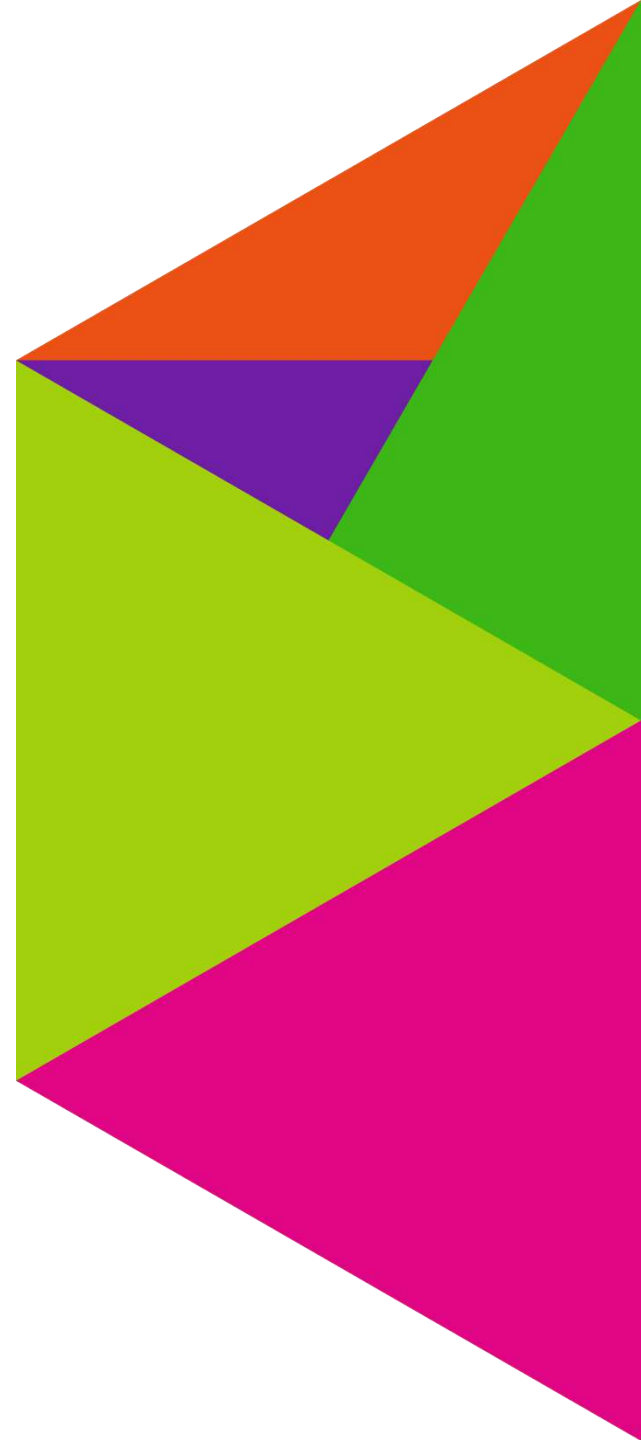
RÉSEAU DES TERRITOIRES INNOVANTS

Politiques numériques pour tous les territoires :

Mise à l'épreuve des dispositifs de coopération et mutualisation pour la stratégie de cybersécurité

5^e réunion plénière

22 septembre 2026



► Les partenaires de la démarche



- Engagée en faveur d'une politique nationale d'aménagement et de transformation numérique ambitieuse
- Marlène le Dieu de Ville, vice-présidente en charge du numérique



- Porter une vision politique du numérique
- Accompagner la montée en compétences des élus et des agents
- Favoriser l'intelligence collective et le partage entre pairs et experts



Accompagnement Numérique Sur Mesure (ANSM)

- Communes de moins de 3 500 habitants
- Intercommunalités de moins de 15 000 habitants

La Suite Territoriale

- Plateforme sécurisée
- Outiller les collectivités dans leurs besoins



Ordre du jour

1. Cartographier les acteurs de l'écosystème mobilisables pour mettre en œuvre la stratégie cybersécurité

➤ Retour d'expérience de la communauté de communes Lacq-Orthez

2. Les dispositifs applicables à la stratégie cybersécurité

➤ Retour d'expérience de Pays d'Iroise Communauté



TERRITOIR'PROD

Accompagner les agents et mettre en œuvre la stratégie

Dédié aux agents des collectivités adhérentes, le programme Territoir'Prod se constitue de groupes de travail thématiques de formation et de partage entre pairs.

L'OBJECTIF ?

- Acquérir les connaissances et compétences nécessaires à la réalisation et au déploiement des stratégies numériques sur son territoire
- Échanger avec d'autres collectivités plus ou moins développées sur les sujets
- Retours d'expérience d'experts et de collectivités

RYTHME DE TRAVAIL SUR CHACUNE DES THÉMATIQUES.

- 3 demi-journées en visioconférence
- 1 journée expert en présentiel



Face à l'accélération des usages de l'IA et à sa diffusion massive dans la vie publique, les collectivités doivent se doter de repères solides pour agir de manière éclairée et responsable.

En 2025, les Territoir'Prod IA ont permis de construire collectivement un carnet d'inspirations pour mieux maîtriser ces systèmes. Les participants ont exploré différentes pratiques de gouvernance, partager leurs retours d'expériences de leurs expérimentations documentées dans la bibliothèque d'IA territoriale et travaillé sur la transparence des usages via les registres d'algorithmes publics.

Le programme 2026 se concentrera sur la mise en application de l'IA sur des cas d'usages concrets en lien avec la bibliothèque d'IA.

LE PROGRAMME DE TRAVAIL

-  Rappel des bonnes pratiques de gouvernance interne et du cadre juridique de l'IA Act, veille sur les chartes et aide à l'appropriation du clausier IA
-  Examen de cas d'usages au service des missions des collectivités à chaque séquence (eau, énergie, mobilité, urbanisme...)
-  Partage de ressources au service de la sensibilisation et la formation à l'IA selon les publics
-  Accompagner la mobilisation du référentiel IA frugale
-  Anticiper les enjeux de dépendances à ces systèmes et contribuer à la qualification de l'offre de solutions d'IA souveraine pour les collectivités (en lien avec le parcours « Tie Break »)

PARTENAIRE ASSOCIÉ

Commissariat Général au
Développement Durable



PROCHAINES DATES : 1^{er} octobre / 26 novembre

Le programme Territoir'Prod Cybersécurité vise à accompagner les collectivités pour **faciliter leur mise en conformité à la directive NIS 2**, transposée dans la loi Résilience qui sera prochainement adoptée.

