

gigalis

CyberLig – Atelier Collectivités



SECALYS

Ateliers menés en novembre et décembre 2026

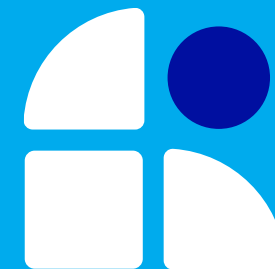
- ✓ 9 ateliers
- ✓ 125 participants
- ✓ 4 phases par atelier → Faire émerger du concret
 - Identifier les irritants clés
 - Définir les leviers
 - Mobiliser l'écosystème
 - Structure la gouvernance
- ✓ 476 idées



1H10



SECALYS

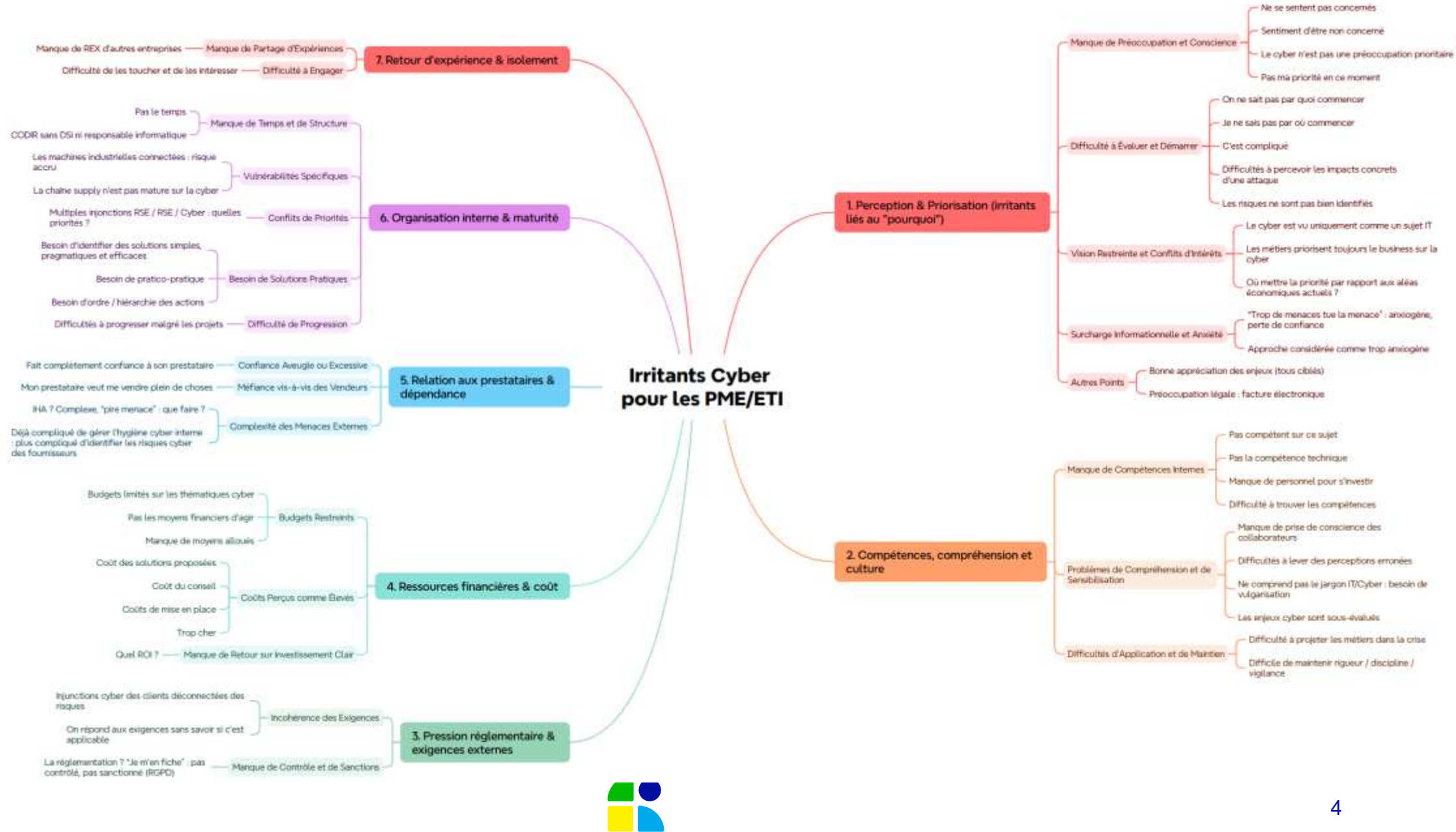


Synthèse
Atelier
ETI/PME/TPE



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber) → 39 retours



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber) → 39 retours

1. Constat général

L'atelier a fait émerger **39 irritants**, illustrant une réalité homogène dans les PME/ETI : la cybersécurité reste un sujet **mal compris, mal priorisé et difficilement actionnable** dans les structures de taille intermédiaire.

Les irritants les plus votés convergent vers quatre constats structurants :

- **Sous-évaluation générale du risque cyber** au niveau des dirigeants comme des équipes.
- Une **vision trop IT** de la cybersécurité, déconnectée de la performance économique et opérationnelle.
- Un **manque de moyens et de compétences**, qui limite toute démarche structurée.
- Un **écosystème jugé complexe**, anxiogène, et souvent inadapté aux réalités des ETI/PME.

2. Top irritants identifiés

1. Les enjeux cyber sont sous-évalués par les entreprises (❤️7)

Risque encore perçu comme lointain, secondaire ou improbable → faible engagement des directions.

2. La cyber est vue uniquement comme un sujet IT (❤️7)

La sécurité n'est pas associée au business, aux risques opérationnels ou à la continuité d'activité.

3. Manque de prise de conscience des collaborateurs (❤️4)

Peu d'appropriation, sentiment de non-concernement, difficulté à responsabiliser les équipes.

4. La cyber "n'apporte pas de valeur" (perception) (❤️4)

Investissements difficiles à justifier face aux priorités business → faible ROI perçu.

5. PME : pas de ressources ni compétences internes en SI / cyber (❤️3)

Absence de DSI, manque de profils qualifiés, dépendance forte aux prestataires.



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber) → 39 retours

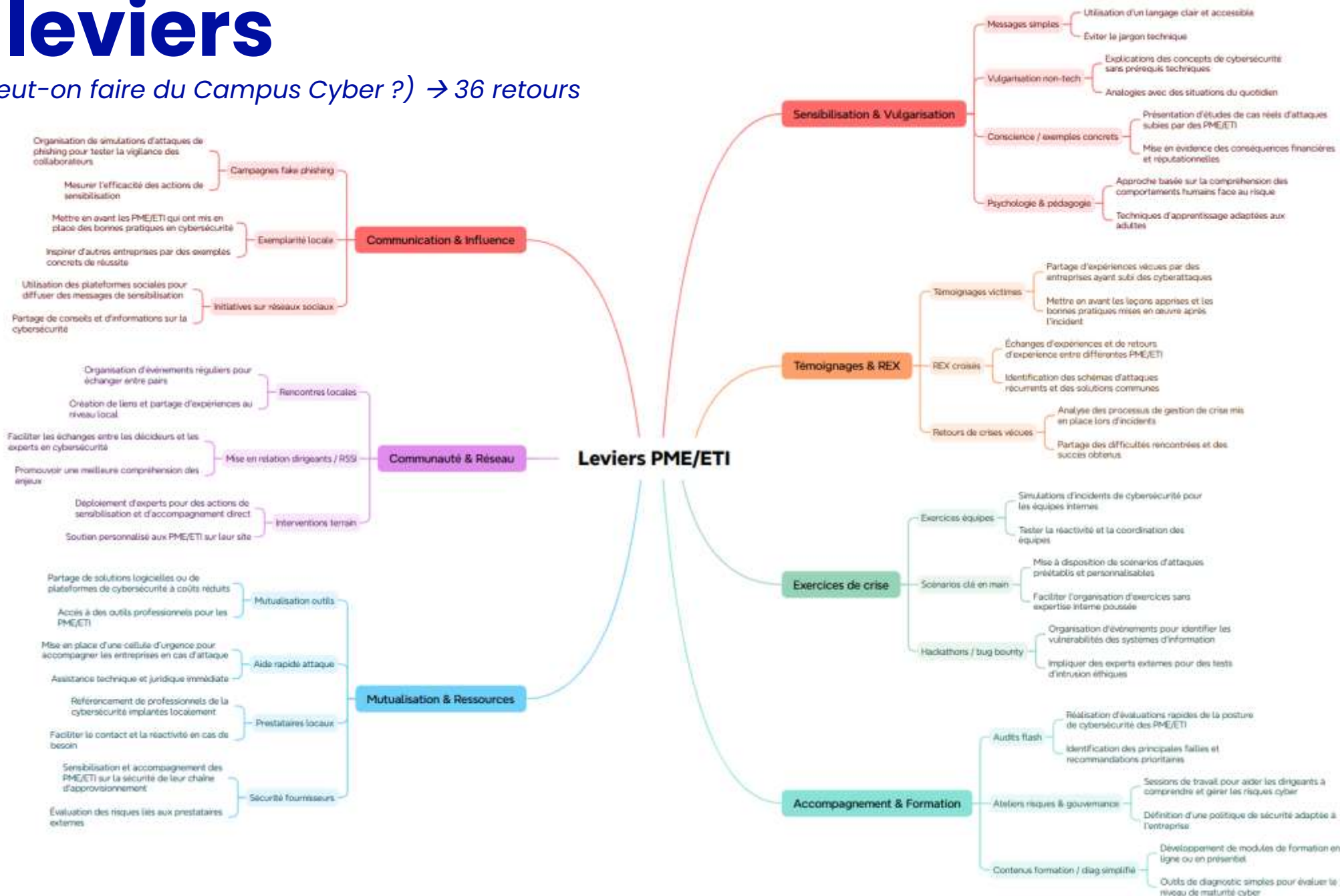
3. Messages à retenir

- ✓ **Les irritants des PME/ETI ne sont pas techniques**, mais relèvent avant tout :
 - d'une **sous-évaluation du risque**,
 - d'un **manque de compréhension**,
 - d'une **incapacité à prioriser**,
 - et d'un **déficit de moyens** (financiers, humains, compétences).
- ✓ **La cyber reste perçue comme un sujet IT**, déconnecté du business, du risque opérationnel et de la continuité d'activité.
- ✓ Les PME expriment surtout un besoin de :
 - **vulgarisation** et d'un langage accessible,
 - **simplicité** et **pragmatisme**,
 - **points d'entrée clairs**,
 - **solutions proportionnées** à leur taille,
 - et d'un **accompagnement non anxiogène**.
- ✓ Le frein principal n'est pas la volonté, mais :
 - **la charge mentale**,
 - **la complexité ressentie**,
 - **l'absence de repères concrets**,
 - et **l'impression d'un effort disproportionné** par rapport à leur réalité quotidienne.
- ✓ **Le territoire a un rôle déterminant** pour créer des approches adaptées, réduire l'isolement et rendre la cyber "faisable" pour les petites structures.



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?) → 36 retours



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?) → 36 retours

1. Constat général

L'atelier fait émerger un volume important d'idées (plus de **45 leviers**), centrés principalement sur :

la **pédagogie** et la **vulgarisation**,

l'**implication active des dirigeants**,

la **mutualisation** des moyens et des retours d'expérience,

la création de **solutions pratiques clés en main**,

la nécessité de **proximité territoriale**,

l'appui sur des **pairs** pour réduire l'isolement et favoriser la confiance.

Les leviers les plus votés insistent fortement sur :

- 👉 **des témoignages concrets**,
- 👉 **des exercices de crise**,
- 👉 **des retours d'expérience structurés**,
- 👉 **des points de rencontre locaux**,
- 👉 **des contenus simples et non techniques**.

Le fil rouge : les PME veulent "voir", "comprendre", "tester", "échanger", et surtout **être accompagnées sans jargon**.

2. Top leviers identifiés

1. Témoignages de victimes (❤️7)

Impacts économiques, psychologiques, réputationnels → très puissant pour la prise de conscience.

2. Trouver de l'aide rapidement en cas d'attaque (❤️5)

Un besoin clair : savoir qui appeler, comment réagir, disposer d'un support immédiat.

3. Mutualiser les moyens (formations, plateformes de phishing...) (❤️3)

Réduire les coûts, accéder à des outils à la hauteur d'une PME.

4. Sensibilisation des équipes non-tech (DAF, RH, métiers...) (❤️3)

Montrer que la cyber dépasse largement le périmètre IT.

5. Audits flash pour les entreprises (❤️2)

Un diagnostic simple, rapide, peu coûteux → lever la première barrière.

6. Ne pas employer un langage technique (❤️2)

Levier central pour réduire la distance avec les dirigeants.

7. Exemples concrets & quantification des pertes financières (❤️2)

Visuels, chiffrés, ancrés dans le réel → très impactant.

8. Ateliers / contenus orientation risques, gouvernance, impact business (❤️2)

Sortir de l'approche purement technique.



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?) → 36 retours

3. Messages à retenir

✓ **Les leviers les plus efficaces sont concrets, pratiques et faciles à s'approprier.**

Les PME veulent des exemples réels, des démonstrations, des exercices, et non des discours théoriques.

✓ **La prise de conscience passe par l'émotion et l'identification.**

Témoignages, incidents vécus, retours de terrain → ce sont les outils les plus puissants.

✓ **La simplicité est un facteur clé de succès.**

Pas de jargon, pas d'approches complexes.
Les dirigeants demandent un langage business, clair, orienté risque.

✓ **Les PME souhaitent de la proximité.**

Des rencontres locales, des relais près de chez eux, un accompagnement humain.

✓ **La mutualisation est un levier majeur.**

Partage des outils, modèles, REX → permet de rendre la cyber financièrement accessible.

4. Opportunités du Campus Cyber

• **Créer un "parcours PME" simple et progressif :**

- diagnostic flash,
- priorisation des actions,
- kits de mise en conformité,
- modèles clés en main.

• **Organiser des témoignages structurés de victimes locales** (dirigeants, DAF, métiers).

Très fort impact pédagogique.

• **Mettre en place un dispositif d'aide immédiate en cas d'incident**

- numéro régional,
- cellule d'appui,
- partenaires certifiés.

• **Mutualiser des plateformes et outils adaptés PME**

- phishing,
- e-learning,
- exercices,
- kits opérationnels.

• **Structurer une communauté de proximité**

- rencontres trimestrielles dans chaque grande ville,
- échanges entre dirigeants et RSSI,
- clubs métiers.

• **Créer des exercices de crise "clé en main"**

- scénarios simples,
- 1h d'animation,
- orientés dirigeants/métiers.

• **Proposer des ateliers sectoriels non techniques**

- risques métier,
- gouvernance,
- assurance,
- impact business.

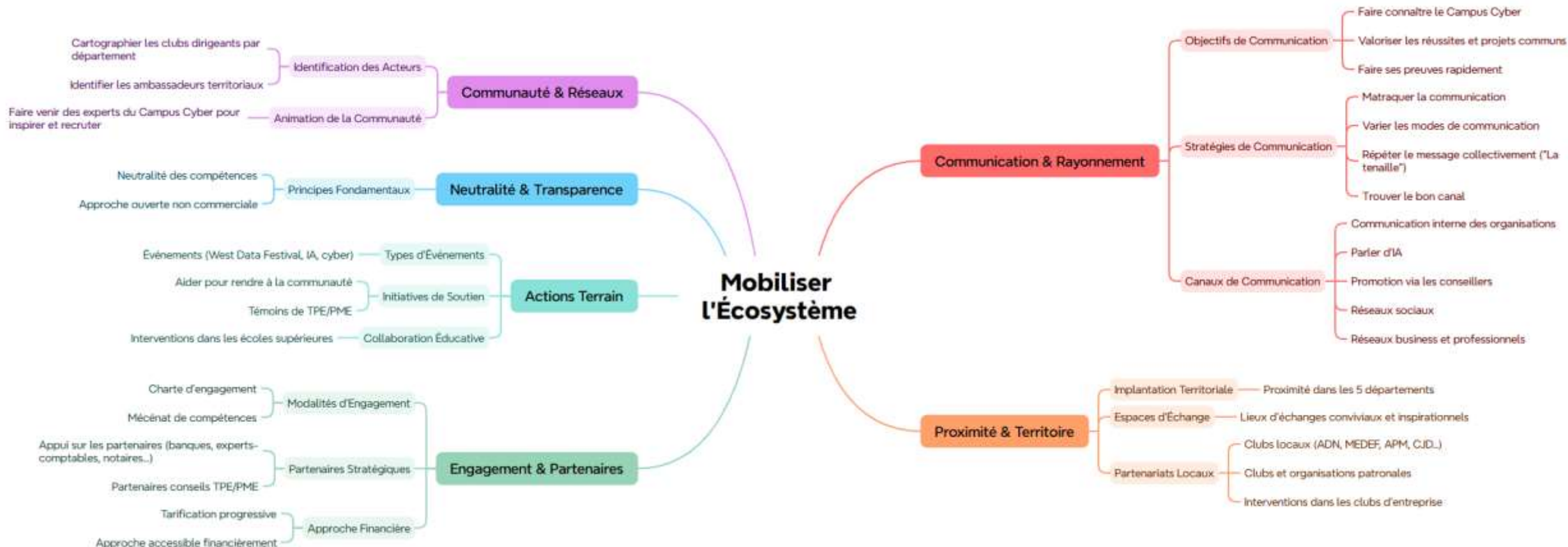
• **Lisibilité de l'écosystème**

- liste régionale des prestataires,
- cartographie des offres,
- recommandations neutres.



