Dossier projet

ENTREZ DANS LA CYBERLIG

LE CAMPUS CYBER EN PAYS DE LA LOIRE

cyberlig@gigalis.fr – 28/05/2026 – V1.0

SOMMAIRE

Table des matières

RESUME EXECUTIF

RÉSUMÉ EXÉCUTIF

CYBERLIG – Un campus cyber pour les Pays de la Loire

La transformation numérique des organisations s'accompagne d'une augmentation continue des risques cyber. Les collectivités territoriales, les PME, les ETI, les établissements publics et les acteurs académiques des Pays de la Loire sont désormais exposés à des menaces systémiques pouvant affecter leur continuité d'activité, leur réputation et la sécurité des données sensibles.

Dans ce contexte, la cybersécurité constitue un enjeu stratégique de souveraineté, de compétitivité et de résilience territoriale.

En novembre et décembre 2025, une phase de réflexion associant 125 acteurs du territoire réunis lors de 9 ateliers thématiques, représentant six communautés (collectivités, entreprises, RSSI, ESN, enseignement supérieur, associations) a eu lieu.

Ces travaux ont permis de faire émerger 476 contributions structurantes, confirmant la nécessité d'un acteur régional neutre, fédérateur et opérationnel en matière de cybersécurité.

Le projet CYBERLIG vise à structurer et fédérer durablement l'écosystème régional de cybersécurité afin de renforcer la protection des organisations ligériennes et d'accompagner la montée en compétences des acteurs locaux.

Un ancrage territorial fort au service d'une stratégie nationale

CYBERLIG s'inscrit dans la dynamique portée par le campus cyber national et rejoint le réseau des campus cyber déployés sur l'ensemble du territoire national. Il constitue la déclinaison pour les Pays de la Loire d'une stratégie visant à structurer durablement la filière cybersécurité à l'échelle régionale.

Ce projet repose aussi sur une logique de proximité territoriale, condition essentielle pour réduire l'isolement des acteurs, favoriser la confiance et rendre la cybersécurité concrète et accessible aux organisations de toutes tailles.

Porté institutionnellement par la Région des Pays de la Loire, la Préfecture de Région, l'ANSSI et par le GIP Gigalis, opérateur public de services numériques des Pays de la Loire, CYBERLIG bénéficie d'un cadre de gouvernance équilibré, assurant coordination institutionnelle, stabilité et neutralité dans la mise en œuvre de ses missions.

Une ambition claire

CYBERLIG a pour objectifs de :

- créer des lieux et un réseau de référence en cybersécurité dans les Pays de la Loire ;
- soutenir le développement d'un environnement numérique plus sûr pour l'ensemble du territoire ;
- contribuer à la montée en compétences des acteurs locaux ;
- structurer un écosystème aujourd'hui fragmenté ;
- Être un tiers de confiance territorial et favoriser la coopération entre acteurs publics et privés.

CYBERLIG vise à fédérer entreprises, institutions, collectivités, monde académique et associations autour d'une stratégie commune de résilience numérique.

Une proposition de valeur différenciante au service de la résilience du territoire

Les ateliers de préfiguration ont confirmé que les freins à la cybersécurité sur le territoire ne sont pas principalement techniques, mais organisationnels et culturels : déficit d'acculturation des dirigeants, sous-évaluation du risque, manque de moyens, complexité perçue de l'écosystème et isolement des acteurs.

L'ensemble des communautés convergent vers un besoin commun : des solutions simples, mutualisées, accessibles et portées par un acteur neutre à l'échelle régionale.

CYBERLIG développera des outils mutualisés, des ressources clés en main, une mise en valeur des actions des communautés professionnelles actives et des dispositifs opérationnels (exercices de crise, retours d'expérience, espaces collaboratifs), répondant directement aux besoins exprimés lors des ateliers territoriaux.

Ainsi, CYBERLIG mettra en place un site internet centralisant l'offre cyber : répertoire des prestataires et éditeurs, catalogue des formations, agenda des événements, identification des clubs et réseaux professionnels. Cette plateforme apportera lisibilité, accessibilité et mise en relation dans un environnement aujourd'hui fragmenté.