Quatre séquences sont organisées pour mieux comprendre ce nouveau cadre réglementaire, en s'appuyant sur le référentiel de sécurité élaboré par l'ANSSI. Afin d'anticiper les obligations à venir, ces séquences visent à :

- Capitaliser sur des retours d'expériences terrain
(mise en œuvre d'un plan de continuité d'activité adapté à la taille de sa collectivité)
- Partager des ressources techniques
(MesServicesCyber et MonServiceSécurisé de l'ANSSI)
- Qualifier collectivement les bonnes pratiques pour renforcer sa politique cyber
(mener une analyse des risques)

LE PROGRAMME DE TRAVAIL

-  Gouvernance : structurer sa stratégie cybersécurité, organisation des plans de sauvegarde (PCS, PICS) et coopérations territoriales
-  Protection : sécuriser les systèmes d'informations et identification d'outils dédiés (exemple : authentification multifacteur – MFA)
-  Résilience : être prêt en cas d'incident cyber et sensibilisation des agents, élus
-  Défense : réagir à une cyberattaque

PARTENAIRE ASSOCIÉ



PROCHAINES DATES : 12 novembre / 3 décembre

VOS PROCHAINS RENDEZ-VOUS

SEPTEMBRE		OCTOBRE		NOVEMBRE		DÉCEMBRE	
3	 Réunion de lancement et de présentation des TP	1 ^{ER}	 TP Intelligence artificielle	4	 TP TIE Break	2	 TP TIE Break
9	 TP TIE Break	7	 TP TIE Break	12	 TP Cybersécurité	3	 TP Cybersécurité
11	 TP Inclusion / accessibilité	8	 TP Inclusion / accessibilité	17	 Numérique pour tous les territoires	10	 TP Data
17	Webinaire Cybersécurité	12	 TP Data	19	 TP Numérique responsable		 Journée Expert
22	 Numérique pour tous les territoires			26	 TP Intelligence artificielle		
24	 TP Numérique responsable				 Journée Expert		



Inscription aux rendez-vous directement sur notre site !

<https://www.interconnectes.com/events>

[Lien vers les livrables de l'association](#)

Les obligations en matière de cybersécurité : ce qu'il faut savoir



Les obligations de la directive NIS 2

Gouvernance

- Définir un cadre de gouvernance de la sécurité numérique des systèmes d'information et responsabiliser les acteurs internes et externes de l'écosystème

Protection

- Sécuriser les systèmes d'information et assurer l'authentification des utilisateurs pour résorber les vulnérabilités

Résilience et Défense

- Anticiper et réagir aux incidents cyber en mettant en œuvre des mécanismes de sauvegarde et en réalisant des tests pour vérifier l'efficacité des outils

Cartographier les acteurs de l'écosystème mobilisables pour mettre en œuvre la stratégie cybersécurité



Cartographier les acteurs de l'écosystème mobilisables

	Accompagnement et sensibilisation	Formation	Financements	Achats
Acteurs institutionnels et publics	<u>Acteurs à l'échelle de l'État</u> ANSSI 17Cyber CERT-FR Cybermalveillance ANCT	<u>Acteurs à l'échelle de l'État</u> ANSSI ANCT	<u>Acteurs à l'échelle de l'État</u> Banque des territoires	<u>Acteurs à l'échelle de l'État</u> ANCT
	<u>Acteurs à l'échelle locale</u> ANSSI en région CSIRT Campus Cyber Syndicats mixtes GIP Gendarmerie Autres collectivités	<u>Acteurs à l'échelle locale</u> Campus Cyber GIP	<u>Acteurs à l'échelle locale</u> Syndicats mixtes Agence technique départementale	<u>Acteurs à l'échelle locale</u> Centrales d'achats
Acteurs privés	Orange Cyberdefense Club de la Continuité d'Activité Club de la Sécurité Numérique des Collectivités			Prestataires de solutions cyber





Les centres d'appel et de réponses aux incidents cyber (CSIRT)

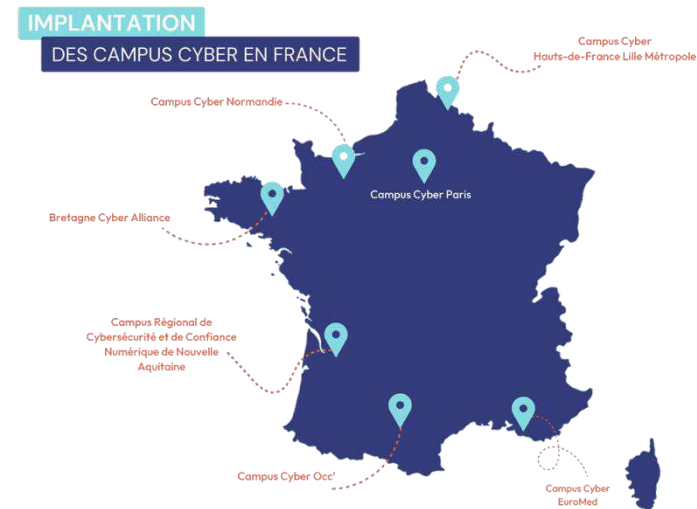
- Réponse de 1^{er} niveau et de proximité aux incidents cyber
- Relais entre les acteurs du secteur privé et du secteur public pour favoriser la mise en relation autour des enjeux de cybersécurité

Territoire	CSIRT/CRC
Atlantique : Guadeloupe, Guyane, Martinique, Saint-Barthélemy, Saint-Martin, Saint-Pierre-et-Miquelon	CSIRT-ATLANTIC
Auvergne-Rhône-Alpes	Cyber Assistance Auvergne-Rhône-Alpes
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
Nouvelle-Calédonie	Centre Cyber du Pacifique
Occitanie	Cyber'Occ
Pays de la Loire	Cyber Assistance
Provence-Alpes-Côte d'Azur	Urgence Cyber région Sud
Réunion	CSIRT La Réunion



► Les Campus Cyber

Campus Cyber	Campus Normandie Cyber	Campus Cyber Occ'	Campus Cyber.IA EuroMed	Hub Grand Est Cybersécurité
Caractéristiques et offres	Rassemblé avec le CSIRT au sein de l'association Normandie Numérique • Accès à des ressources et expertises cyber • Évènements et actions de sensibilisation	Héberge le CSIRT Ressources pour réagir en cas d'incident cyber Catalogue des formations en cybersécurité	Partenaire du CSIRT Urgence Cyber Accompagnement des acteurs locaux pour • Renforcer la cybersécurité • Adopter une IA sécurisée	Sensibilisation et formation • Développer les compétences cyber sur le territoire Fédérer les acteurs publics, privés et académiques