Mobiliser l'écosystème

(ou.. Comment l'écosystème peut animer le campus cyber ?)



Mobiliser l'écosystème

(ou.. Comment l'écosystème peut animer le campus cyber ?)

1. Amplifier la communication & la visibilité du Campus

Relayant les messages auprès de leurs membres, clients, réseaux.

Multipliant les supports : newsletters, vidéos, réseaux sociaux, spots, communication interne.

Répétant un message simple et partagé ("la tenaille").

Valoriser les réussites, témoignages, projets communs.

Faire connaître le Campus via conseillers habituels (banques, assurance, experts-comptables...).

Démontrer rapidement l'efficacité du Campus (effet bouche-à-oreille).

Constituer un réseau d'ambassadeurs territoriaux par club ou département.

👉 *Créer un effet de marque territoriale : un Campus identifié, relayé et incarné.*

2. Créer du lien et ancrer le Campus dans le territoire

Organiser des rencontres régulières par département.

Faire du Campus un lieu d'échanges conviviaux et inspirationnels.

S'appuyer sur les clubs locaux (ADN, MEDEF, APM, CJD, ETI PDL...).

Proposer des interventions du Campus dans les clubs d'affaires.

Faciliter la mise en relation des dirigeants, PME, ETI, collectivités, partenaires.

Encourager les entreprises aidées à "rendre à la communauté".

👉 *Faire du Campus le point de convergence de l'écosystème régional.*

3. Participer & co-animer les actions du Campus

Intervenir dans des webinaires, conférences, tables rondes.

Apporter des témoignages concrets (succès, échecs, REX crises).

Mettre à disposition leurs propres bonnes pratiques et outils.

Accueillir ou co-animer des ateliers spécialisés.

Participer à des groupes de travail territoriaux.

Fournir des relais pour les campagnes de sensibilisation.

👉 *Passer d'un Campus "prestataire" à un Campus "co-animé par l'écosystème".*



Mobiliser l'écosystème

(ou.. Comment l'écosystème peut animer le campus cyber ?)

4. Soutenir les acteurs locaux les moins matures

Consacrer du temps à la montée en compétence des petites structures.

Sensibiliser au nom de l'écosystème (approche non commerciale).

Mettre à disposition des ressources mutualisées.

Faire intervenir des conseillers TPE/PME.

Envisager du mécénat de compétences.

Mobiliser des forces publiques (ex : Gendarmerie pour sensibilisation & enquêtes).

👉 *Créer une dynamique de solidarité territoriale où les plus avancés tirent les autres.*

5. Proposer des approches adaptées et accessibles

Les acteurs peuvent contribuer en :

Proposant une tarification proportionnée au niveau de maturité.

Favorisant des formats courts, pratiques, répliquables.

Rendant les contenus et messages accessibles financièrement.

S'assurant de la neutralité des compétences et de l'absence de biais commerciaux.

👉 Rendre la cybersécurité "faisable" pour tous, sans barrière d'entrée.

6. Ouvrir les bons canaux de communication

L'écosystème peut :

Faciliter l'accès au bon public via réseaux business, clubs dirigeants, réseaux sociaux.

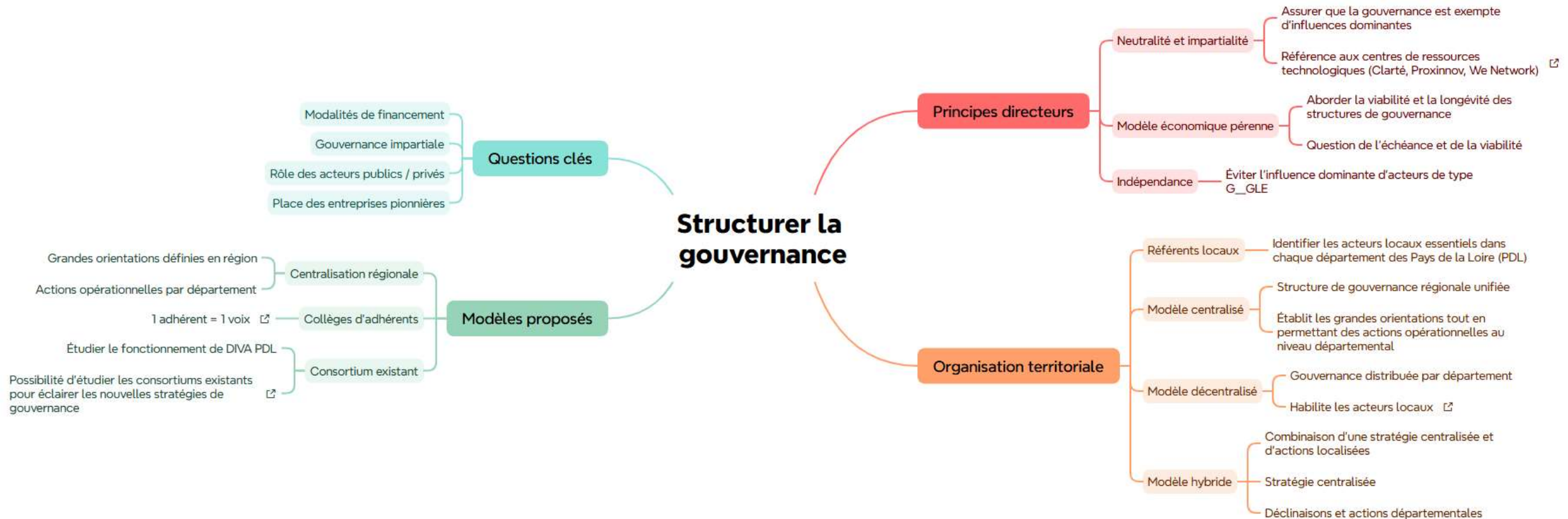
Trouver les bons relais pour toucher les TPE/PME.

Aider à identifier les témoins locaux, influenceurs, entrepreneurs inspirants.

👉 Aller là où les dirigeants se trouvent déjà.



Structurer la Gouvernance

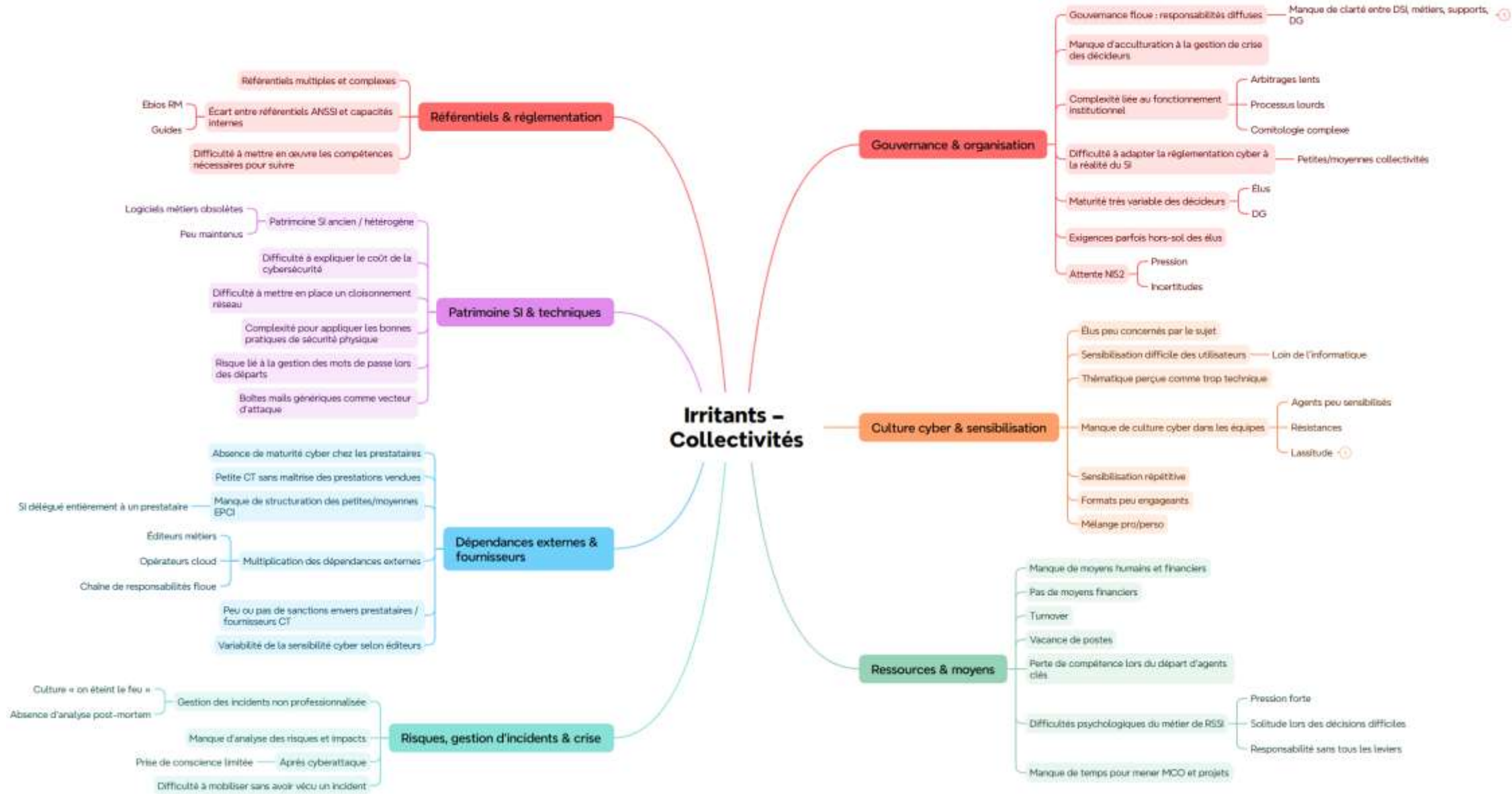


Synthèse
Ateliers
Collectivités



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber) → 39 retours



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber) → 39 retours

1. Constat général

L'atelier a fait émerger **40 irritants**, révélant une réalité très homogène dans les collectivités : la cybersécurité reste **un sujet mal compris, mal porté politiquement et difficilement opérationnalisable**, en particulier dans les structures petites et moyennes.

Les irritants les plus votés mettent en lumière quatre constats structurants :

• Un déficit d'acculturation stratégique au niveau des décideurs

Les élus et directions n'ont pas les réflexes de gestion de crise, peinent à mesurer les risques et ne priorisent pas la cybersécurité.

• Une gouvernance floue et des responsabilités diffuses

DSI, métiers, prestataires, DG... aucun rôle n'est clairement défini → lenteurs, arbitrages complexes, actions hétérogènes.

• Un manque généralisé de moyens humains et financiers

Ressources limitées, difficulté à recruter, dépendance forte aux prestataires, maturité inégale.

• Un écosystème perçu comme complexe et anxiogène

Multipliation des référentiels, difficultés d'alignement, variabilité forte des exigences, vision hétérogène du risque.

2. Top irritants identifiés

1. Gouvernance floue et responsabilités diffuses (❤️8)

Personne ne sait clairement qui décide, qui arbitre ou qui est responsable → fragmentation, lenteurs et inefficience.

2. Manque d'acculturation à la gestion de crise des décideurs (❤️8)

Les élus et directions ne maîtrisent pas les mécanismes de crise, ne perçoivent pas les signaux faibles et sous-estiment les impacts.

3. Élus peu concernés par le sujet (❤️6)

La cybersécurité est souvent perçue comme secondaire → faible engagement politique et arbitrages défavorables.

4. Manque de moyens humains et financiers (❤️6)

Peu de ressources internes, profils difficiles à recruter, surcharge opérationnelle → frein majeur à toute montée en maturité.

5. L'attente NIS2... (❤️6)

Flou, pression réglementaire, sentiment d'injonction contradictoire → inquiétude accrue et difficulté de se projeter.



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber) → 39 retours

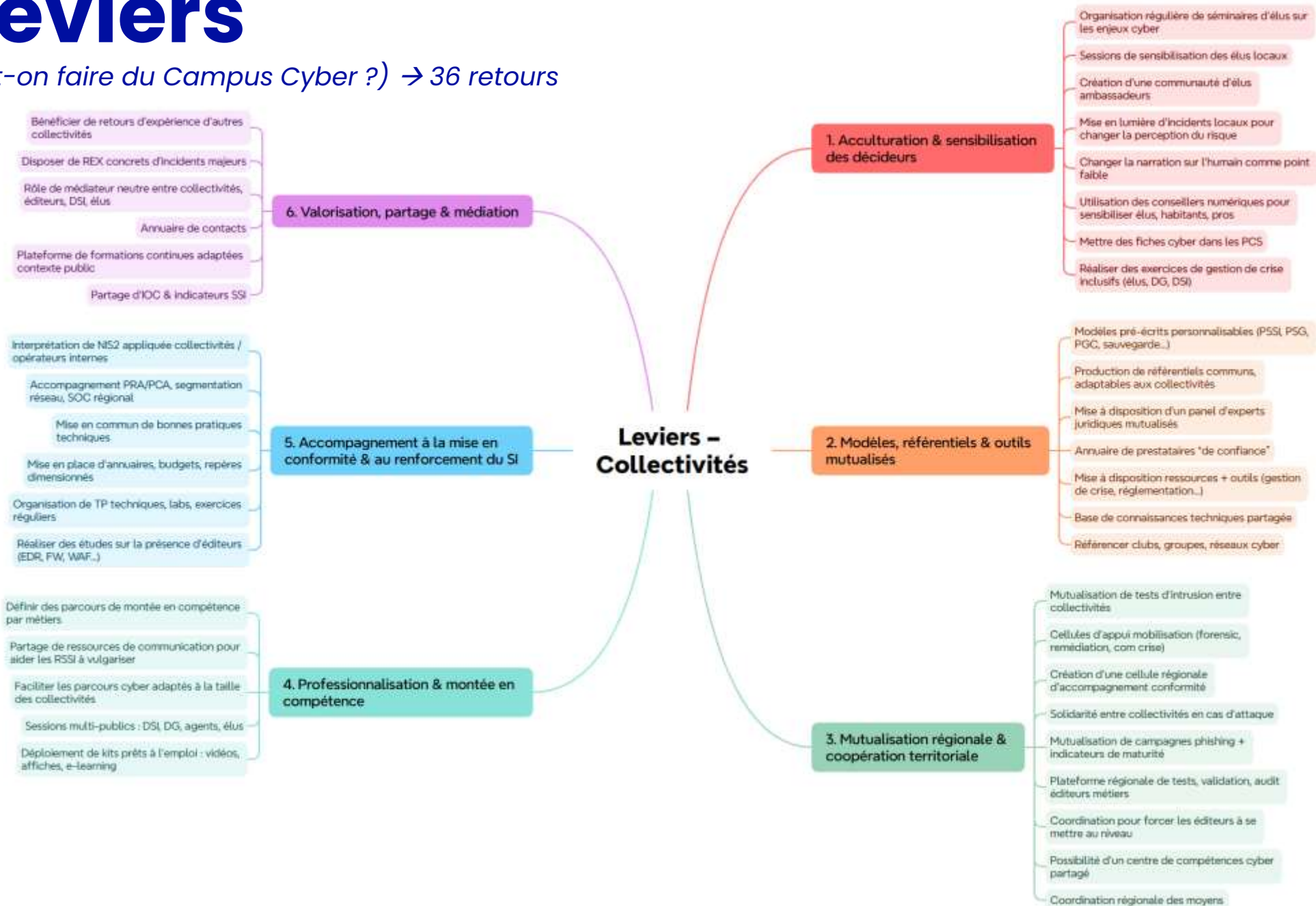
3. Messages à retenir

- ✓ Les irritants des collectivités **ne sont pas techniques** : ils relèvent surtout
 - d'un déficit d'acculturation des décideurs,
 - d'une gouvernance inadaptée,
 - d'une sous-évaluation du risque,
 - et d'un manque de moyens (humains, financiers, compétences).
- ✓ La cybersécurité reste **perçue comme un sujet IT**, loin des enjeux de continuité d'activité, de services aux citoyens ou de résilience territoriale.
- ✓ Les collectivités expriment un besoin fort de :
 - **vulgarisation**, pédagogie et langage accessible,
 - **gouvernance claire** : qui décide de quoi ?
 - **solutions proportionnées** à leur taille et à leurs contraintes,
 - **accompagnement non anxiogène**, réaliste et territorial.
- ✓ Le frein principal n'est pas la mauvaise volonté, mais :
 - la **charge mentale** des équipes,
 - la **complexité ressentie** de la cyber,
 - l'absence de repères simples et actionnables,
 - un **effort perçu comme disproportionné** par rapport aux capacités internes.
- ✓ Le territoire joue un rôle déterminant pour **structurer l'entraide**, réduire l'isolement et rendre la cyber **réaliste, faisable et utile** pour les collectivités.