Les adhérents bénéficieront de services mutualisés favorisant la coopération, la visibilité et l'intelligence collective. Les partenaires pourront valoriser leur expertise dans un cadre structuré et neutre.

Dans une logique d'intérêt général, CYBERLIG proposera également à l'ensemble des professionnels — adhérents ou non — un socle de services de premier niveau (sensibilisation, information, orientation) afin de renforcer la prise en compte des fondamentaux de cybersécurité sur tout le territoire.

Par cette approche à la fois structurante et inclusive, CYBERLIG se positionnera comme une référence territoriale de confiance en cybersécurité, plutôt qu'un prestataire supplémentaire.

Un modèle économique soutenable et collectif

Le modèle économique de CYBERLIG repose sur un financement diversifié et équilibré, combinant :

- les cotisations des adhérents ;
- des cotisations renforcées pour les partenaires ;
- des contributions issues du mécénat.

Cette structuration permet de mutualiser l'effort financier, de limiter la dépendance à des subventions publiques et de garantir l'indépendance stratégique de CYBERLIG.

Le développement du projet s'inscrira dans une trajectoire progressive sur quatre ans. La montée en puissance du nombre d'adhérents et de partenaires s'accompagnera d'un déploiement graduel des services proposés, afin d'assurer une cohérence entre les ressources disponibles et l'offre opérationnelle.

Durant cette phase de consolidation, certains moyens et fonctions — notamment les locaux, les services supports (RH, fonctions administratives) et une partie des équipements — seront mutualisés avec le GIP Gigalis. Cette organisation transitoire permettra :

- d'optimiser les coûts de structure ;
- de sécuriser le démarrage opérationnel ;
- de concentrer les investissements sur les actions à forte valeur ajoutée ;
- de réduire le risque financier lors de la phase de montée en puissance.

Cette approche pragmatique garantit une croissance maîtrisée et un équilibre financier durable. À horizon quatre ans, CYBERLIG vise l'atteinte d'un modèle stabilisé, fondé sur une base d'adhésion consolidée, une offre de services pleinement déployée et une autonomie organisationnelle progressive.

Un cadre de gouvernance garantissant neutralité et équilibre

CYBERLIG est attendu comme un tiers de confiance régional, capable de structurer l'écosystème, de réduire sa complexité et de favoriser la coopération sans logique concurrentielle.

CYBERLIG sera structuré sous la forme d'une association reposant sur une gouvernance collégiale représentative de l'ensemble de l'écosystème régional.

L'organisation s'articulera autour de collèges représentant les différentes communautés parties prenantes : entreprises, collectivités, adhérents, associations, professionnels de la cybersécurité, organismes de formation, partenaires, mécènes et les centres de ressources cyber départementaux, institutionnels, notamment le GIP Gigalis, la Région Pays de la Loire, la Préfecture de Région, et l'ANSSI.

Chaque collège disposera d'une représentation au sein du Conseil d'administration ainsi que le GIP Gigalis, la Région Pays de la Loire, la Préfecture de Région, et l'ANSSI, garantissant :

- une vision stratégique équilibrée ;
- la prise en compte des attentes de chaque communauté ;
- une gouvernance transparente ;
- une stricte neutralité dans les orientations et les actions de CYBERLIG.

Ce modèle collégial permettra d'assurer que CYBERLIG demeure un outil d'intérêt général au service du territoire, tout en préservant son indépendance vis-à-vis des intérêts particuliers.

Une opportunité stratégique pour les financeurs

Soutenir CYBERLIG, c'est contribuer à la structuration durable de la cybersécurité en Pays de la Loire et participer activement au renforcement de la résilience numérique dans un territoire de confiance.

Le projet répond à un enjeu d'intérêt général : sécuriser les collectivités, accompagner les PME et ETI, développer les compétences et renforcer l'attractivité économique régionale. En s'inscrivant dans la dynamique nationale des campus cyber, CYBERLIG offre aux financeurs l'opportunité d'associer leur engagement à une initiative structurante, visible et à fort impact territorial.

Pour les partenaires et mécènes, l'implication au sein de CYBERLIG constituera également un levier de valorisation institutionnelle et d'ancrage territorial, tout en contribuant concrètement à l'élévation du niveau de maturité cyber des organisations locales.