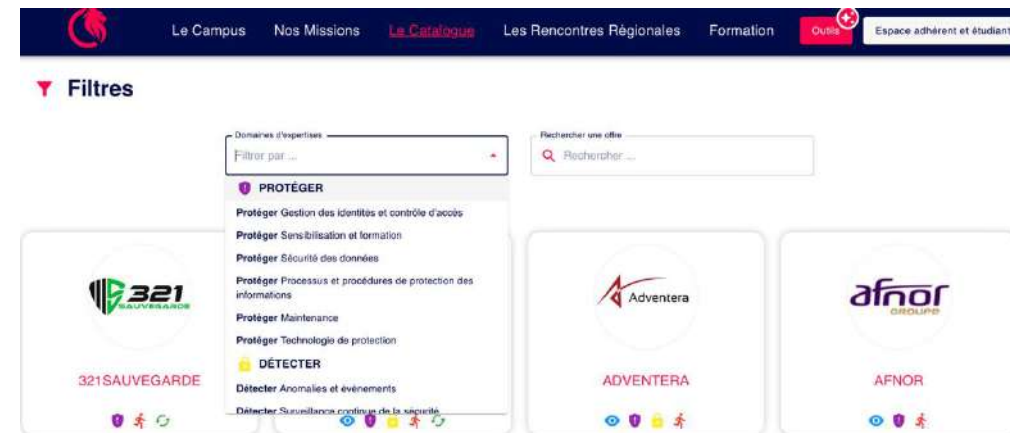
► Les Campus Cyber

Campus Cyber	Campus Cyber Paris	Campus Cyber Hauts-de-France Lille Métropole	Bretagne Cyber Alliance	Campus Régional de Cybersécurité et de Confiance Numérique de Nouvelle-Aquitaine
Caractéristiques et offres	Partenaire du CSIRT Urgence Cyber • Formations • Sensibilisation	Formations • Cyber Range • Capture the Flag (CTF) Répertoire des formations en cybersécurité dans la région	Partenaire du CSIRT Breizh Cyber • Guide des parcours de sécurisations et des aides mobilisables	Formation et sensibilisation • Projets « Référentiel de compétences », « Contenu pédagogique référent cyber », « Mallette de sensibilisation » Veille technologique Prévention Catalogue de l'offre cyber régionale

► Les Campus Cyber : leurs ressources en ligne



[Lien vers le guide des parcours de sécurisations et des aides mobilisables](#)



[Lien vers le catalogue de l'offre cyber régionale](#)



[Lien vers le répertoire des formations en cybersécurité de la région](#)

► Les prestataires de solutions cybersécurité

Prestataires de solutions	PACS (prestataires d'accompagnement et de conseil en sécurité)	PASSI (prestataires d'audit en sécurité des systèmes d'information)	PAMS (prestataires d'administration et de maintenance sécurisée)	PDIS (prestataires de détection des incidents de sécurité)	PRIS (prestataires de réponses aux incidents de sécurité)
	Accompagnent le commanditaire dans la démarche de sécurisation de son SI et de son maintien en condition de sécurité	Évaluent qu'un système d'information satisfait aux critères d'audit sélectionnés par le commanditaire	Assurent l'infogérance, ou prise en charge des ressources informatiques, des systèmes d'information	Supervisent en temps réel les activités au sein d'un système d'information pour détecter toute activité anormale ou potentiellement malveillante	Interviennent pour qualifier un incident cyber, voire identifier le mode opératoire de l'attaquant et ses objectifs



► Les prestataires de solutions cybersécurité

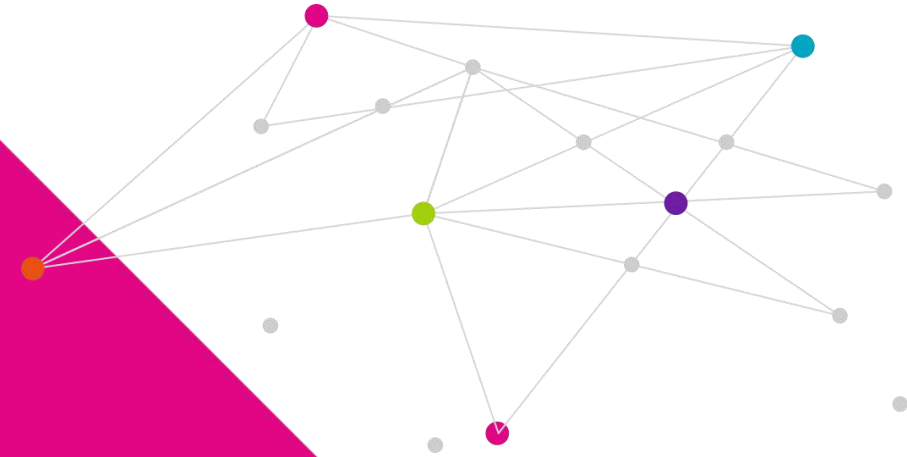


[Catalogue des produits et services qualifiés par l'ANSSI](#)

Retour d'expérience

Marlène Le Dieu de Ville

- *Conseillère communautaire, Communauté de communes Lacq-Orthez*
- *Vice-Présidente d'Intercommunalités de France en charge du numérique*
- *Co-présidente de la Commission numérique*



1. Un territoire, plusieurs écosystèmes

Première étape : distinguer les périmètres, les moyens et les responsabilités

CCLO — SON PÉRIMÈTRE

- Une organisation informatique propre
- Des moyens cyber pour ses propres systèmes
- Des métiers et services nombreux

- La CCLO intervient peu ou pas directement dans la cybersécurité des communes

60 COMMUNES — DES RÉALITÉS DIVERSES

- De très petites communes à une ville de plus de 11 000 habitants
- Peu de compétences informatiques internes dans les plus petites
- Des outils numériques propres
- Des prestataires informatiques propres

AUTRES ACTEURS DU TERRITOIRE

- Hôpital, SDIS, entreprises, industriels...
- Des infrastructures et systèmes propres
- Des responsabilités distinctes
- Des interdépendances possibles en cas de crise

Idée clé : le territoire n'est pas un SI unique, mais une juxtaposition d'acteurs et de responsabilités.

2. Pour sécuriser l'EPCI : cartographier ses appuis

Deuxième étape : distinguer les ressources internes, de proximité et spécialisées

1 — EN INTERNE

- Service informatique / DSI : exploitation et sécurité au quotidien
- RSSI : gouvernance, risques et règles de sécurité
- Services métiers : besoins, données et continuité
- Médiateurs numériques : prévention et sensibilisation

2 — À PROXIMITÉ

- Fibre64 : outils, prestations et réseau RIL
- Campus Cyber Nouvelle-Aquitaine
- CRiC-NA : assistance technique en cas d'incident
- Délégués territoriaux ANSSI : conseil et orientation

3 — EXPERTISES À MOBILISER

- ANSSI : méthodes, référentiels et dispositifs
- Prestataires spécialisés : audit, risques, pentest, conseil
- Compétences externes mobilisées lorsque l'interne ne suffit pas
- Exemple CCLO : France Relance → audit approfondi → fonction RSSI

La cybersécurité n'est pas seulement un sujet informatique : les métiers et la direction ont aussi un rôle.