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?) → 36 retours



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?) → 36 retours

1. Constat général

L'atelier a fait émerger **un volume important de leviers (près de 60)**, révélant une volonté forte des collectivités d'avancer, malgré des contraintes structurelles fortes.

Les idées convergent autour de grands besoins :

• Renforcer l'acculturation des élus et décideurs

La prise de conscience reste insuffisante ; les collectivités demandent des formats pédagogiques simples, concrets et réguliers.

• Disposer de modèles, outils et référentiels "clés en main"

Les petites collectivités n'ont ni le temps ni les compétences pour produire seules PSSI, PSG, PGC, PRA/PCA, référentiels techniques... Elles veulent du prêt-à-l'emploi.

• Mutualiser les moyens à l'échelle territoriale

Experts, audits, tests d'intrusion, campagnes de phishing, exercices de crise, kits de sensibilisation, REX... La mutualisation est perçue comme indispensable.

• Créer une dynamique de proximité

Cellules régionales, communautés d'élus, conseillers numériques, viviers d'experts : la proximité territoriale est vue comme le levier le plus concret pour réduire l'isolement.

• Favoriser la coopération inter-collectivités

La solidarité, le partage d'indicateurs, la mutualisation d'outils et l'homogénéisation des pratiques sont vus comme des accélérateurs de maturité.

Le fil rouge est clair :

👉 **Les collectivités veulent des solutions simples, mutualisées, accessibles, non anxiogènes, et un accompagnement pérenne.**

2. Top leviers identifiés

1. Organisation régulière de séminaires d'élus sur les enjeux cyber (❤️7)

Fort impact : pédagogie, acculturation, engagement politique → levier déterminant.

2. Modèles pré-écrits clés en main (PSSI, PSSIE, PSG, PGC, sauvegarde...) (❤️7)

Répond directement au manque de temps et de ressources internes → adoption immédiate.

3. Mutualisation de campagnes de phishing + d'indicateurs de maturité (❤️7)

Permet de mesurer, comparer, piloter la maturité et optimiser les efforts.

4. Sessions de sensibilisation d'élus locaux (❤️6)

Complément essentiel : formats courts, concrets, orientés risque et continuité d'activité.

5. Réalisation d'exercices de gestion de crise inclusifs (élus, DG, DSI...) (❤️6)

Acculturation rapide, prise de conscience forte, renforcement des chaînes décisionnelles.



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?) → 36 retours

3. Messages à retenir

✓ **Les leviers les plus efficaces sont ceux qui impliquent les élus.**

Acculturation, sensibilisation, exercices... Dès que les décideurs s'engagent, la dynamique change.

✓ **Le "clé en main" est indispensable.**

Modèles, référentiels, kits opérationnels, outils mutualisés → les collectivités n'ont pas la bande passante pour produire elles-mêmes.

✓ **La mutualisation est un levier central.**

Tests d'intrusion, experts, campagnes, formations, REX : le territoire devient un multiplicateur de maturité.

✓ **La proximité crée la confiance.**

Communautés locales, conseillers numériques, viviers régionaux → réduction de l'isolement et meilleure appropriation.

✓ **La simplicité prime.**

Pas de jargon, des supports pédagogiques accessibles, des exemples concrets, des démonstrations plutôt que des discours.

✓ **Le changement s'opère par l'expérience.**

Exercices de crise, incidents locaux, retours d'expérience : ce sont les outils pédagogiques les plus puissants.

4. Opportunités du Campus Cyber

Créer une offre "Collectivités" structurée et progressive

- parcours de montée en maturité adapté aux tailles des collectivités,
- modèles pré-remplis (PSSI, PGC, PRA/PCA),
- kits opérationnels (communication, sensibilisation, exercices),
- indicateurs de maturité mutualisés.

Construire un réseau territorial d'acculturation des élus

- séminaires réguliers d'élus,
- communauté d'élus ambassadeurs,
- conseillers numériques "référents cyber" du territoire,
- REX locaux pour ancrer la prise de conscience.

Mettre en place une plateforme régionale de mutualisation

- tests, audits, certification régionale des solutions éditeurs,
- campagnes de phishing mutualisées,
- partage d'IOC, guides, référentiels compatibles collectivités,
- viviers d'experts mobilisables.

Renforcer la préparation opérationnelle

- exercices de crise inclusifs (élus, DG, DSI, métiers),
- TP techniques (segmentation réseau, PRA/PCA, durcissement),
- ateliers risques / gouvernance / impact business adaptés au public non technique.

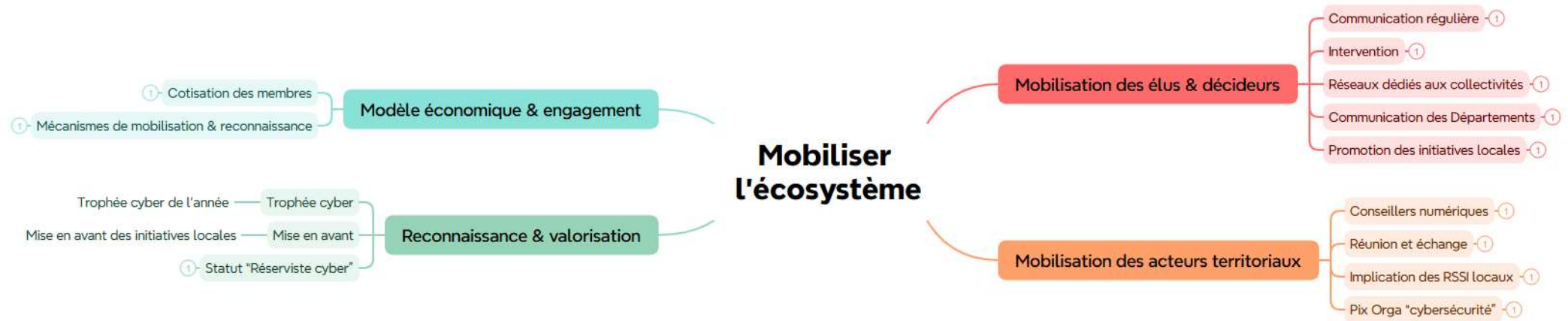
Structurer une communauté de proximité

- groupes locaux de RSSI, DSI, élus,
- rencontres trimestrielles,
- échanges de bonnes pratiques et retours d'expérience,
- entraide en cas d'incident (solidarité territoriale).



Mobiliser l'écosystème

(ou.. Comment l'écosystème peut animer le campus cyber ?)



Mobiliser l'écosystème

(ou.. Comment l'écosystème peut animer le campus cyber ?)

1. Amplifier la mobilisation des élus & décideurs

(C'est clairement le cœur de ton atelier)

L'écosystème doit jouer un rôle de **relai politique** pour faire progresser la maturité cyber.

Les leviers identifiés :

- Communiquer régulièrement auprès des élus sur les actions du Campus
- Intervenir dans les réunions d'élus
- Mobiliser les réseaux institutionnels (DGS, AMF, Départements...)
- Mobiliser les Départements pour la communication
- Créer une dynamique visible : initiatives locales valorisées, trophée cyber annuel
- Développer un "Pix Orga cybersécurité" mutualisé pour agents & élus

👉 **Objectif : installer durablement la cyber comme sujet de gouvernance locale.**

2. Activer les relais territoriaux & partenaires locaux

Les collectivités veulent une mobilisation **proche du terrain**, structurée et coordonnée.

Leviers identifiés :

- Mobiliser les conseillers numériques à proximité
- Impliquer les RSSI locaux (rôle à définir)
- Réunir et échanger avec les prestataires des collectivités
- Rendre visibles les initiatives locales
- S'appuyer sur les cadres territoriaux (Départements / Région) comme relais naturels

👉 **Objectif : créer un écosystème local qui s'auto-entretient et qui diffuse les bonnes pratiques.**

3. Favoriser l'engagement & la contribution des collectivités

L'écosystème peut stimuler la participation active des collectivités à travers différents mécanismes.

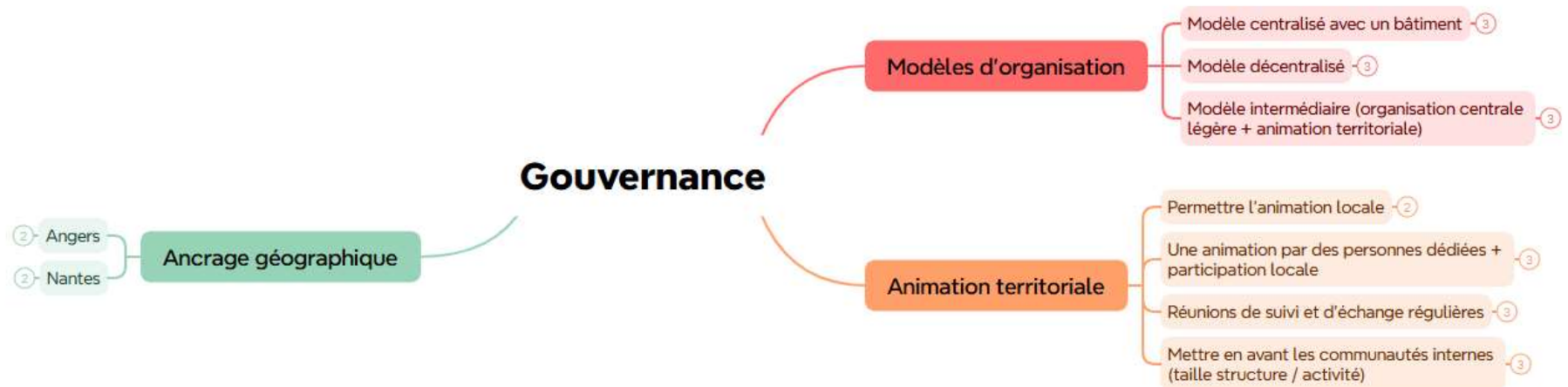
Leviers identifiés :

- Cotisation proportionnelle à la taille pour accéder aux services
- Possibilité d'un statut "réserviste cyber"
- Organisation d'un trophée cyber annuel
- Mise en valeur des initiatives locales pour encourager l'engagement
- Participation aux temps d'échange régionaux (réunions, ateliers, événements)

👉 **Objectif : transformer les collectivités en co-acteurs de la dynamique territoriale.**



Structurer la Gouvernance



Synthèse Ateliers RSSI



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber) → 39 retours



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber) → 39 retours

1. Constat général

L'atelier a fait émerger **39 irritants** exprimés par les RSSI du territoire, couvrant l'ensemble du spectre : gouvernance, ressources, écosystème, moyens et maturité organisationnelle.

Les irritants les plus votés sont liés à la **gouvernance**, au **positionnement du RSSI**, et au **manque de réseau local**.

2. Top irritants identifiés

1. Sensibilisation des dirigeants (❤️11)

Difficulté majeure à obtenir une compréhension et un engagement réel du top management sur les enjeux cyber.

2. Positionnement hiérarchique insuffisant (❤️8)

RSSI placé sous des non-spécialistes ou en dehors des instances de décision (CoDir).

3. Confusion des acteurs régionaux & manque de lisibilité (❤️8)

Méconnaissance des rôles ANSSI, ADN, CCI, UIMM... → incohérence perçue.

4. Difficulté à réseauter localement (❤️8)

Les RSSI expriment un besoin clair de communauté de pairs.

5. RSSI sous la DSI avec budgets/priorités non maîtrisés (❤️5)

Perte d'indépendance, arbitrages techniques subis plutôt que pilotés.



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber) → 39 retours

3. Messages à retenir

✓ **La cybersécurité n'est pas entravée par des enjeux techniques, mais par des enjeux humains, organisationnels et territoriaux.**

✓ **Les RSSI demandent avant tout :**

une meilleure **reconnaissance** du rôle,

un meilleur **positionnement**,

une **communauté locale** forte et structurée,

des **moyens adaptés**,

et une montée en maturité **globale**, pas uniquement technique.

✓ **Le territoire a un rôle essentiel à jouer pour réduire l'isolement, mutualiser les pratiques et clarifier l'écosystème.**

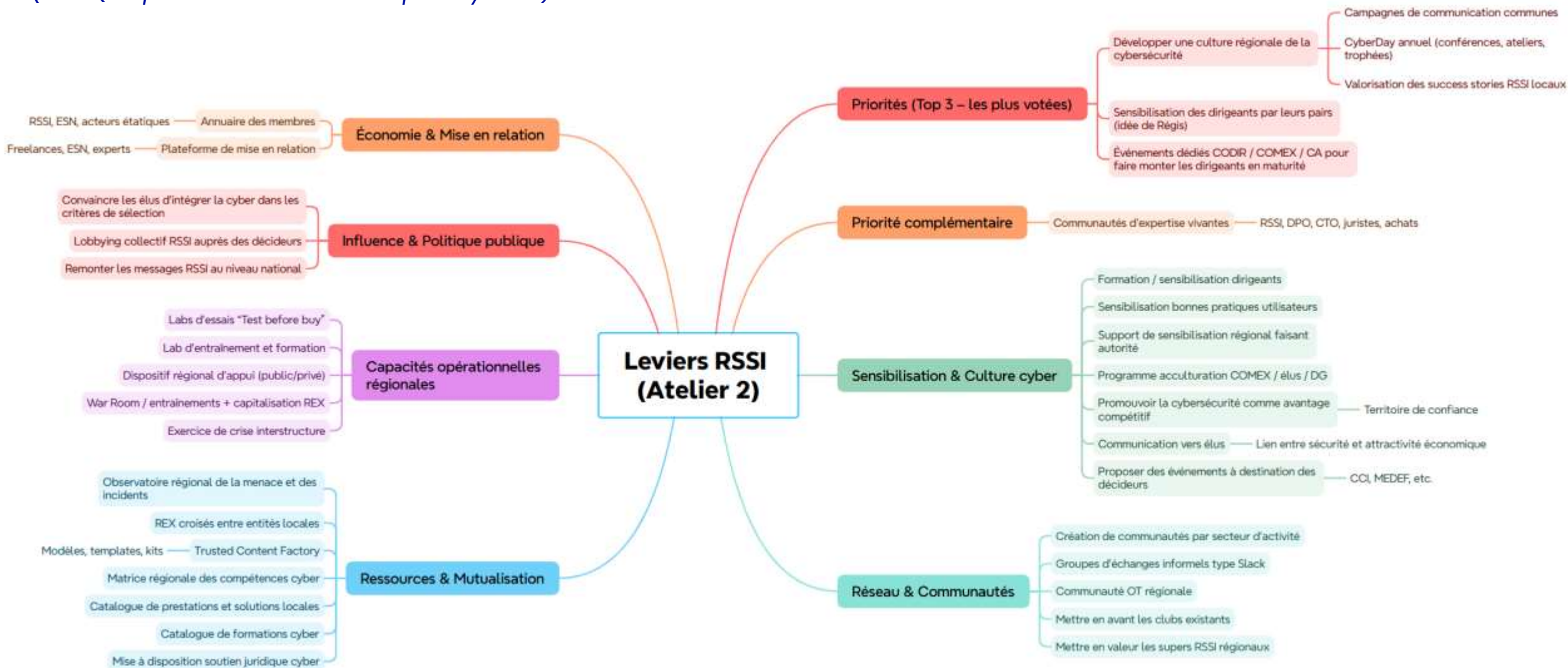
4. Opportunités du Campus Cyber

- Structurer une communauté RSSI territoriale (rencontres régulières, canal dédié).
- Clarifier les rôles des acteurs publics et para-publics.
- Proposer un parcours dirigeants dédié (sensibilisation + obligations réglementaires).
- Mutualiser les REX, exercices, kits métiers, bonnes pratiques locales.
- Favoriser des ressources locales en gestion de crise et en conformité.