Investir dans CYBERLIG, c'est faire le choix d'un projet collectif, progressif et durable, conçu pour devenir à horizon quatre ans la plateforme régionale de référence en matière de cybersécurité

.

Chapitre 1

CONTEXTE ET ENJEUX TERRITORIAUX

CONTEXTE ET ENJEUX TERRITORIAUX

Une menace cyber devenue systémique

La transformation numérique des organisations s'est accélérée au cours des dernières années : dématérialisation des services publics, généralisation du télétravail, interconnexion des systèmes d'information, dépendance accrue aux prestataires numériques et aux services cloud.

Parallèlement, la menace cyber s'est intensifiée, industrialisée et professionnalisée. Les attaques par rançongiciel, les compromissions de comptes, les vols de données et les fraudes financières touchent désormais toutes les catégories d'organisations, indépendamment de leur taille ou de leur secteur d'activité.

L'émergence et la démocratisation des technologies d'intelligence artificielle transforment profondément le paysage cyber : elles représentent un levier puissant d'optimisation des défenses, mais offrent également aux acteurs malveillants des capacités augmentées d'industrialisation, d'adaptation et de contournement des dispositifs de sécurité.

À l'échelle nationale, l'ANSSI et le GIP Cybermalveillance.gouv.fr, constatent une augmentation continue des incidents affectant les collectivités territoriales, les établissements de santé, les PME et les opérateurs économiques stratégiques. La cybersécurité n'est plus un sujet réservé aux grandes entreprises ou aux infrastructures critiques : elle constitue un enjeu transversal de continuité d'activité et de souveraineté.

Dans ce contexte, la structuration territoriale de la réponse cyber devient un levier stratégique.

Un territoire économiquement dense et exposé

Les Pays de la Loire comptent environ **313 000 établissements actifs** et **1 228 communes**, représentant un tissu économique et institutionnel particulièrement diversifié. Ce maillage dense constitue un atout en matière de dynamisme économique, mais également un facteur d'exposition accru aux risques numériques.

Le territoire se caractérise par la présence de filières structurantes à forte valeur ajoutée et à forte exposition numérique :

- **industrie et aéronautique**, avec un écosystème industriel intégré et fortement numérisé ;
- **économie maritime et portuaire**, stratégique pour les chaînes logistiques et énergétiques ;
- **agroalimentaire**, secteur majeur de la région, fortement dépendant de la continuité de production et des systèmes industriels connectés ;
- **santé et établissements hospitaliers**, confrontés à des exigences croissantes de protection des données sensibles et de continuité des soins ;
- **tourisme et économie événementielle**, reposant largement sur des plateformes numériques, des systèmes de réservation et des flux de données ;

- **numérique et services**, notamment autour de la métropole nantaise.

Cette diversité constitue une force économique majeure, mais accroît également la surface d'exposition aux risques cyber. Les chaînes de valeur sont interconnectées, les systèmes industriels intègrent de plus en plus de technologies numériques (IT/OT), et les données deviennent un actif stratégique dans l'ensemble des secteurs.

Or nombre de ces structures — en particulier les PME, les établissements de santé ou les collectivités — ne disposent pas toujours des ressources internes nécessaires pour faire face à une menace en constante évolution.

Vulnérabilités spécifiques des PME et des collectivités

Les PME et ETI du territoire expriment des difficultés récurrentes :

- une sous-évaluation du risque cyber au niveau des dirigeants ;
- une vision encore majoritairement technique et IT du sujet ;
- un manque de priorisation stratégique ;
- des moyens humains et financiers limités ;
- une difficulté à identifier des solutions adaptées et proportionnées.

La cybersécurité est souvent perçue comme un centre de coût plutôt que comme un levier de résilience et de performance.

Les collectivités territoriales, notamment les plus petites structures, rencontrent des difficultés similaires :

- déficit d'acculturation des élus et des directions générales ;
- gouvernance floue entre DSI, directions métiers et prestataires ;
- absence de modèles opérationnels adaptés à leur taille ;
- difficulté à recruter ou à mutualiser des compétences spécialisées.

Dans les deux cas, la complexité perçue de l'écosystème cyber (référentiels multiples, dispositifs nationaux, offres variées, obligations réglementaires) renforce le sentiment d'isolement et d'impuissance.