3. Pour une petite commune : cartographier un écosystème plus diffus

Troisième étape : identifier les interlocuteurs réellement accessibles au quotidien

AU QUOTIDIEN

- Élus et secrétariat de mairie
- Prestataire informatique habituel
- Postes, réseau, sauvegardes, logiciels...
- Des compétences cyber variables selon les prestataires

RESSOURCES TERRITORIALES

- Fibre64 : centre de ressources pour les collectivités (Bouclier Cyber); outils et actions de sensibilisation ; centrale d'achats, interlocuteur LaSuite numérique de l'ANCT
- APGL : accompagnement DPO / RGPD selon les besoins
- Des dispositifs existants, mais pas toujours connus des petites communes

EN CAS DE BESOIN

- Gendarmerie : interlocuteur spontanément saisi lors d'une attaque
- Prestataire informatique : remise en fonctionnement selon ses compétences
- CCLO : pas de service cyber mutualisé pour les communes
- Les circuits restent aujourd'hui largement propres à chaque commune

Une petite commune n'est pas sans ressources : son écosystème est simplement plus extérieur et moins structuré.

4. Des écosystèmes distincts... mais pas étanches

Quatrième étape : repérer les interfaces et savoir qui fait quoi lorsqu'un incident survient

INTERACTIONS COMMUNES ↔ CCLO

- Échanges de données et outils selon les compétences, notamment le SIG
- Relations quotidiennes entre collectivités ; actions de sensibilisation possibles avec Gendarmerie / ANSSI

SI LA CCLO EST ATTAQUÉE

- DSI / RSSI : pilotage interne
- CRiC-NA : assistance technique
- ANSSI : notification / appui selon le cas
- Forces de l'ordre : plainte et enquête

SI UNE COMMUNE EST ATTAQUÉE

- Gendarmerie : généralement saisie directement
- Prestataire informatique : intervention technique
- CCLO : informée par la commune et/ou la Gendarmerie
- Fibre64 : informée ; mobilisée si son propre champ est concerné

Une autonomie informatique qui n'exclut ni les échanges ni les interdépendances.

5. Des pistes de travail envisagées

Réflexions non encore validées ni engagées par la CCLO — partagées comme sources d'inspiration

1 — VOLET CYBER DU PICS

- Fiches réflexes utilisables par les communes
- Qui appeler ? Qui informer ? Que faire immédiatement ?
- Articulation possible avec le PCS communal
- Relations avec la CCLO en cas d'incident partagé
- Continuité des services essentiels
- Information de la population en mode dégradé

2 — CHARTE DE SOLIDARITÉ TERRITORIALE CYBER

- Une piste quand on n'a pas les moyens de tout mutualiser
- **Associer communes, hôpital, SDIS, SOBEGI, industriels, entreprises...**
- Identifier des points de contact
- Partager bonnes pratiques et retours d'expérience
- Connaître les compétences et ressources de chacun
- Créer des habitudes de coopération avant la crise

3 — EXERCICE TERRITORIAL

- Construire un scénario réaliste pour le territoire
- Partir d'une attaque sur un acteur ou une infrastructure
- Observer les effets en chaîne sur le territoire
- Associer **communes, CCLO, Préfecture, SDIS, Gendarmerie, Armées...**
- Tester les circuits d'alerte, d'information et de coordination
- Identifier les dépendances entre acteurs et intégrer les conséquences pour la population

Préparer → coopérer → tester : mieux articuler les moyens existants plutôt que créer une nouvelle structure.

Les dispositifs applicables à la stratégie cybersécurité





Les dispositifs applicables à la stratégie cybersécurité

Étapes de la stratégie	Actions à mener	Dispositifs possibles	Acteurs
Gouvernance	Élaborer une politique de sécurité des systèmes d'information (PSSI)	Inscrire les actions de mutualisation pour atteindre les objectifs fixés (Mutualiser la DSI, le RSSI, etc.)	Communes-membres, communes-membres, syndicats mixtes, prestataires, fournisseurs
	Constituer un comité de pilotage de la stratégie	Mutualiser le poste de référent cybersécurité	Communes-membres, syndicats mixtes, agence technique départementale
	Mettre en place une cellule de gestion de crise	Organiser des temps d'échanges dédiés	Gendarmerie, CSIRT, Région, prestataires
	Réaliser un audit de sécurité ou diagnostic pour évaluer le niveau de sécurité des systèmes d'information	Groupements de commandes	Prestataires certifiés par l'ANSSI





Les dispositifs applicables à la stratégie cybersécurité

Étapes de la stratégie	Actions à mener	Dispositifs possibles	Acteurs
Protection	Coordonner et veiller au respect des actions de la PSSI	Mutualiser le RSSI • Service commun • Mise à disposition d'un agent • Achat auprès d'un prestataire	Communes-membres, syndicats mixtes, agence technique départementale
	Acquérir des prestations de cybersécurité certifiées et mise en place d'outils de sécurité • Hébergement sécurisé des données • Authentification multifacteur • Processus de gestion des comptes individuels et mots de passe pour accéder aux ressources des systèmes d'informations	Groupements de commandes	Prestataires certifiés par l'ANSSI Centrales d'achats
	Migrer vers des outils de la Suite territoriale	Groupements de commandes	Structures de mutualisation partenaires de l'ANCT





Les dispositifs applicables à la stratégie cybersécurité

Étapes de la stratégie	Actions à mener	Exemples de dispositifs possibles	Acteurs
Résilience et Défense	Participer à un exercice de gestion de crise pour savoir comment réagir en cas d'incident et auprès de qui le déclarer	Rempar25 (organisé par le syndicat mixte Manche numérique)	Intercommunalité, ANSSI, CSIRT, 17Cyber, gendarmerie, syndicat mixte
	Mettre en œuvre une stratégie d'entraînement pour assurer la continuité des services en mode numérique dégradé	Rejoindre les initiatives d'entraide d'autres collectivités (exemple : Charte de Solidarité Territoriale Cybersécurité de Nantes métropole)	Prestataires, intercommunalités de plus grande taille, Département, Région