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?) → 36 retours



Les leviers → Déclinaison des 3 meilleures idées

(ou.. Que peut-on faire du Campus Cyber ?) → 36 retours

Leviers prioritaires

1. Culture cyber régionale

Créer une identité cyber territoriale qui fédère, rend visible, donne envie, et donne du poids aux initiatives locales.

2. Sensibilisation des dirigeants par leurs pairs

Arrêter de sensibiliser par la technique, parler le langage dirigeant, et faire porter les messages par des pairs, pas par des experts.

3. Communautés d'expertise vivantes

Rompre l'isolement du RSSI et créer un espace où l'expertise se nourrit, se partage et se consolide au quotidien.

Déclinaisons opérationnelles proposées

Baromètre / Observatoire / Cyber Tour / Communauté OT / Newsletter / Communication claire

Acculturation COMEX/DG, influence politique, REX anonymisés, cercle ambassadeurs

Clubs RSSI, communautés sectorielles, rencontres régulières, partages de REX



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?) → 36 retours

1. Constat général

Les leviers proposés montrent une dynamique claire : **les RSSI souhaitent un Campus Cyber qui structure, connecte, outille et influence.**

Plusieurs tendances fortes émergent :

- **Une volonté de changer la culture des dirigeants**

Les 3 leviers les plus votés concernent directement la sensibilisation et la montée en maturité des COMEX/CODIR.

- **Un besoin de communautés vivantes (pairs, juristes, CTO, achats...)**

Les RSSI veulent des espaces de partage structurés, récurrents, multi-expertises.

- **Une demande claire de ressources mutualisées**

Observatoire, contenus prêts à l'emploi, matrice compétences, catalogues locaux.

- **Une attente de capacités opérationnelles partagées**

Labs, War Room, exercices régionaux.

- **Une ambition de positionner le territoire comme exemplaire**

Image, attractivité, communication, lobbying collectif.

2. Top irritants identifiés

- Culture cyber territoriale – communication + CyberDay + success stories (❤️9)
- Sensibilisation des dirigeants par leurs pairs (❤️9)
- Événements COMEX/CA pour montée en maturité (❤️8)
- Communautés d'expertise vivantes (❤️8)
- Annuaire des acteurs cyber du territoire (❤️5)
- Observatoire régional de la menace (❤️3)
- Plateforme mise en relation experts / ESN / freelances (❤️3)
- War Room + REX régionaux (❤️3)



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?) → 36 retours

3. Messages à retenir

Les leviers prioritaires expriment la volonté d'un territoire qui veut se doter d'un véritable écosystème cyber : visible, fédérateur, utile et orienté dirigeants.

Les RSSI demandent des actions structurantes : monter les dirigeants en maturité, créer des communautés vivantes, partager des ressources concrètes et renforcer les capacités opérationnelles locales.

4. Opportunités du Campus Cyber

A – Renforcer la culture cyber territoriale

- Campagnes régionales coordonnées
- CyberDay annuel
- Visibilité médiatique des RSSI locaux

B – Structurer des communautés multi-expertises

- RSSI pairs, CTO, DPO, juristes, achats
- Clubs sectoriels
- Canaux d'échanges (Slack/Discord)

C – Produire des ressources mutualisées

- Observatoire régional
- Kits prêts à l'emploi (clauses, modèles, politiques)
- Matrice de compétences
- Catalogue de formations et prestataires locaux

D – Développer des capacités opérationnelles communes

- Labs techniques partagés
- War Room territoriale
- Exercices inter-structures

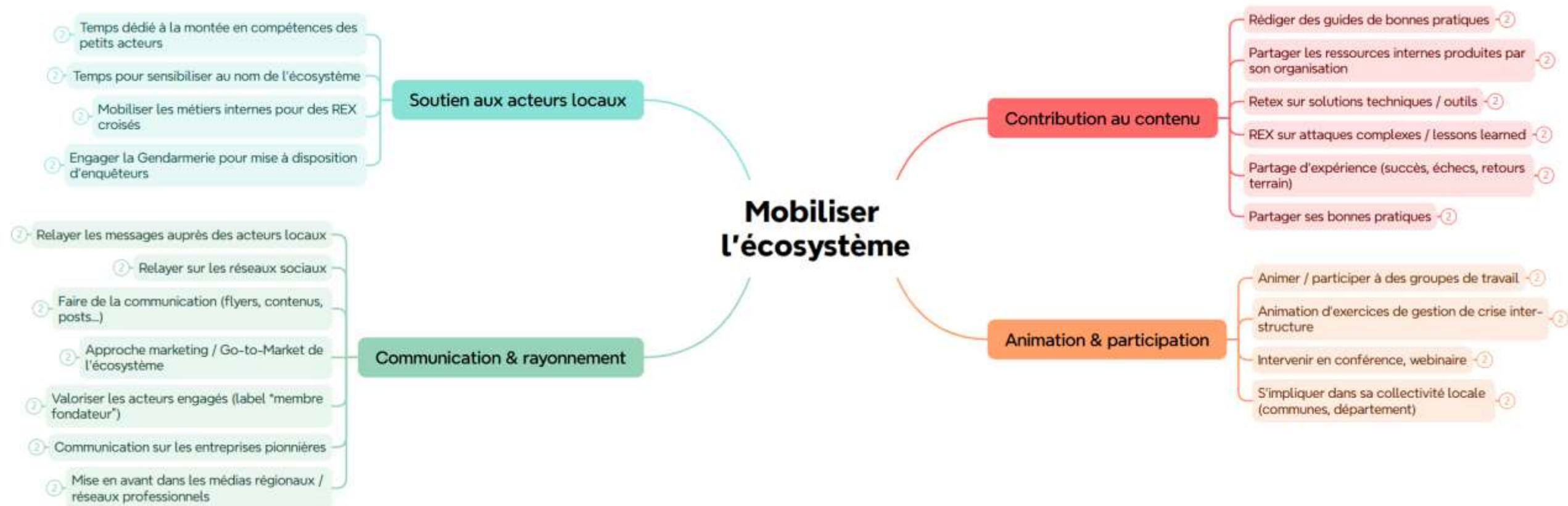
E – Porter la voix cyber du territoire

- Événements COMEX / CA
- Lobbying collectif
- Messages consolidés vers le national



Mobiliser l'écosystème

(ou.. Comment l'écosystème peut animer le campus cyber ?)



Mobiliser l'écosystème

(ou.. Comment l'écosystème peut animer le campus cyber ?)

1. Produire et partager du contenu utile

Les acteurs peuvent contribuer en apportant :

REX sur attaques complexes et retours terrain

Partages d'expérience (réussites / échecs)

Retex techniques sur outils / solutions

Ressources internes réutilisables (docs, pratiques)

Guides de bonnes pratiques

Partage de leurs propres bonnes pratiques

👉 *Enrichir le Campus par une production collective de savoirs opérationnels.*

2. Participer & animer les activités du Campus

L'écosystème est prêt à :

Animer ou co-animer des groupes de travail

Participer aux GT existants

Animer des exercices de crise inter-structure

Intervenir en conférences, webinaires

Mobiliser les métiers internes pour des REX croisés

👉 *Passer d'un Campus consommé à un Campus co-animé.*

3. Relayer et amplifier la communication du Campus

Les acteurs peuvent :

Relayer les messages auprès des acteurs locaux

Relayer les communications sur les réseaux sociaux

Produire des contenus (flyers, posts...)

Valoriser les entreprises pionnières

Faire rayonner les initiatives dans les médias et réseaux pro

Porter un label « Membre fondateur du Campus Cyber »

👉 *Faire du Campus un signal territorial fort.*

4. Soutenir les acteurs locaux moins matures

L'écosystème peut aussi :

Dédié du temps à la montée en compétences des petits acteurs

Sensibiliser au nom de l'écosystème

S'impliquer dans sa collectivité locale

Engager la Gendarmerie (mise à disposition d'enquêteurs)

👉 *Créer une dynamique de solidarité territoriale.*



Structurer la Gouvernance

Gouvernance du Campus Cyber

Principes fondamentaux

- Unité — Cohésion et alignement des objectifs.
- Partage / entraide — Collaboration et soutien mutuel entre les acteurs.
- Représentation des territoires — Assurer une présence équitable des différentes régions.
- Transparence — Clarté et ouverture dans les décisions et les actions.
- Neutralité — Impartialité et absence de parti pris.
- Pas de conflit d'intérêts — Éviter toute situation où les intérêts personnels pourraient influencer les décisions.
- Pas d'instance de promotion des fournisseurs IT / Cyber — Ne pas favoriser des entreprises spécifiques.
- Pas de politique / pas d'ego — Privilégier la solidarité et la bienveillance.

Modèles de gouvernance proposés

- Modèle centralisé
 - Une tête forte qui impulse, produit et pilote toutes les activités.
 - Le Campus est le centre de gravité.
 - La centralisation ne signifie pas une concentration exclusive sur une ville (ex: Nantes).
 - Répartition juste des acteurs sur l'ensemble du territoire.
 - Autorité "Tech" forte au niveau régional.
- Modèle décentralisé — Gouvernance distribuée par pôles ou territoires.
- Modèle ultra-centralisé — Des Groupes de Travail (GT) agissent comme des "bras opérationnels" du Campus Cyber.
- Modèle collégial
 - Gouvernance par collèges.
 - Gouvernance avec un Conseil d'Administration (CA).
 - Un CA régional auquel siègent les CA départementaux.
 - Des Conseils d'Administration départementaux.
- Modèle orchestré / intelligence distribuée
 - Le Campus agit comme un orchestrateur.
 - L'intelligence est distribuée parmi les acteurs.
 - Les acteurs (RSSI, écoles, industriels, chercheurs, etc.) portent les missions.
 - Le Campus coordonne et orchestre ces missions.

Ressources & outils

- Centre de ressources partagées — Contient des livrables et des documents utiles.
- Schéma de gouvernance proposé — Structure allant du stratégique à l'opérationnel.

Valeur ajoutée régionale

- Label Cyber Régional — Mettre en avant les talents locaux. Valoriser les compétences et savoir-faire régionaux. Co-construire un référentiel commun.

Recommandations et garde-fous

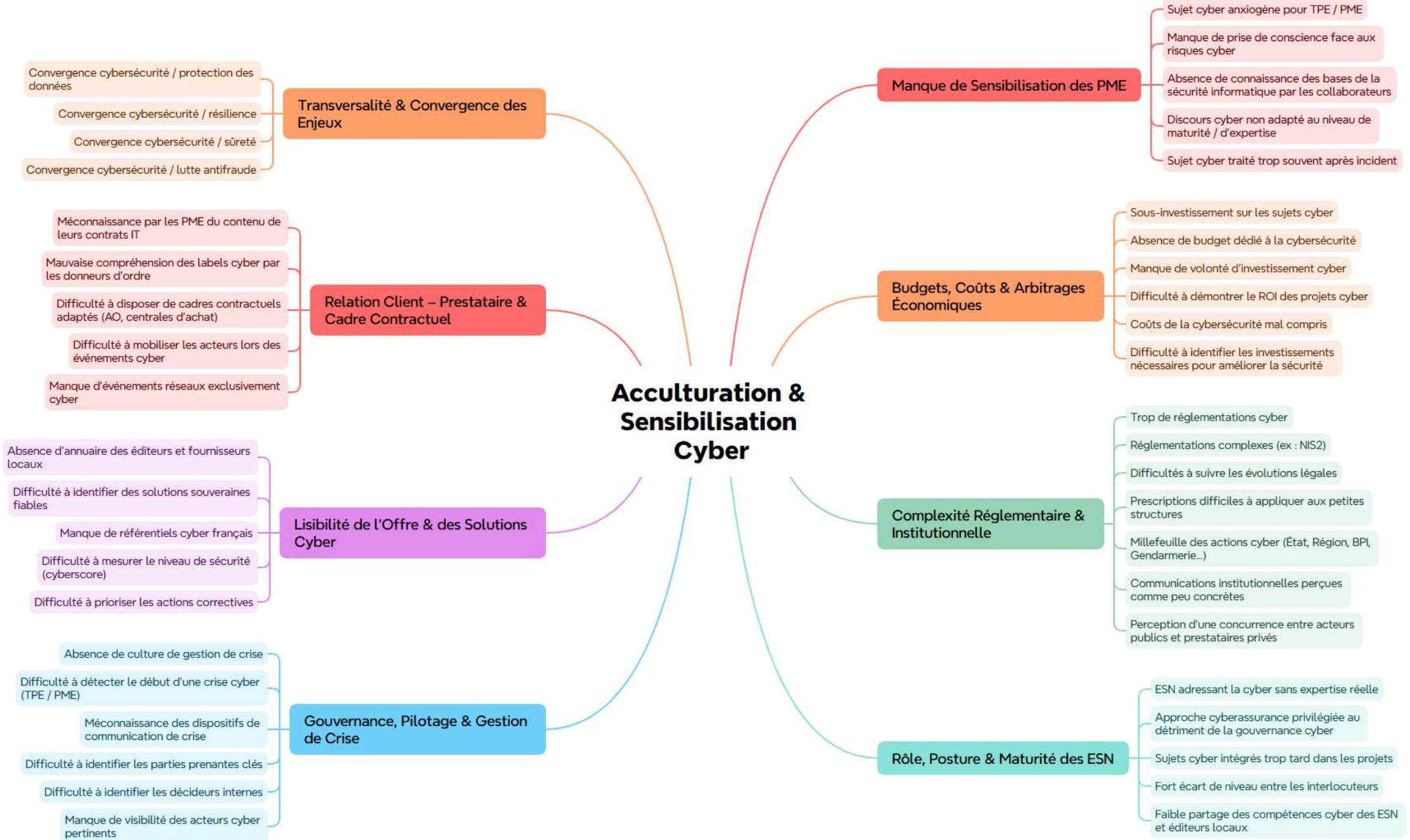
- Financement et pilotage — Ceux qui financent ne doivent pas obtenir de droit de pilotage. Éviter qu'une instance soit majoritairement pilotée par des élus.
- Équilibre de représentation — Prévenir un déséquilibre entre Métropole, Région et Département. Assurer une juste représentation de l'ensemble du territoire.

Synthèse Atelier ESN



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber)



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber) → 44 retours

1. Constat général

L'atelier ESN a fait émerger **44 irritants**, révélant une réalité largement partagée sur le territoire : la cybersécurité reste **mal comprise, mal structurée et difficilement actionnable**, aussi bien pour les **PME/ETI clientes** que pour les **ESN elles-mêmes**, prises dans un écosystème complexe.

Les irritants les plus votés convergent vers **quatre constats structurants** :

- Une **faible acculturation cyber** des dirigeants, des collaborateurs et parfois des décideurs publics, générant anxiété, incompréhension et inertie.
- Une **sous-évaluation persistante du risque cyber**, encore perçu comme secondaire, lointain ou purement technique.
- Un **déficit de moyens, de compétences et de repères concrets**, tant côté clients que côté prestataires.
- Un **écosystème cyber jugé complexe, fragmenté et peu lisible**, mêlant réglementations, acteurs publics, labels, solutions et offres difficilement compréhensibles pour les PME/ETI.

2. Top irritants identifiés

1. Manque de sensibilisation et de prise de conscience cyber (♥ 5)

Le sujet cyber reste anxiogène, mal compris et peu approprié par les PME/ETI et leurs collaborateurs.
→ Faible engagement, actions tardives, souvent déclenchées **après incident**.

2. Sous-investissement et difficulté à justifier la valeur de la cyber (♥ 4)

La cybersécurité est majoritairement perçue comme un **centre de coût** sans valeur directe pour le business.
→ ROI difficile à démontrer, arbitrages défavorables, budgets inexistantes ou insuffisants.

3. Manque de prise de conscience des collaborateurs (♥ 3)

Faible appropriation des enjeux cyber au quotidien, sentiment de non-concernement.
→ Difficulté à responsabiliser durablement les équipes.

4. La cyber n'est pas reliée aux enjeux business et opérationnels (♥ 3)

La cybersécurité reste perçue comme un **sujet IT**, déconnecté :

- du risque opérationnel,
- de la continuité d'activité,
- et de la performance globale.

5. Absence de ressources et de compétences internes dans les PME (♥ 3)

Pas ou peu de DSI, manque de profils qualifiés, forte dépendance aux prestataires.
→ Difficulté à piloter, challenger et prioriser les actions cyber.



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber)

3. Messages à retenir

✓ **Les irritants exprimés ne sont pas d'abord techniques**, mais relèvent principalement :

- d'un **déficit d'acculturation et de pédagogie**,
- d'une **sous-évaluation du risque**,
- d'une **incapacité à prioriser**,
- et d'un **manque de moyens et de repères concrets**.

✓ **La cybersécurité reste trop souvent perçue comme un sujet IT**, déconnecté :

- du business,
- des risques opérationnels,
- et de la continuité d'activité.

✓ Les PME/ETI comme les ESN expriment un besoin fort de :

- **vulgarisation et langage commun**,
- **simplicité et pragmatisme**,
- **cadres clairs et lisibles**,
- **solutions proportionnées à la taille et à la maturité**, et d'un **accompagnement non anxiogène**.

✓ Le principal frein n'est pas la mauvaise volonté, mais :

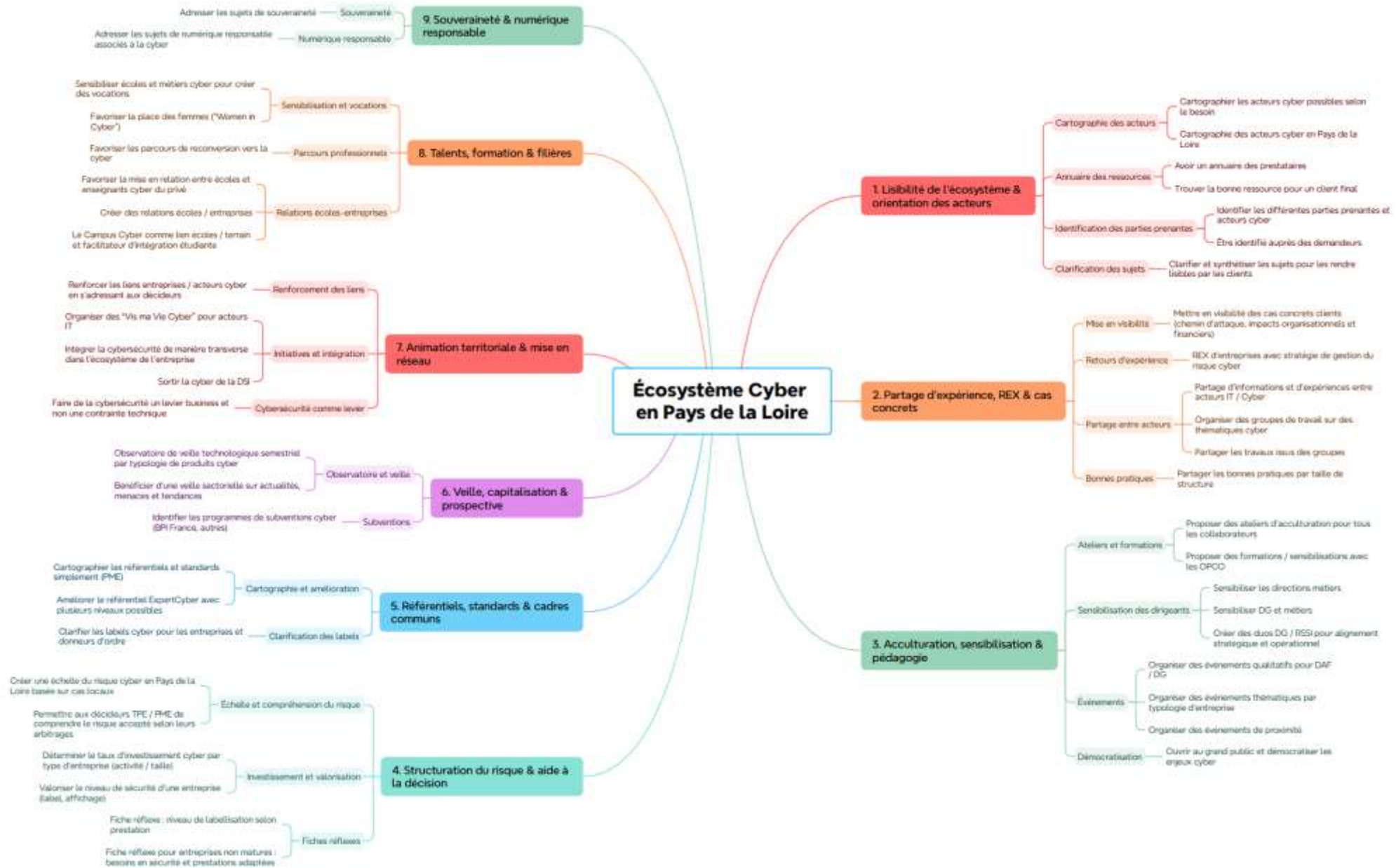
- la **charge mentale**,
- la **complexité perçue**,
- l'**absence de repères structurants**,
- et le sentiment d'un **effort disproportionné** au regard des capacités réelles des PME/ETI.

✓ **Le Campus Cyber a un rôle clé** pour :

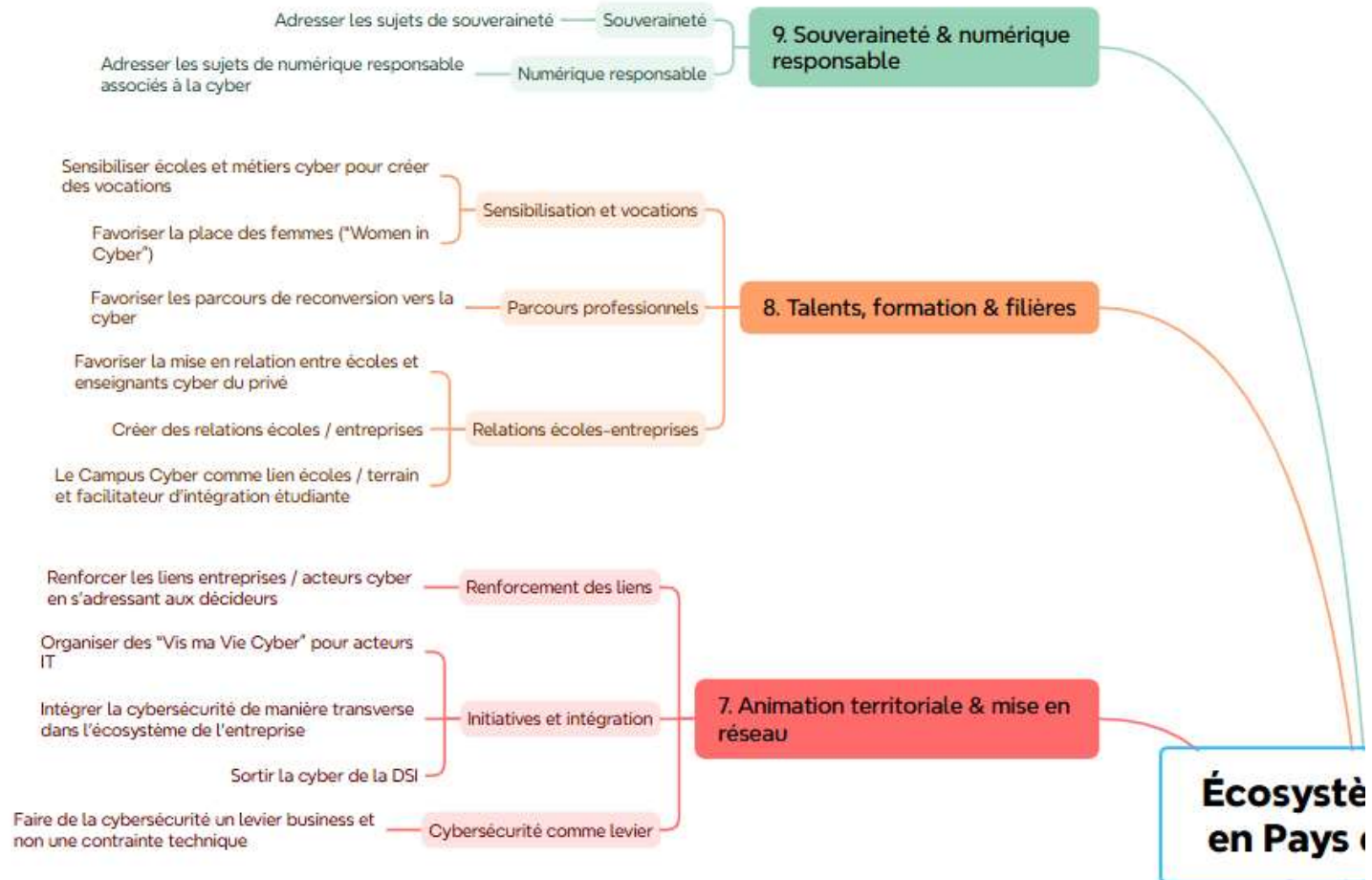
- structurer l'écosystème ESN,
- créer un langage commun clients / prestataires / institutions,
- réduire la complexité,
- et rendre la cybersécurité **concrète, accessible et actionnable** à l'échelle du territoire.



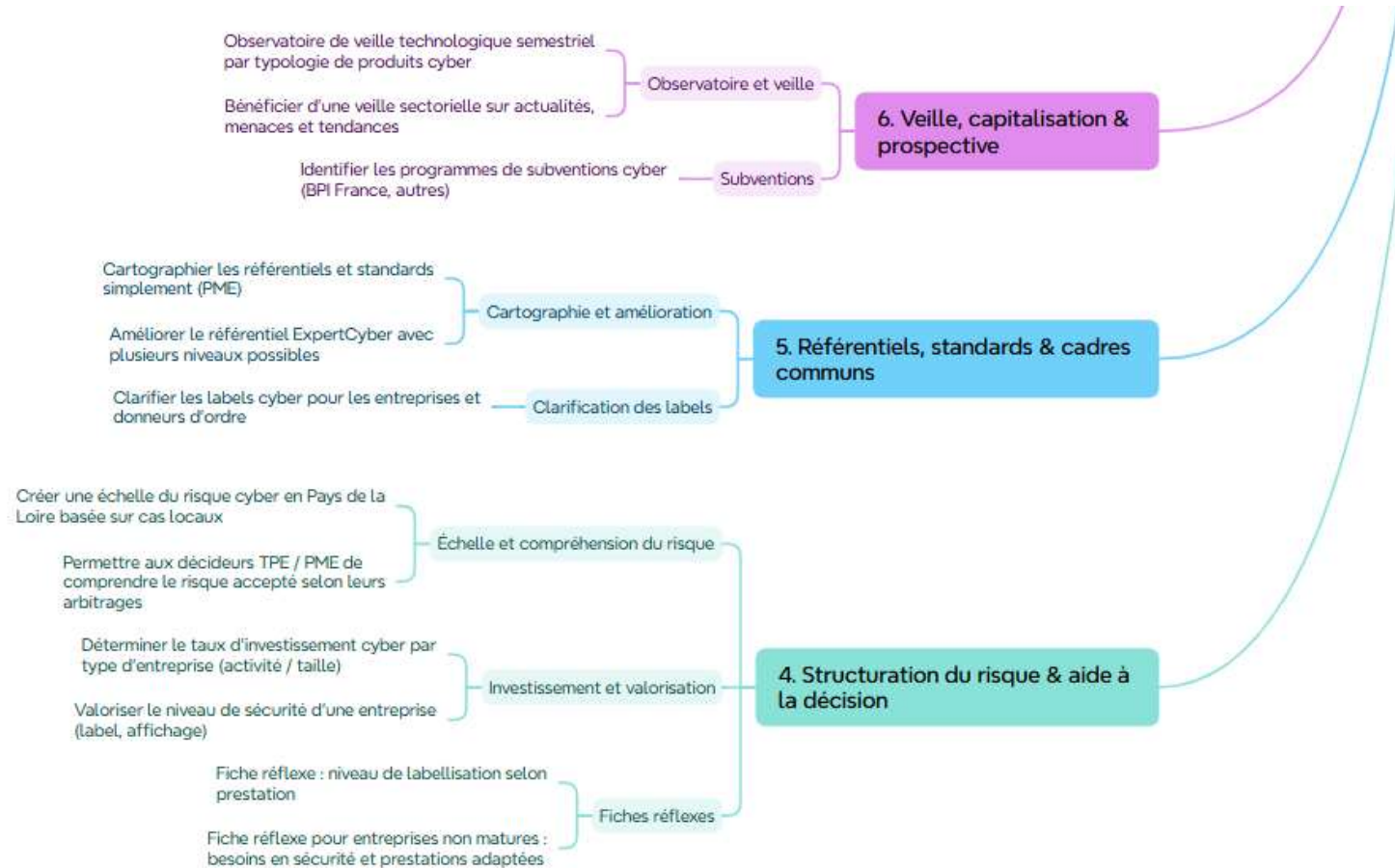
Les leviers (ou.. Que peut-on faire du Campus Cyber ?)



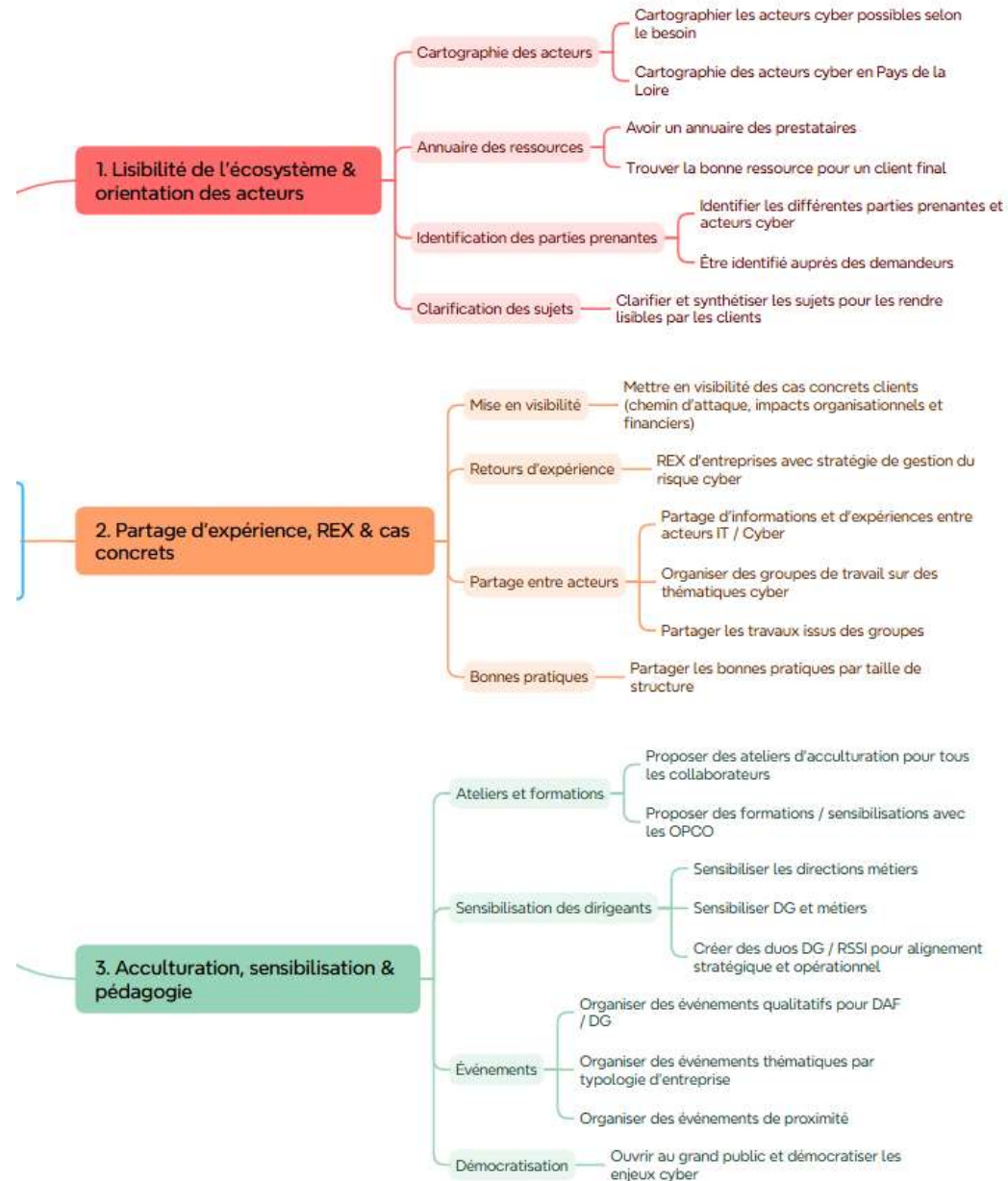
Les leviers *(ou.. Que peut-on faire du Campus Cyber ?)*



Les leviers *(ou.. Que peut-on faire du Campus Cyber ?)*



Les leviers *(ou.. Que peut-on faire du Campus Cyber ?)*



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?)