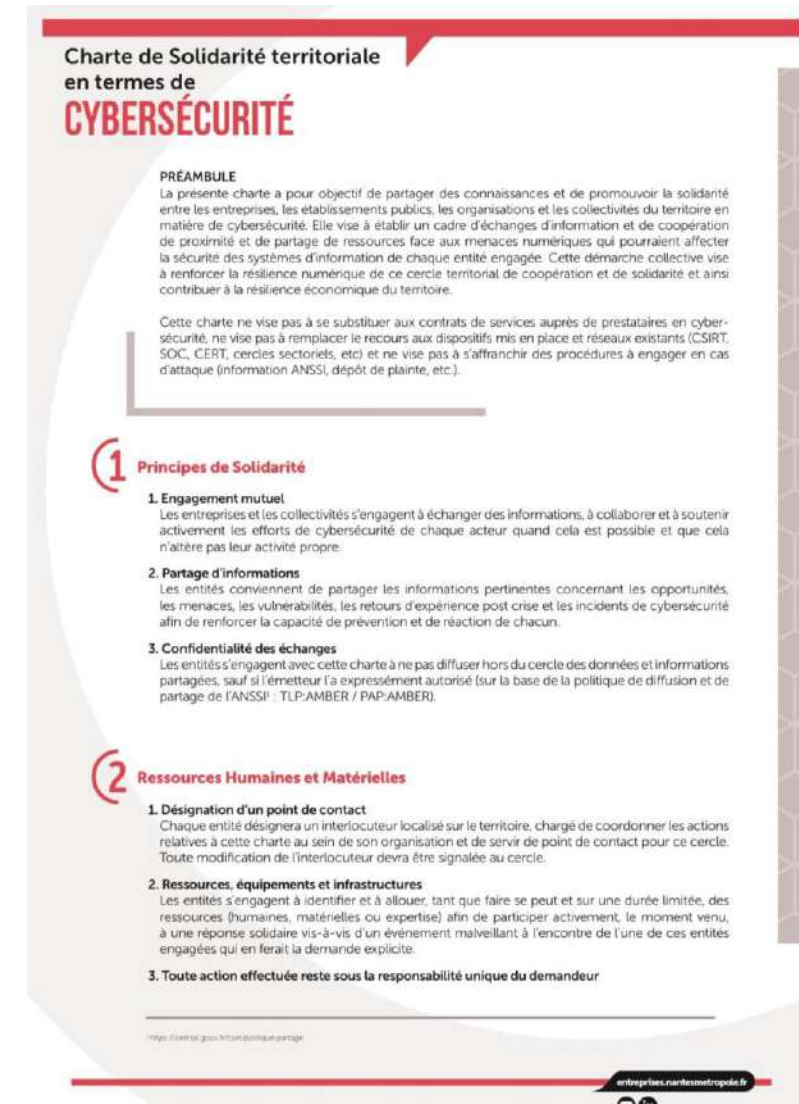
► Charte de Solidarité Territoriale Cybersécurité de Nantes métropole

Objectifs

- **Partager des expériences et promouvoir la solidarité** entre entreprises, établissements publics, organisations et collectivités du territoire
- Mettre en place un cadre sécurisé d'**échanges d'information et de coopération de proximité, de partage de ressources** face aux **menaces numériques**

Cette charte ne vise pas à :

- *se substituer aux contrats de services*
- *remplacer le recours aux dispositifs et réseaux existants (CSIRT, SOC, CERT, cercles sectoriels, etc)*
- *s'affranchir des procédures à engager en cas d'attaque*

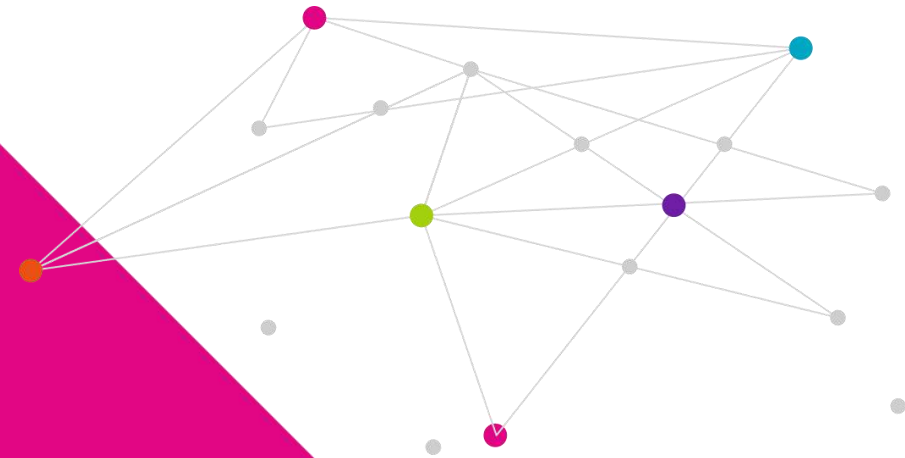


[Lien vers la charte](#)

Retour d'expérience

Cédric Kerebel

- *Responsable du service des systèmes d'information mutualisé, Pays d'Iroise Communauté*



Services Système d'informations Mutualisé

**Présentation et fonctionnement du projet de service
commun**

Pourquoi un service informatique communautaire ?

Répondre à une attente des communes et de l'intercommunalité

Disposer d'une expertise technique

MCO/MCS - Infogérance - Supervision

Cybersécurité - EDR (SOC) - PRA - Sensibilisation - Durcissement des systèmes

Assistance - Dépannage - Proximité des intervenants

Relais prestataires - Migration Liens Telecom - Editeurs - Accompagnement

Transparence budgétaire - Pas de coûts non budgétés - L'ensemble des prestations liées aux prestations de renouvellement, changement des équipements est inclus (hors logiciel et matériel)

Rechercher des économies d'échelle - Marchés / Groupement de commande

Solidarité de territoire en permettant aux petites comme aux plus grandes communes de disposer des services numériques