1. Constat général

L'atelier ESN a fait émerger **36 leviers**, traduisant une attente forte vis-à-vis du Campus Cyber comme **acteur structurant, lisible et fédérateur** de l'écosystème.

Les idées exprimées se concentrent principalement sur :

- la **lisibilité de l'écosystème cyber** (acteurs, offres, référentiels),
- la **pédagogie et l'acculturation**, en particulier des décideurs et des métiers,
- la **mise en visibilité de cas concrets et de retours d'expérience**,
- la **mutualisation des ressources, des outils et des connaissances**,
- la **proximité territoriale** et l'animation de communautés locales,
- le **lien entre entreprises, ESN, écoles et institutions**.

Les leviers les plus plébiscités confirment un besoin de **solutions concrètes, pragmatiques et directement actionnables**, loin des approches trop techniques ou théoriques.

2. Top leviers identifiés

1. Cartographier et rendre lisible l'écosystème cyber (♥ 8)

Cartographier les acteurs cyber en fonction des besoins, disposer d'annuaires clairs (prestataires, ressources, solutions) et aider à identifier la "bonne" ressource pour un client final.

2. Mettre en visibilité des cas concrets et des retours d'expérience (♥ 7)

Valoriser des cas clients réels (chemins d'attaque, impacts organisationnels et financiers), partager des REX d'entreprises et des bonnes pratiques adaptées à la taille des structures.

3. Organiser et animer des événements de proximité (♥ 5)

Événements locaux, thématiques ou sectoriels, groupes de travail, temps d'échange entre pairs pour réduire l'isolement et favoriser la confiance.

4. Partager et mutualiser les connaissances et les ressources (♥ 4)

Partage d'informations entre acteurs IT/Cyber, mutualisation des outils, diffusion des bonnes pratiques et des référentiels simplifiés.

5. Structurer l'acculturation des dirigeants et des métiers (♥ 3)

Sensibilisation DG, DAF, métiers, création de duos DG/RSSI, ateliers non techniques orientés risque, gouvernance et business.



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?)

3. Messages à retenir

✓ **Les leviers attendus sont avant tout organisationnels et humains**, plus que technologiques.

Les participants demandent des **repères clairs**, des **points d'entrée simples** et des **solutions compréhensibles**.

✓ **La valeur vient du concret** :

cas réels, retours d'expérience, bonnes pratiques locales, échanges entre pairs.

✓ **La proximité territoriale est un facteur clé de succès** :

événements locaux, animation continue, mise en relation directe.

✓ **La mutualisation est un levier majeur** :

partager outils, ressources, veille et connaissances permet de rendre la cybersécurité accessible aux PME/ETI.

✓ **Le Campus Cyber est attendu comme un tiers de confiance**, capable de structurer, relier et rendre lisible l'écosystème ESN.

4. Opportunités du Campus Cyber

• **Créer une cartographie régionale dynamique de l'écosystème cyber**

- annuaire des prestataires et ressources,
- orientation selon les besoins des entreprises,
- clarification des offres et des labels.

• **Structurer et diffuser des retours d'expérience concrets**

- cas clients anonymisés,
- REX d'entreprises locales,
- bonnes pratiques par typologie et taille d'entreprise.

• **Animer des communautés de proximité**

- événements locaux et sectoriels,
- groupes de travail thématiques,
- échanges entre dirigeants, métiers et ESN.

• **Déployer des parcours d'acculturation non techniques**

- ateliers dirigeants / métiers,
- sensibilisation des collaborateurs,
- mise en valeur de la cyber comme levier business.

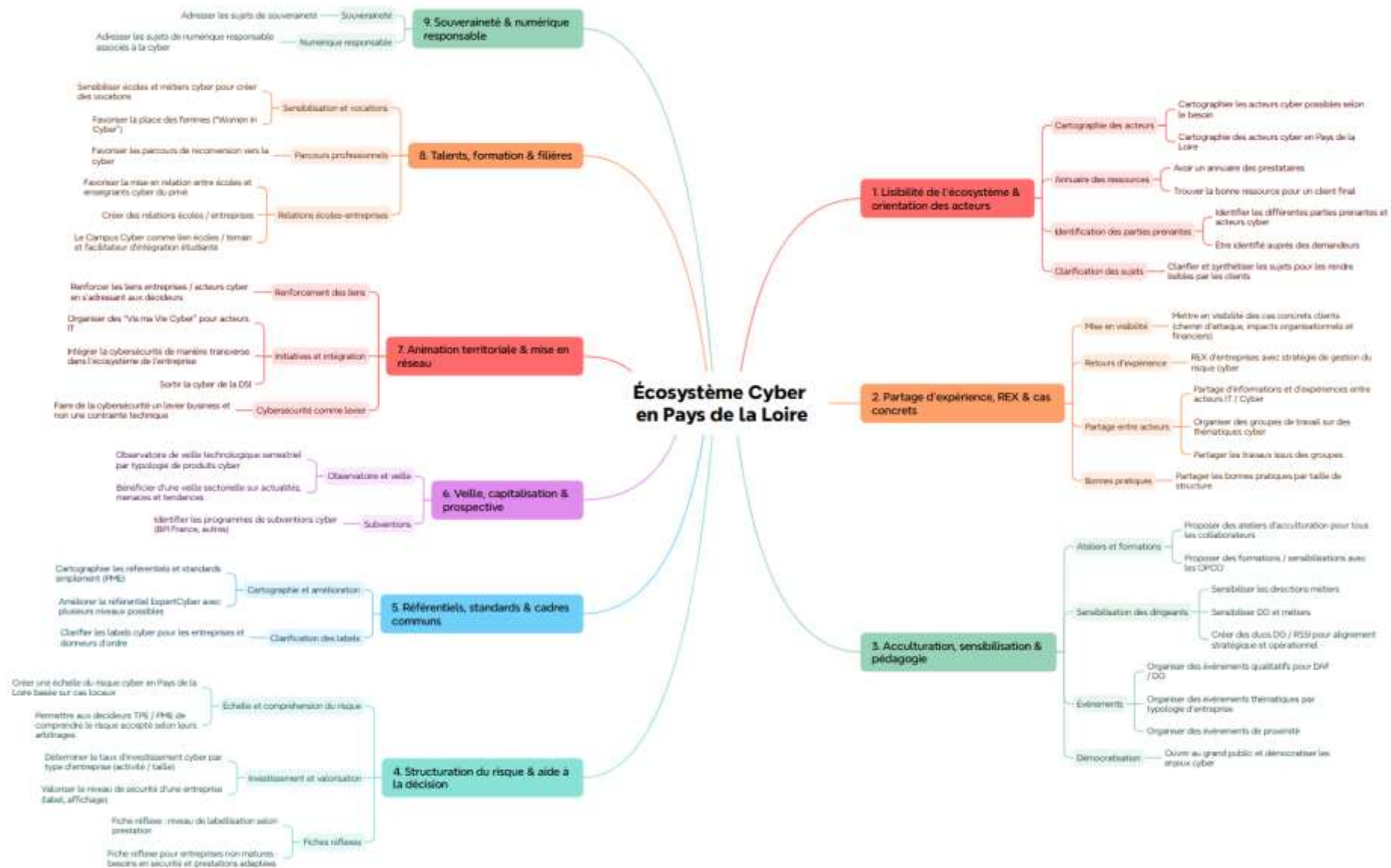
• **Jouer un rôle de passerelle**

- entre entreprises, ESN, écoles et institutions,
- favoriser les talents, les reconversions et les vocations,
- intégrer les étudiants et jeunes profils dans l'écosystème local.



Mobiliser l'écosystème

(ou.. Comment l'écosystème peut animer le campus cyber ?)



Mobiliser l'écosystème

(ou.. Comment l'écosystème peut animer le campus cyber ?)

1. Animer et faire vivre la communauté cyber

- Organiser des **événements locaux et régionaux** (cyber et non-cyber).
- Proposer des **conférences, webinaires et ateliers thématiques**.
- Créer des **événements structurants** (Cyber Tour, événement majeur en PDL).
- Mettre en place des **formats dynamiques** : tables rondes, business dating, pentest live.

👉 Faire du Campus un **lieu vivant**, identifié et attendu

2. Produire et diffuser des contenus concrets et accessibles

- Partager des **témoignages sur des cas d'attaques réels**.
- Créer des **podcasts, talks, formats courts et vulgarisés**.
- Organiser des formats **"Ask Me Anything"** avec des profils cyber variés.
- Proposer des **guides pratiques**, fiches d'orientation, feuilles de route.

👉 Démystifier la cyber par le **concret et le retour terrain**.

3. Faciliter les rencontres et la coopération entre acteurs

- Mettre en relation **entreprises, ESN, experts indépendants et RSSI**.
- Organiser des **rencontres ciblées** (RSSI / acteurs cyber / dirigeants).
- Créer et animer des **groupes de travail thématiques**.
- Aider à identifier la **bonne ressource** pour le bon besoin.

👉 Transformer le Campus en **carrefour de confiance**.

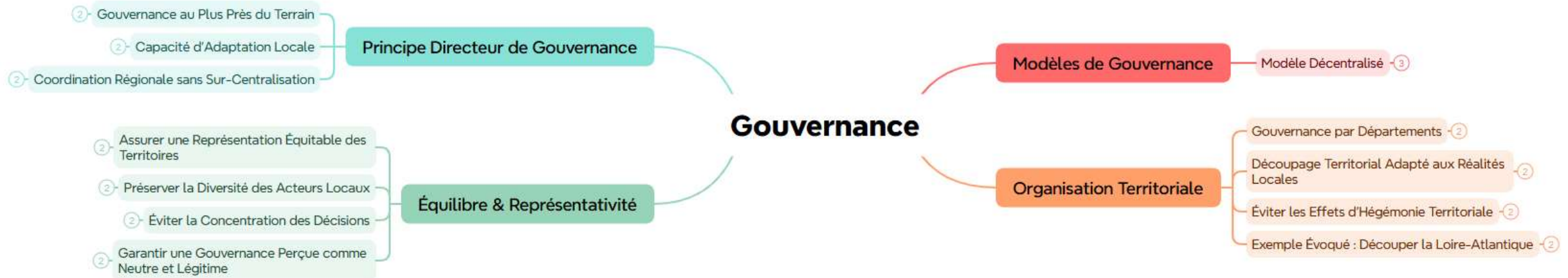
4. Transmettre, former et créer des passerelles durables

- Proposer des **formations et actions de sensibilisation**.
- Impliquer les **écoles, enseignants et étudiants**.
- Mettre à disposition des **formateurs** et experts.
- Favoriser les **reconversions** et la **diversité** (Women in Cyber).

👉 Faire du Campus un **pont entre talents, terrain et entreprises**.



Structurer la Gouvernance

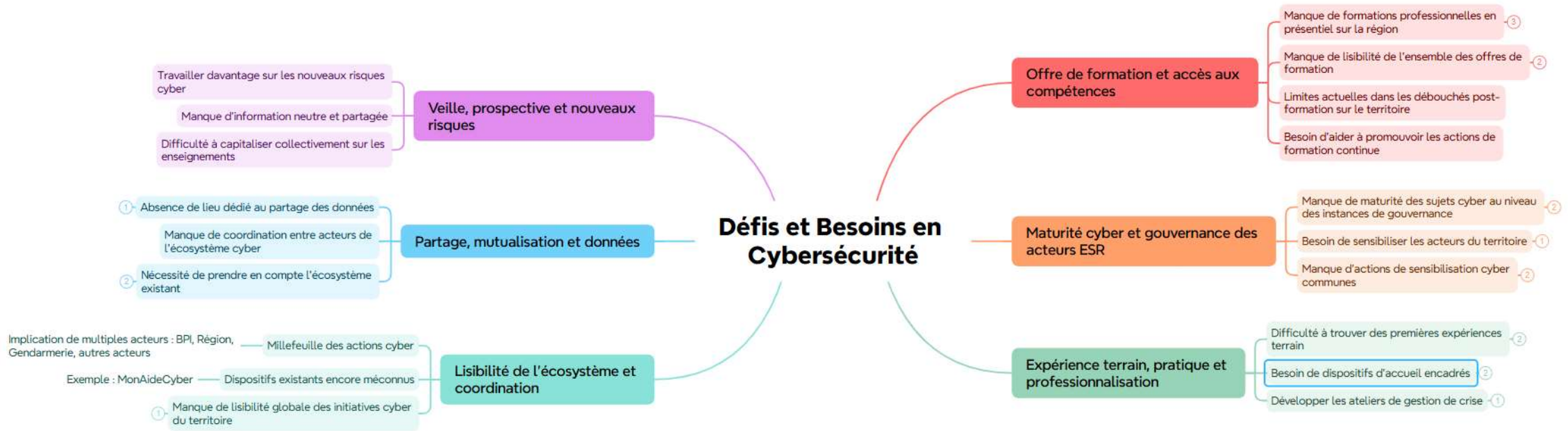


Synthèse atelier
Enseignement
supérieur /
Recherche



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber)



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber) → 44 retours

1. Constat général

L'atelier **ESR** a fait émerger des irritants forts, révélant un **décalage structurel** entre :

- l'offre de formation cyber,
- les besoins opérationnels du territoire,
- et la réalité du marché de l'emploi et des compétences.

Les échanges mettent en évidence une situation où :

- la **formation cyber existe**, mais reste **peu lisible, peu accessible localement** et parfois déconnectée du terrain,
- la **maturité cyber des instances de gouvernance** (dirigeants, COMEX, CODIR) demeure hétérogène,
- les **dispositifs existants** sont nombreux mais **fragmentés et mal connus**,
- les **passerelles entre formation, pratique et emploi** sont insuffisamment structurées.

2. Top irritants identifiés

1. Manque de formations professionnelles cyber accessibles localement (❤️ 4)

Absence ou rareté de formations clés en présentiel sur la région (ex. Lead Implementor / Lead Auditor ISO 27001, EBIOS RM, NIS2). → Dépendance à Paris, coûts logistiques élevés, frein à la montée en compétences locale.

2. Manque de lisibilité de l'offre de formation et des débouchés (❤️ 2)

Difficulté à identifier :

- les formations existantes (initiales, continues, alternance),
- les parcours possibles,
- et les débouchés concrets post-formation sur le territoire.

3. Difficulté d'accès à l'expérience terrain et à la pratique réelle (❤️ 2)

Peu d'opportunités d'observation, de formation en situation de travail ou d'immersion. → Fracture entre théorie académique et réalité opérationnelle.

4. Faible maturité cyber des instances de gouvernance (❤️ 1)

Les sujets cyber restent insuffisamment portés au niveau :

- dirigeants,
- COMEX / CODIR,
- gouvernance des établissements et partenaires.

5. Écosystème cyber fragmenté et peu coordonné (❤️ 3)

Millefeuille d'actions et de dispositifs (Région, BPI, Gendarmerie, etc.) → Manque de coordination, redondances, dispositifs existants encore méconnus (ex. MonAideCyber).



Les irritants

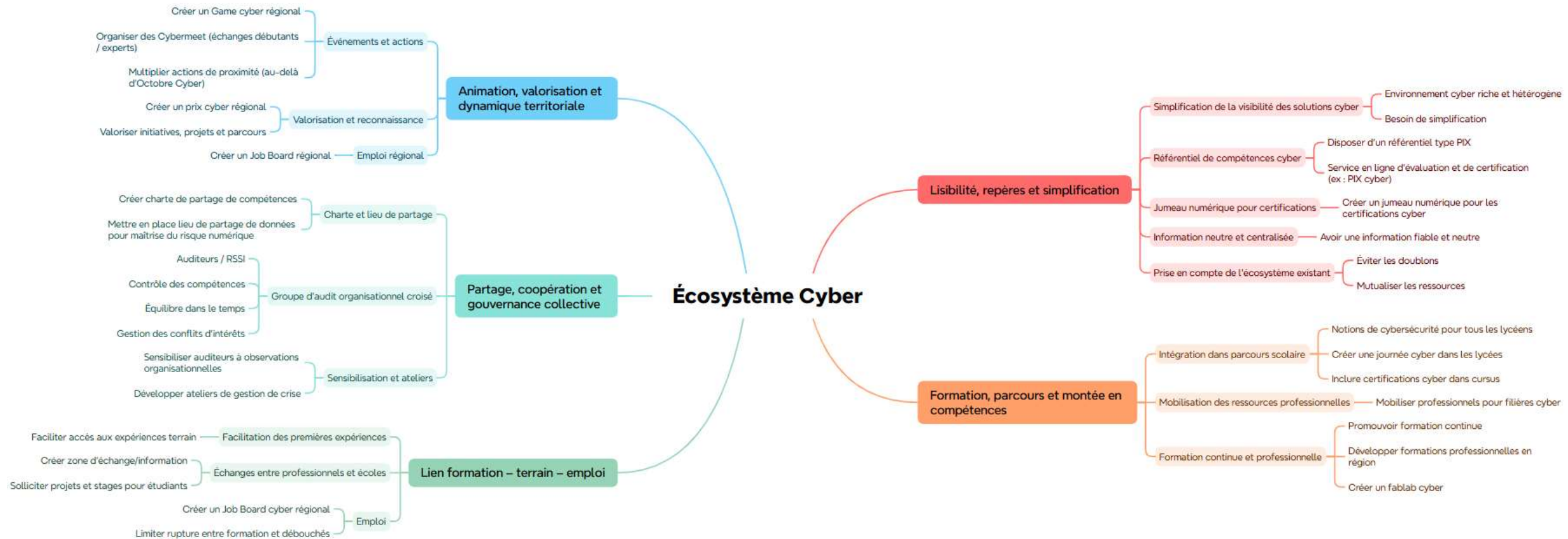
(ou.. Pourquoi a-t-on besoin d'un Campus Cyber)

3. Messages à retenir

- ✓ **Les irritants ESR sont d'abord structurels**, pas techniques. Ils portent sur l'**organisation de l'offre**, la **lisibilité des parcours** et la **connexion au terrain**.
- ✓ **La montée en compétences cyber locale est freinée** par :
 - l'absence de formations clés sur le territoire,
 - le manque de visibilité des dispositifs existants,
 - et la difficulté à acquérir une expérience pratique encadrée.
- ✓ **Le lien entre formation, pratique et emploi est insuffisamment structuré**, ce qui limite :
 - l'employabilité,
 - la professionnalisation,
 - et la rétention des talents sur le territoire.
- ✓ **Le principal besoin exprimé n'est pas de créer plus de dispositifs**, mais de :
 - mieux coordonner l'existant,
 - mutualiser les ressources,
 - centraliser l'information,
 - et offrir une lecture claire et neutre de l'écosystème.
- ✓ **Le Campus Cyber est attendu comme un tiers de confiance** capable de :
 - structurer l'offre ESR,
 - créer des passerelles vers le terrain,
 - et renforcer la cohérence territoriale.



Les leviers (ou.. Que peut-on faire du Campus Cyber ?)



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?)

1. Constat général

L'atelier **ESR** a fait émerger un volume important de leviers, révélant une attente forte vis-à-vis du Campus Cyber comme **acteur structurant des parcours de compétences** et **coordinateur de l'écosystème formation-emploi**.

Les idées exprimées se concentrent principalement sur :

- la **lisibilité des parcours et des compétences cyber**,
- l'**accès aux formations et certifications** sur le territoire,
- la **connexion entre formation théorique, pratique terrain et emploi**,
- la **mutualisation des ressources et des initiatives existantes**,
- la **valorisation des talents, des projets et des parcours**.

Les leviers les plus plébiscités traduisent un besoin clair de **repères communs, neutres et opérationnels**, plutôt que la création de dispositifs supplémentaires.

2. Top leviers identifiés

1. Créer des repères communs sur les compétences cyber (♥ 4)

Mettre en place un **référentiel de type PIX**, des outils d'évaluation et de certification, et améliorer la lisibilité des compétences cyber acquises ou attendues.

2. Développer et rendre visibles les parcours de formation cyber (♥ 4)

Intégrer la cybersécurité dans les parcours initiaux (lycées), inclure des certifications dans les cursus, promouvoir la formation continue et structurer une offre locale plus lisible.

3. Relier formation, terrain et emploi (♥ 2)

Faciliter l'accès aux premières expériences terrain (observation, projets, stages), créer des espaces d'échange entre écoles et professionnels, et structurer les débouchés sur le territoire.

4. Simplifier et coordonner l'écosystème existant (♥ 2)

Mieux prendre en compte les dispositifs existants, éviter les doublons, mutualiser les ressources et proposer une information neutre et centralisée.

5. Valoriser et animer la dynamique territoriale cyber (♥ 2)

Créer des événements fédérateurs (Game cyber, Cybermeet, prix cyber régional) et multiplier les actions de proximité tout au long de l'année.



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?)

3. Messages à retenir

✓ **Les leviers ESR sont avant tout structurels et pédagogiques,** pas technologiques.
Ils visent à clarifier les parcours, rendre les compétences lisibles et faciliter l'orientation.

✓ **Le principal enjeu est la continuité :**
continuité entre formation initiale, formation continue, pratique terrain et emploi.

✓ **La valeur du Campus Cyber réside dans sa neutralité :**
capacité à structurer, comparer, orienter et mutualiser sans concurrence avec les acteurs existants.

✓ **Les participants n'attendent pas plus d'offres,** mais :

- plus de lisibilité,
- plus de coordination,
- et plus de passerelles concrètes.

4. Opportunités du Campus Cyber

• **Créer un socle commun de compétences cyber**

- référentiel type PIX,
- outils d'évaluation,
- certifications lisibles.

• **Structurer des parcours de formation territoriaux**

- lycée → enseignement supérieur → formation continue,
- intégration de certifications,
- valorisation des parcours.

• **Faciliter l'accès au terrain**

- projets réels,
- stages,
- dispositifs d'observation encadrés.

• **Jouer un rôle de hub neutre**

- information centralisée,
- coordination des initiatives,
- mutualisation des ressources.

• **Animer et valoriser l'écosystème**

- événements fédérateurs,
- prix et reconnaissances,
- mise en lumière des talents et des projets.

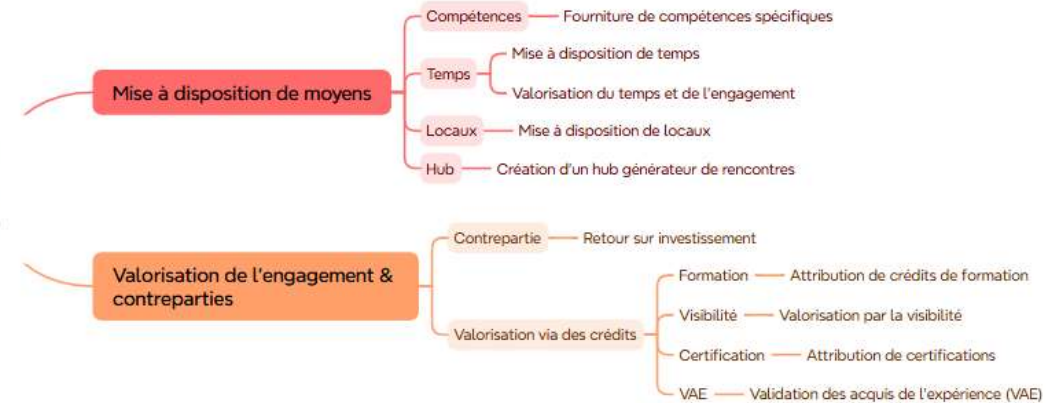


Mobiliser l'écosystème

(ou.. Comment l'écosystème peut animer le campus cyber ?)



Engagement et Valorisation au Campus Cyber



Mobiliser l'écosystème

(ou.. Comment l'écosystème peut animer le campus cyber ?)

1. Mettre à disposition des moyens concrets pour s'engager

- Mise à disposition de **compétences** (expertise, encadrement, accompagnement).
- Mise à disposition de **temps**, avec une **valorisation explicite de l'engagement**.
- Mise à disposition de **locaux** pour fédérer et créer un hub de rencontres.

👉 Permettre l'engagement sans friction, clair et reconnu.

2. Valoriser l'engagement et créer un retour sur investissement

Reconnaître l'engagement par des **contreparties visibles**.

Valorisation via des **crédits** :

- formation,
- visibilité,
- certification,
- VAE.

👉 Passer d'un engagement "bénévole" à un engagement **utile et valorisé**.

3. Co-construire des services et dispositifs soutenus par le Campus

Offrir la possibilité de contribuer à des **services portés par le Campus** :

- analyses technologiques,
- audits / analyses de sites,
- dispositifs d'accompagnement.

Favoriser l'**apprentissage par la pratique** :

- parrainage,
- accueil de stagiaires,
- jurys, concours.

👉 Faire du Campus un **cadre sécurisé pour apprendre et transmettre**.

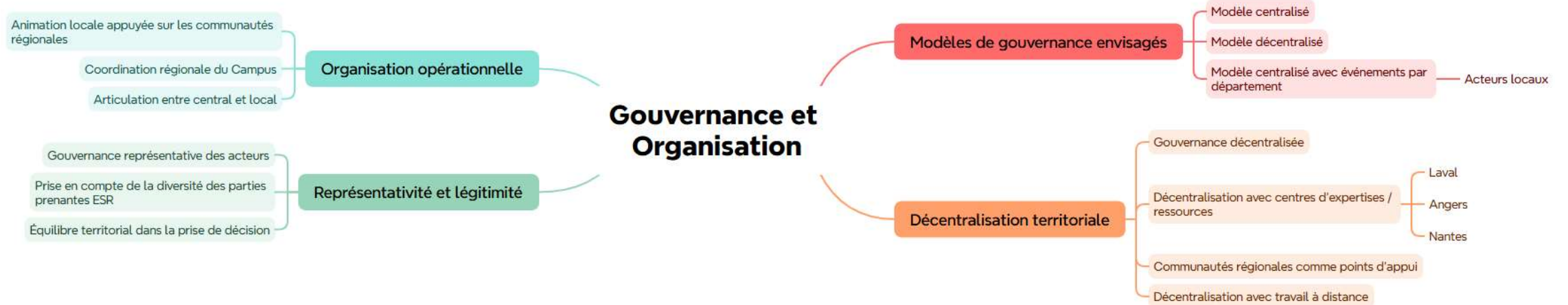
4. Animer une dynamique collective et visible

- Monter des **événements fédérateurs** :
- Créer des rendez-vous identifiables et réguliers.

👉 Donner une **visibilité collective** à l'écosystème ESR et à ses actions.



Structurer la Gouvernance

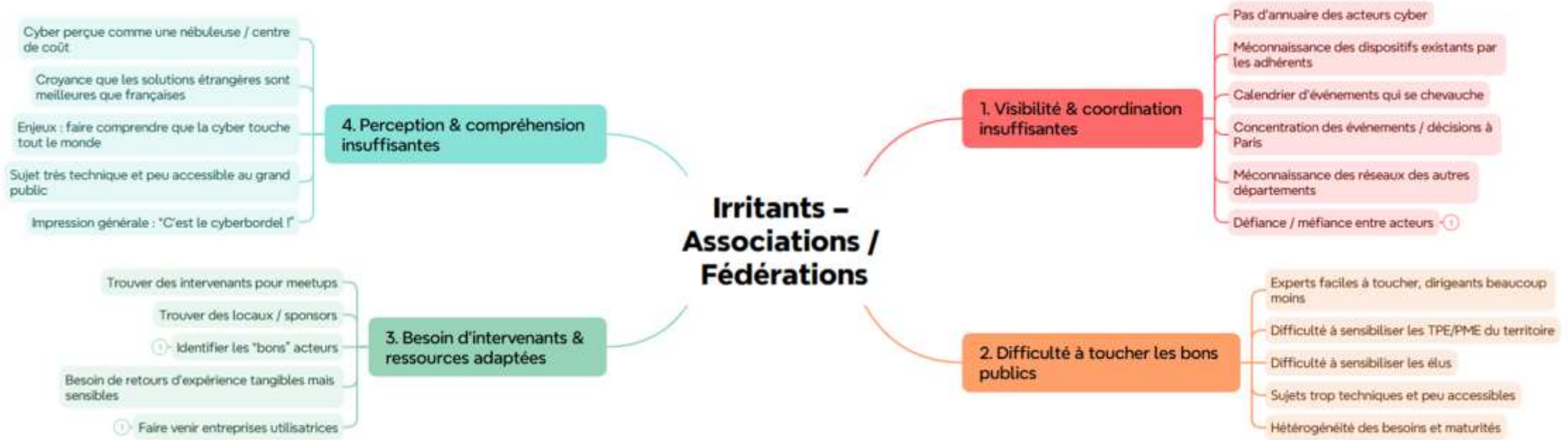


Synthèse atelier
Association
Fédération



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber) → 39 retours



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber) → 39 retours

1. Constat général

L'atelier a fait émerger **un ensemble d'irritants fortement convergents**, révélant que les associations et fédérations jouent un rôle clé dans la diffusion de la culture cyber, mais disposent **de moyens fragmentés, d'une visibilité insuffisante**, et opèrent dans un écosystème **peu lisible et difficile à coordonner**.

Les retours montrent quatre constats structurants :

• **Un manque de visibilité et d'accès à l'information**

Absence d'annuaire des acteurs, méconnaissance des dispositifs, difficulté à identifier les bons intervenants ou les bonnes solutions, dispersion des initiatives.

• **Une difficulté à toucher les bons publics**

Les experts et passionnés sont accessibles, mais **les dirigeants, élus, TPE-PME et publics non-techniques restent difficiles à sensibiliser**.

• **Un écosystème fragmenté et peu coordonné**

Calendriers qui se chevauchent, actions menées isolément, méfiance entre acteurs, hétérogénéité des maturités.

• **Des besoins de contenus concrets, accessibles et adaptés**

REX tangibles mais sensibles, sujets souvent trop techniques, besoin d'un langage simple et d'exemples ancrés dans la réalité des territoires.

2. Top irritants identifiés

1. Absence d'un annuaire opérationnel des acteurs / associations cyber (♥9)

→ Ralentit la coopération, empêche la mutualisation, réduit la lisibilité du paysage.

2. Difficulté à toucher les dirigeants, comparé à la facilité de toucher les experts (♥7)

→ Frein majeur à l'acculturation : les messages n'atteignent pas les décideurs.

3. Difficulté à sensibiliser les TPE/PME du territoire (♥5)

→ Public prioritaire mais peu atteint : manque de temps, de moyens, d'intérêt initial.

4. Méconnaissance des dispositifs existants par les adhérents (♥4)

→ Les initiatives existent, mais ne sont pas connues → perte d'impact.

5. Chevauchement des calendriers d'associations (♥4)

→ Fragmentation, dilution de l'attention, perte de synergie.



Les irritants

(ou.. Pourquoi a-t-on besoin d'un Campus Cyber) → 39 retours

3. Messages à retenir

✓ **La fragmentation est le frein principal.**

Absence de coordination, méfiance, calendriers concurrents, manque de visibilité → les efforts se neutralisent au lieu de se renforcer.