Hébergement des systèmes d'information

Communes adhérentes 2026



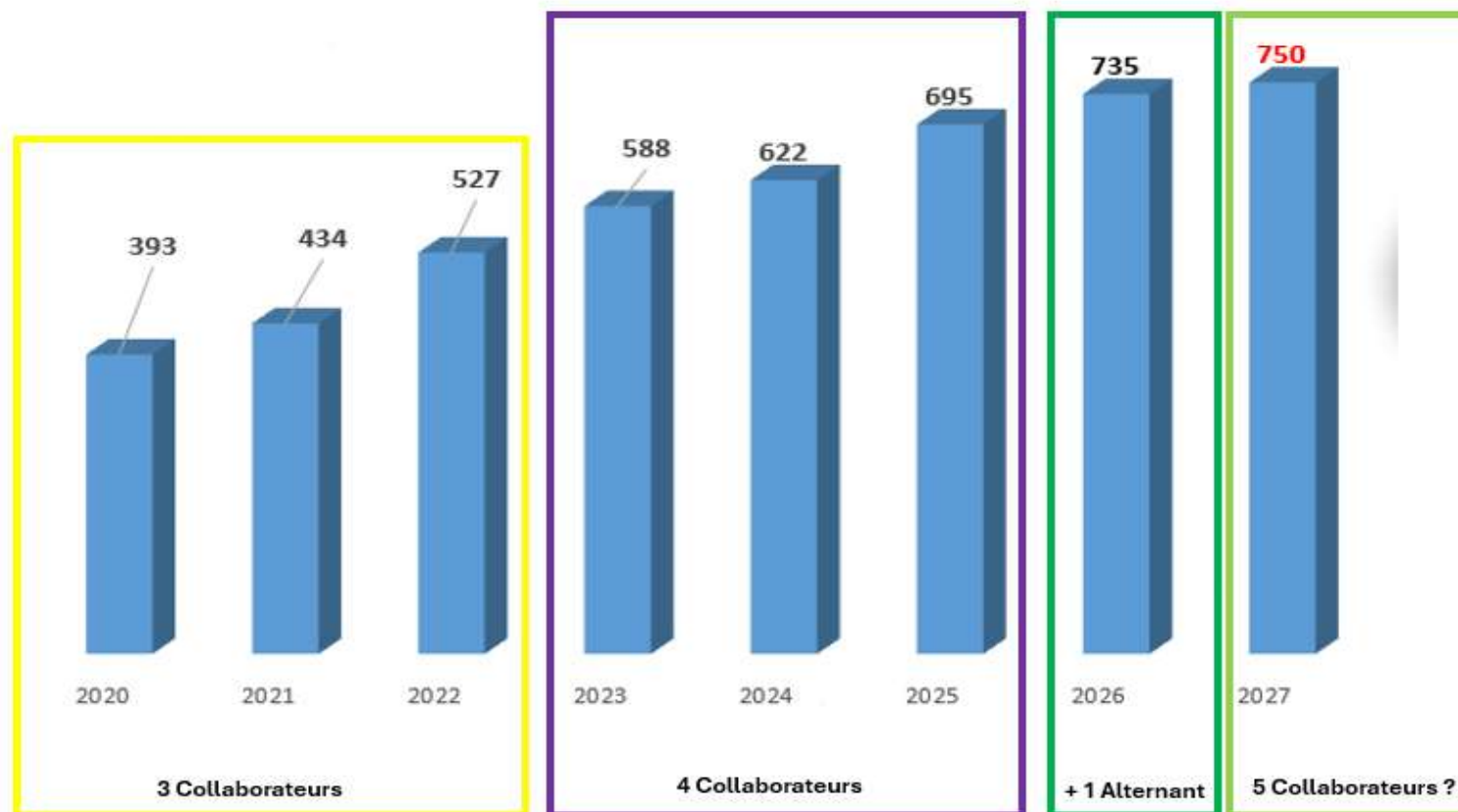
17 Communes adhérentes

Commune partenaire : St Renan



Projection 2027 - Service informatique mutualisé Evolution du parc + Equipe

Evolution du parc 2020-2027





PAYS
D'IROISE
COMMUNAUTÉ
BRO AN HIRWAZH

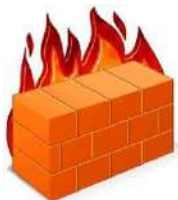
Les domaines d'intervention



BreizhCyber



Syndicat mixte de coopération territoriale



Service Informatique



Projet de mutualisation

Mutualisation n'est pas transfert de compétences

En mutualisation, le pouvoir décisionnel appartient à chaque entité adhérente (achat, abonnement, etc.)

Les achats (matériels/logiciels) sont réalisés par les communes
Via marché mutualisé si existant

Détails des services



- Sécurisation du système d'informations (SI) - Cybersécurité
- Infogérance incluant 4 à 5 passages par an en préventif
- Assistance utilisateurs (télémaintenance/sur site)
- Installation - Renouvellement
- Gestion de projets
- Préparation aux budgets et Plan Pluriannuel d'investissements
- Téléphonie
- Accompagnement des utilisateurs sur le SI - Prévention - Sensibilisation
- Supervision des équipements

Infogérance


 INFOGÉRANCE - CR PRÉVENTIF
Demi-journée préventive

COMMUNES:
 CONTACT CLIENT:
 AUTEUR:
 DATE:
 ARRIVÉE:
 DÉPART:
 NB SERVEURS:

+ Nouveau CR Enregistrer (json) Charger un CR Exporter CSV Exporter PDF Envoyer par mail Gérer le modèle de checklist

SYNTHÈSE DE L'INTERVENTION & COMMENTAIRES GÉNÉRAUX
 Synthèse de l'intervention:
 Commentaires généraux:

Serveurs 16 point(s)

POIDS	ACTION	PRÉVU	RÉAL	COMMENTAIRE / À FAIRE
3	Les pannes curatives non bloquantes Serv - Dépanner	☒	☒	RAS, à planifier...
3	Etat des RAID + Erreurs Disques Serv - Contrôler	☒	☒	RAS, à planifier...
3	Vérifier Contrôle et fonctionnement ZABBIX Serv - Contrôler	☒	☒	RAS, à planifier...
3	Vérifier la remontée des agents Zabbix et ajouts si nécessaire Serv - Contrôler	☒	☒	RAS, à planifier...
3	L'activation du FireWall Serv - Vérifier	☒	☐	RAS, à planifier...
3	Alertes (rouges), observation des événements systèmes Serv - Contrôler	☒	☐	RAS, à planifier...
3	L'activation du logiciel de gestion de l'onduleur Check-list - Vérifier	☒	☐	RAS, à planifier...
3	Vérification minutée de contrôles HYPER-V sur une de production (normal sur central)	☒	☐	RAS, à planifier...

- Définition d'un calendrier annuel de demi journées préventives entre 4 et 5 passages par an
- Contrôle **préventif** des équipements du système d'informations
- Point sur les échéances matérielles (garantie , licences) et les échéances des prestataires
- Validation du niveau de sécurité du système d'informations
- Audit complet du parc informatique / Schéma réseau réalisés au démarrage du partenariat

CCPI Rapports ANSSI

Ce sont des outils fournis par l'ANSSI pour auditer respectivement l'exposition sur Internet et l'Active Directory en profondeur.
Ils ont été utilisés à la CCPI et sont planifiés sur les communes pour l'été 2025.

Exposition Internet

Analyse d'exposition sur Internet / Communauté de communes Pays d'Iroise - CC_Pays_Iroise

Niveau de sécurité



Problème important 0

Point d'attention 0

	Cartographie (pour IVRE)
	Tous les problèmes (CSV)
	Tous les points (CSV)
	JSON

Sécurité Active Directory

Analyse de la forêt AD "domaine.local"

2024-11-09 06:35:00 ?

Niveau de sécurité



Progression dans le niveau

700 / 700

Progression globale

9300 / 9300

Point de durcissement 1

Points d'attention 5

☐ Afficher le rapport complet (tous niveaux)

☒ Voir les points d'information

 Télécharger les données au format JSON

Domaine 1

Utilisateurs 400

Ordinateurs 186

Contrôleurs de domaine 3

GPOs 37

Niveau fonctionnel de la forêt Windows 2016 / 2019 / 2022

Progression depuis le précédent relevé 183 (+ 2%)

Progression sur l'ensemble des relevés précédents 3500 (+ 60%)

Mairie : Sécurité Active Directory PingCastel

Outil gratuit utilisé pour analyser une base annuaire Active Directory et mener des actions en vue de sa sécurisation.

Plan d'action pour la sécurisation du Système d'Information de la mairie de Locmaria.			
Vulnérabilité	Action	Priorité	Cibles
Compte admin déléguable	Cocher la case "le compte est sensible et ne peut pas être délégué".	1	administrateur admin_
Mot de passe compromis	Changer le mot de passe	1	
Mot de passe identique	Changer le mot de passe	1	
Politique de mots de passes	Se conformer aux préconisations de l'ANSSI : 14 caractères avec complexité plus verrouillage de compte en cas d'erreurs	1	MARIE LOCAL
Comptes obsolètes	Supprimer le compte (non connecté depuis plus d'un an). Désactiver les comptes (connecté depuis moins d'un an).	2	adjoint1 (désactivation) a.goux (désactivation) animateurs (désactivation) assistante RH (suppression) c.marquier (désactivation) conseil (désactivation) SCSI (suppression) test (suppression)

Audits et corrections apportées une fois par an par le service sur l'ensemble des annuaires Active Directory des communes.

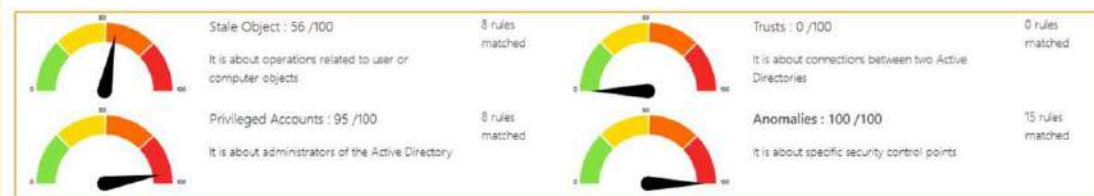
Avant

Après

Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators



Active Directory Indicators

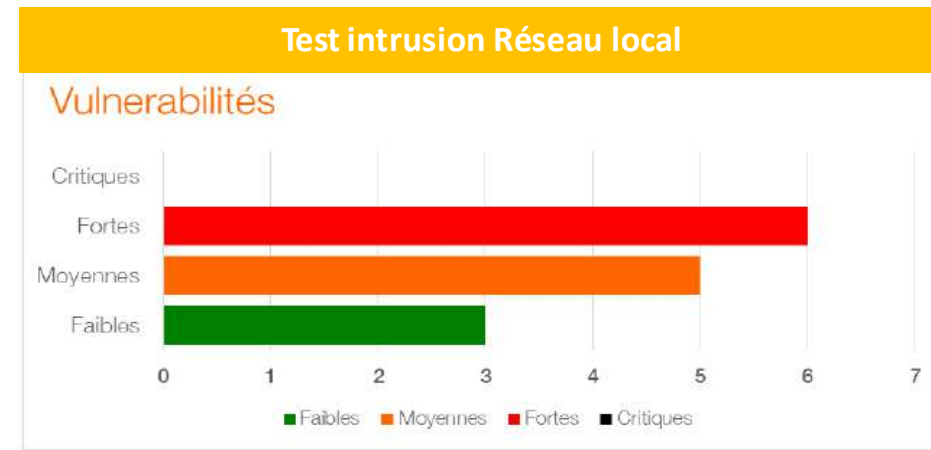
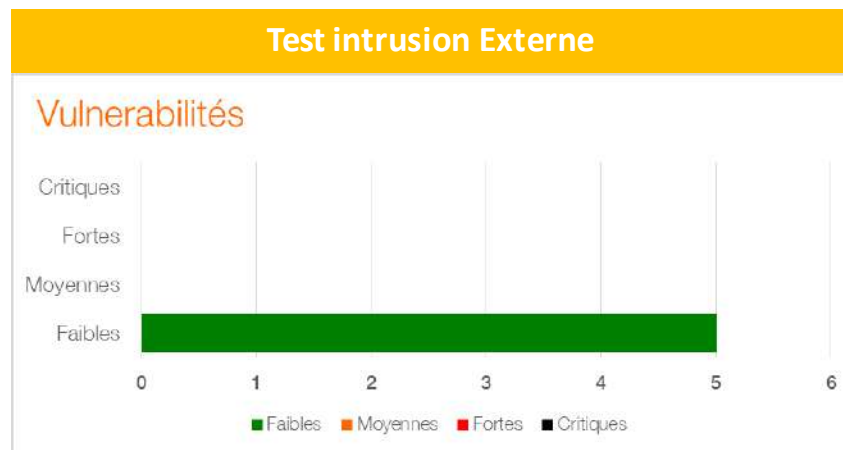
This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators



Cybersécurité CCPI

Point rapport test d'intrusion 2024



**Réaliser un nouveau
test d'intrusion tous les
3 ans**

Le périmètre interne dans son ensemble présente un niveau de sécurité supérieur à la moyenne constatée sur ce type de structure (surtout en considérant qu'il s'agit seulement du second audit sur l'infrastructure).

Audit interne depuis le réseau	
Référence	Titre
TEC.SYS.006	Composants logiciels obsolètes et non supportés
TEC.WIN.019	Signature du protocole SMB non requise
TEC.TOM.003	Interface d'administration Tomcat accessible avec identifiants par défaut
TEC.TII.004	Chemins de contrôle dangereux entre des objets de l'Active Directory
TEC.TII.013	Réutilisation de compte administrateur local sur plusieurs les machines (no LAPS)
TEC.TII.045	SMBv1 non désactivé

Vulnérabilités éditeurs !!

Sécurité antivirus WithSecure

Isolation automatique

WITHSECURE ELEMENTS ENDPOINT DETECTION AND RESPONSE

Automated response alert

Device P [REDACTED].local has been isolated due to suspicious activity (ID 322545483-18083)

WithSecure Elements Endpoint Detection and Response detected the following activity:

Category:	Injection Target
Risk level:	High risk 77
Affected devices:	P [REDACTED].local
Company:	COMMUNE DE [REDACTED]

To view this detection and to remove automated isolation, open WithSecure Elements Endpoint Detection and Response.