✓ **Le public prioritaire n'est pas le public le plus facile à toucher.**

Dirigeants, élus, TPE/PME : ce sont eux qui ont le plus à gagner, mais les messages cyber n'atteignent pas leur quotidien.

✓ **Le besoin n'est pas technique : il est organisationnel et pédagogique.**

Les associations demandent :

- plus de lisibilité,
- des outils pratiques,
- des messages simples,
- des exemples locaux,
- des lieux de coordination,
- et des REX concrets (mais sécurisés).

✓ **Le territoire joue un rôle déterminant.**

Les acteurs locaux sont prêts à s'impliquer, mais ils manquent d'un cadre, d'un annuaire, d'une coordination et d'un soutien continu.

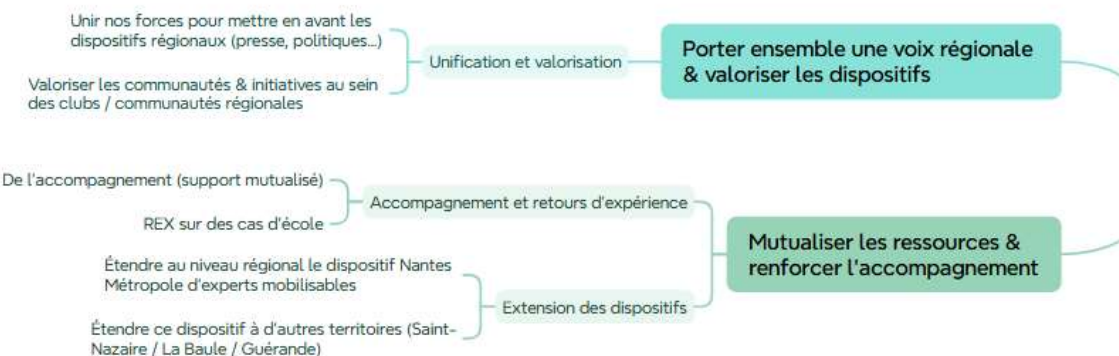
✓ **L'écosystème veut coopérer, mais manque d'un point de convergence.**

Une structure territoriale, neutre, partagée, pourrait décupler l'impact.

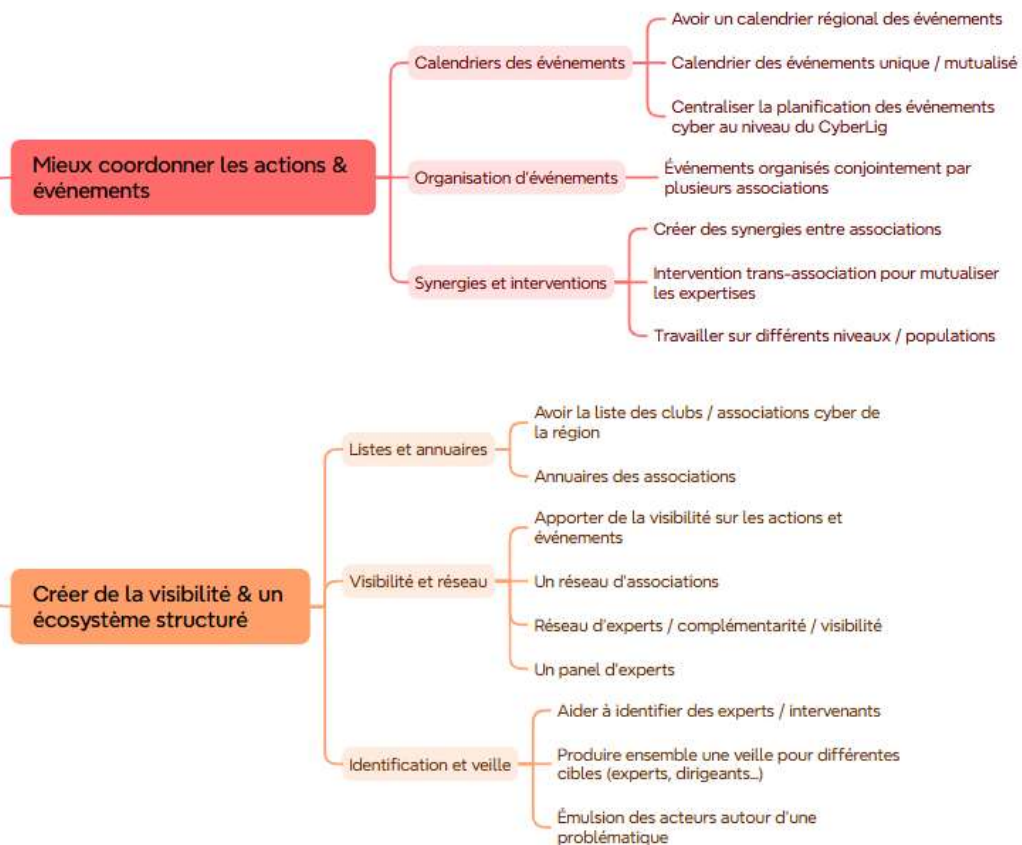


Les leviers

(ou.. Que peut-on faire du Campus Cyber ?) → 36 retours



Leviers – Associations / Fédérations



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?) → 36 retours

1. Constat général

L'atelier a fait émerger **un volume important de leviers**, révélant une volonté forte des associations et fédérations d'agir davantage **ensemble**, tout en soulignant un écosystème encore **trop fragmenté, peu visible**, et **insuffisamment coordonné**.

Les idées convergent autour de besoins structurants :

▪ Une meilleure coordination des événements et des actions

Superpositions de calendriers, initiatives isolées, manque de synergies → perte d'impact collectif.

▪ Une plus grande visibilité des acteurs, ressources et expertises

Les membres manquent d'un repère clair : qui fait quoi, où trouver qui, comment identifier un expert fiable ?

▪ Une véritable mise en réseau territoriale

Les initiatives locales existent, mais doivent être connectées, structurées et valorisées pour gagner en portée.

▪ Une mutualisation accrue des ressources

Experts mobilisables, veille, panels, accompagnement... Les associations veulent **faire ensemble** ce qu'elles ne peuvent pas porter seules.

Le fil rouge est clair :

👉 **Les associations veulent se coordonner, se rendre visibles, mutualiser leurs forces et structurer un réseau régional puissant.**

2. Top leviers identifiés

1. Avoir la liste des clubs / associations cyber de la région (❤️6)

Un outil simple mais déterminant pour naviguer dans l'écosystème et améliorer la coordination.

2. Apporter davantage de visibilité aux actions & événements des communautés (❤️6)

Permet d'éviter les doublons, d'augmenter la participation et de renforcer l'impact territorial.

3. Des événements organisés conjointement par plusieurs associations (❤️6)

Croiser les réseaux, mixer les publics, renforcer l'effet de masse → levier très puissant.

4. Avoir un calendrier des événements (❤️5)

La demande la plus opérationnelle : un calendrier partagé, lisible, régionalisé.

5. Produire une veille mutualisée (❤️3)

Utile pour toucher différentes cibles : dirigeants, experts, publics non-tech.



Les leviers

(ou.. Que peut-on faire du Campus Cyber ?) → 36 retours

3. Messages à retenir

✓ **Le besoin premier : structurer l'écosystème.**

Annuaire, calendrier, coordination des événements, synergies inter-associations → ce sont les fondations d'un réseau efficace.

✓ **La visibilité est un vecteur d'engagement.**

Les associations veulent être vues, reconnues et connectées. Rendre visibles les actions renforce la dynamique collective.

✓ **La mutualisation est perçue comme naturelle et nécessaire.**

Experts, REX, panels, veilles, accompagnements → ce que chaque structure ne peut porter seule peut être porté ensemble.

✓ **L'impact naît de la coopération.**

Les événements co-organisés, les actions croisées, les projets communs montrent une maturité collective croissante.

✓ **Un rôle régional est attendu.**

Un acteur neutre pourrait harmoniser, faciliter, soutenir et amplifier les efforts existants → exactement dans la continuité de la logique Campus Cyber.

4. Opportunités du Campus Cyber

• **Créer une plateforme régionale de coordination**

- Calendrier mutualisé
- Annuaire des acteurs / experts
- Espace d'échange inter-associations
- Mise en avant automatique des actions locales

• **Structurer un réseau d'experts mobilisables**

- Panel régional
- Extension des dispositifs existants (ex. Nantes Métropole)
- Mise à disposition en cas d'incident ou d'événement

• **Développer des synergies événementielles**

- Co-organisation d'événements multi-associations
- Formats mutualisés (ateliers, conférences, sensibilisation dirigeants)
- Projets communs presse / politiques / économiques

• **Créer et diffuser une veille mutualisée**

- Veille par cible (dirigeants, experts, élus, TPE/PME)
- Diffusion territoriale via les réseaux associatifs
- Valorisation des contenus produits par les membres

• **Valoriser les initiatives locales**

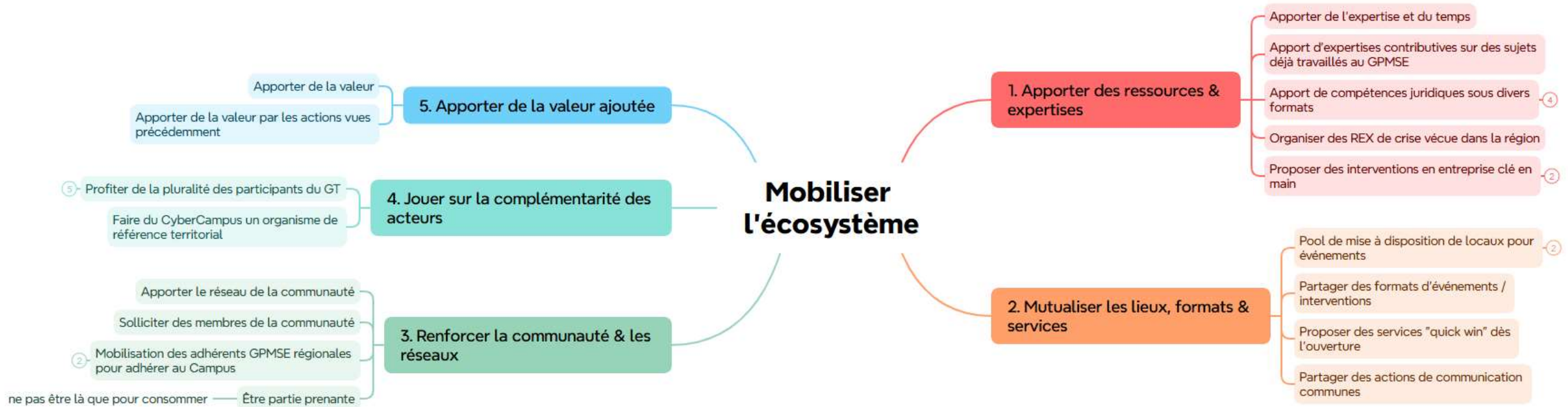
- Vitrophanie régionale (qui fait quoi ?)
- Mise en avant des actions exemplaires
- Promotion des synergies inter-associations

👉 **Objectif : fournir l'infrastructure, les outils et l'animation permettant aux associations de collaborer, se rendre visibles, et amplifier leur impact.**



Mobiliser l'écosystème

(ou.. Comment l'écosystème peut animer le campus cyber ?)



Mobiliser l'écosystème

(ou.. Comment l'écosystème peut animer le campus cyber ?)

1. Mieux connecter et structurer la communauté

Les associations ont exprimé un besoin clair : **mieux se connaître, mieux se coordonner et mieux synchroniser leurs actions.**

Cela passe par :

La création d'un **annuaire régional des associations, experts et intervenants**, pour identifier facilement "qui fait quoi".

Un **calendrier partagé des événements** afin d'éviter les chevauchements, mutualiser les efforts, et renforcer la portée des actions.

La **visibilisation des actions de chaque communauté** (événements, interventions, productions).

La mise en évidence des **complémentarités** entre acteurs (experts, institutions, dirigeants, entreprises).

👉 Créer une **carte de l'écosystème cyber fédéré**, claire, lisible et actualisée.

2. Co-animer des actions concrètes et visibles dans les territoires

L'atelier fait émerger une forte appétence pour des initiatives **conjointes**, structurantes et à fort impact :

Organiser des **événements co-portés par plusieurs associations** (❤️6).

Faire remonter et diffuser des **REX de cas d'école**, pour alimenter la compréhension collective du risque.

Produire ensemble une **veille mutualisée**, destinée à des publics variés (experts, dirigeants...).

Partager des **formats d'événements**, des bonnes pratiques et des supports réutilisables.

👉 Passer d'actions isolées à une **programmation territoriale coordonnée**, où les forces se combinent plutôt que de se disperser..

3. Apporter de la valeur ajoutée au Campus & au territoire

Les associations souhaitent contribuer activement, chacune selon ses forces :

Apporter **des expertises ciblées** (techniques, juridiques, communication, gestion de crise...).

Fournir **du temps, des intervenants, des animateurs**, quand pertinent.

Participer au développement de **services "quick win"** dès l'ouverture : locaux partagés, formats clé en main, interventions en entreprise.

Valoriser des dispositifs exemplaires existants (ex. **mise à disposition d'experts en cas d'attaque**, modèle Nantes Métropole → extension régionale potentielle ❤️3).

👉 Faire du Campus un **référentiel régional** sur lequel chaque acteur peut s'appuyer et contribuer.



Mobiliser l'écosystème

(ou.. Comment l'écosystème peut animer le campus cyber ?)

4. Encourager une dynamique commune & inclusive

Un message revient fortement :

“Ne pas être là que pour consommer, mais pour contribuer.”

Cela implique :

Favoriser l'**implication des adhérents des fédérations** dans le Campus (GPMSE, clubs cyber, réseaux pro... ❤️3).

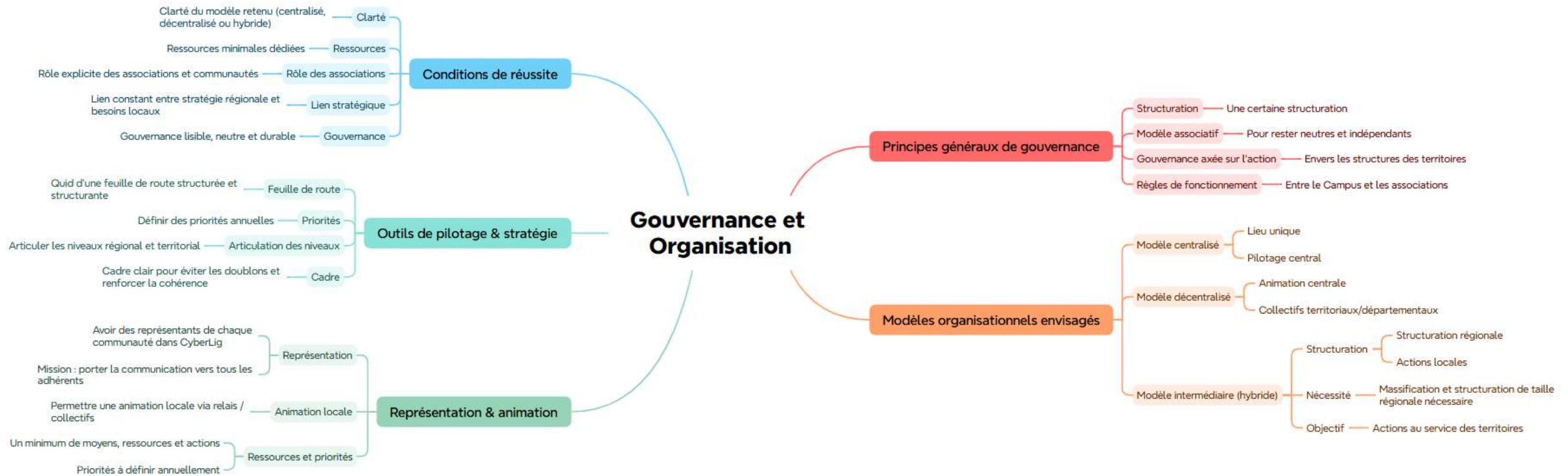
Permettre une **synergie entre populations différentes** (experts, élus, dirigeants, TPME...).

Renforcer l'**émulsion collective**, en partant de problématiques partagées.

👉 Passer d'un Campus “prestataire” à un Campus **co-animé par l'écosystème**, impliqué, visible et fédérateur.



Structurer la Gouvernance





Hôtel de la Région 1 rue de la Loire
44 966 Nantes Cedex09