[Open portal](#)

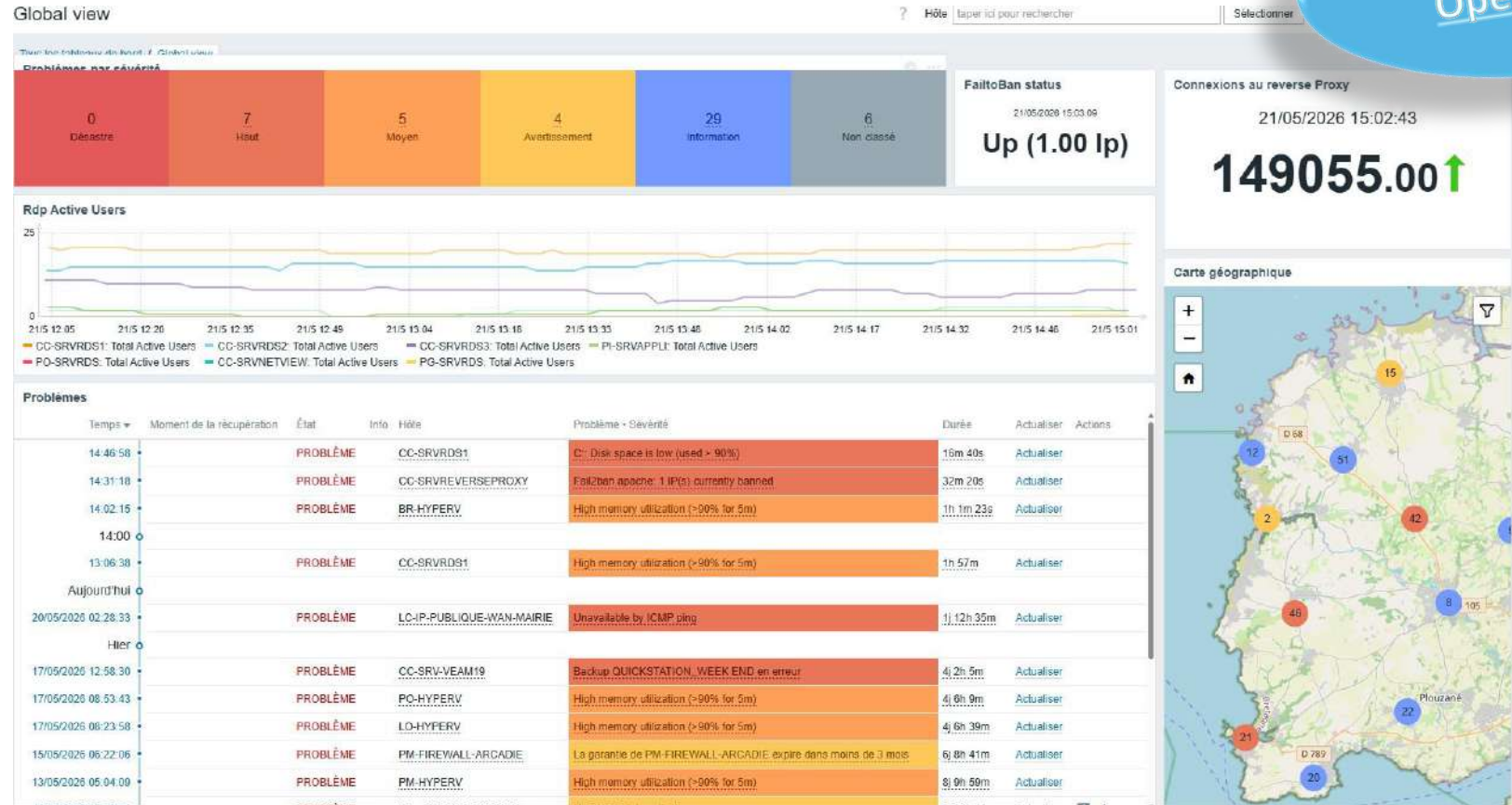
La couche EDR (Endpoint Detection & Response) de l'antivirus WithSecure isole le poste automatiquement en cas de détection d'une alerte Grave/Elevée en journée et Grave/Elevée/Modérée Week end et nuit, pour éviter une compromission ou une propagation vers d'autres cibles.



PAYS
D'IROISE
COMMUNAUTÉ
BRO AN HIRWAZH

Supervision

Solution Zabbix
Open Source !!!



Supervision des équipements sur le territoire
Serveurs - Swicths - Bornes Wifi - Connexion Internet - Sauvegarde - Ressources

Test de Reprise d'Activité Informatique

Test Plan de Reprise d'Activité			
<i>Restauration de vos serveurs à partir d'une sauvegarde externalisée sur un serveur test du SI de la CCPI.</i>			
		Date :	05/02/2025
Noms de serveurs virtuels	SRVAD	SRVAPPLIS	SRVRDS
Lecture du RDX (support de sauvegarde)			
	Ok	Ok	Ok
Import sous Veeam (logiciel de sauvegarde)			
	Ok	Ok	Ok
Restauration du VHDX (disque dur virtuel)			
	Ok	Ok	Ok
Fonctionnement/démarrage du serveur			
	Ok	Ok	Ok
Bilan :			
Test validé - L'ensemble des ressources serveurs est fonctionnel après restauration			

En cas d'indisponibilité du serveur ou du poste principal le service informatique peut restaurer la ou les ressources sur une autre machine à partir d'une K7 de sauvegarde.

Ces tests sont réalisés une fois par an pour chaque commune, un rapport est transmis attestant le bon fonctionnement du test.



Télémaintenance et déplacement sur site
Assistance - actuellement 5 demi journées garanties -
Priorisation des interventions
Déclaration et suivi de l'incident via portail Web + Mails - GLPi
Reporting des historiques et des délais de résolution via le portail WEB



KEREBEL Cédric

Rappel du ticket

Soumettre la demand

Tous	Non lus	Rechercher Boîte aux lett...	Boîte aux lettres actuelle
! @ DE	OBJET	REÇU	TAILLE
Date: Aujourd'hui			
Informatique	[GLPI #0000012] Clôture du ticket Poste redémarre	jeu. 12/09/2019 16...	11 Ko
Informatique	[GLPI #0000012] Nouveau ticket Poste redémarre	jeu. 12/09/2019 16...	10 Ko



Bilan des séances CCPI au 15/05/2026



Date	13-janv	20-janv	22-janv	29-janv	24-mars	28-avr	TOTAL
Nombres d'agents sensibilisés	12	12	9	10	8	8	59

Chaque agent doit suivre une séance de sensibilisation au moins tous les 3 ans

Le nombre d'agents par séance est limité à 12

La sensibilisation s'appuie sur un **quizz interactif** conçu à l'aide d'une application web

Les agents y accèdent via un lien idéalement depuis un smartphone

Facturation du service



Parc	1 serveur	1 Vms	1 PC
Administratif	2	2	1
Scolaire	2		0,75

Exemple avec un budget du service à 300 000 €
Parc de 800 postes pondérés

375 €TTC par poste

► Les prochaines réunions de travail

Mardi 17 novembre, 9h-10h30 : mise à l'épreuve des dispositifs identifiés pour la stratégie IA et data

Jeudi 12 novembre, 9h-12h : Territoir'Prod Cybersécurité

Jeudi 3 décembre, 9h-12h : Territoir'Prod Cybersécurité

[Lien vers le site](#) pour vous inscrire
et accéder aux ressources

► Votre contact



Jules Podczaski

Conseiller numérique

jpodczaski@interconnectes.com

06 59 03 72 70

A network diagram with nodes and connecting lines, featuring a large magenta arrow pointing right.

Merci pour votre participation