Une complexification croissante du cadre réglementaire

Au-delà de l'évolution de la menace, les organisations doivent désormais faire face à un renforcement significatif du cadre réglementaire européen et national en matière de cybersécurité.

La directive européenne NIS2 (Network and Information Security), entrée en vigueur au niveau européen, élargit considérablement le périmètre des entités soumises à des obligations renforcées en matière de gestion des risques cyber, de continuité d'activité et de notification des incidents. Elle concerne désormais un nombre accru d'organisations, y compris des PME et ETI opérant dans des secteurs jugés essentiels ou importants.

En France, cette directive est en cours de transposition dans le cadre du projet de loi relatif à la «

résilience des infrastructures critiques et au renforcement de la cybersécurité », qui vise à adapter le droit national aux nouvelles exigences européennes et à renforcer les obligations pesant sur les acteurs publics et privés concernés.

Par ailleurs, le règlement européen relatif à la résilience cyber des produits numériques (Cyber Resilience Act) impose de nouvelles exigences aux fabricants et éditeurs de solutions numériques, notamment en matière de sécurité dès la conception et de gestion des vulnérabilités.

Ces évolutions réglementaires s'ajoutent à un environnement déjà structuré par le RGPD, des référentiels et les exigences sectorielles.

Pour les collectivités territoriales, les PME et les acteurs économiques du territoire, cette accumulation normative génère plusieurs difficultés :

- une compréhension partielle des obligations applicables ;
- une incertitude sur le périmètre exact de responsabilité ;
- une difficulté à prioriser les actions à mener ;
- un risque juridique et réputationnel accru en cas de non-conformité.

Les ateliers de préfiguration ont confirmé que cette complexité réglementaire renforce le besoin d'un accompagnement territorial structuré, capable de :

- traduire les exigences réglementaires en actions concrètes et proportionnées ;
- mutualiser les outils et référentiels ;
- clarifier les responsabilités ;
- offrir un cadre pédagogique accessible aux dirigeants.

Dans ce contexte, la structuration d'un campus cyber régional apparaît comme un levier stratégique pour accompagner les organisations ligériennes dans l'appropriation progressive de ces nouvelles exigences, tout en évitant une approche anxiogène ou disproportionnée.

Enseignements des ateliers de préfiguration

La phase de préfiguration du projet CYBERLIG a permis de réunir **125 acteurs du territoire lors de 9 ateliers**, représentant six communautés : collectivités, RSSI, entreprises de services numériques, établissements d'enseignement supérieur et de recherche, PME/ETI, associations et fédérations

Ces ateliers ont fait émerger **476 contributions**, structurées autour des irritants et des leviers d'action.

Les constats convergents sont clairs :

- les freins à la cybersécurité sont majoritairement organisationnels et culturels, plus que techniques ;
- le déficit d'acculturation des dirigeants et des élus constitue un obstacle majeur ;
- les organisations souffrent d'un manque de repères simples et opérationnels ;
- l'écosystème est perçu comme fragmenté et peu lisible ;
- l'isolement des acteurs, notamment des PME et petites collectivités, freine la montée en maturité.

Un message transversal ressort fortement : le territoire dispose déjà de nombreuses compétences, initiatives et offres, mais celles-ci sont dispersées, insuffisamment coordonnées et peu visibles.

Les participants n'expriment pas un besoin de création massive de nouveaux dispositifs, mais plutôt :

- de lisibilité ;
- de coordination ;
- de mutualisation ;
- de valorisation des expertises existantes ;
- de simplification des parcours et des points d'entrée.

Dans cette perspective, CYBERLIG n'aura pas vocation à se substituer aux acteurs existants ni à devenir un prestataire de services concurrentiel. Il est attendu comme un tiers de confiance régional, capable :

- d'agréger et de structurer l'offre existante ;
- de mettre en relation les besoins et les compétences ;
- de coordonner les initiatives ;
- de mutualiser certaines ressources ;
- et de créer un cadre de coopération durable entre les communautés.

La valeur ajoutée de CYBERLIG résidera ainsi moins dans la production directe de prestations que dans sa capacité à organiser, fédérer et rendre accessible un écosystème déjà riche mais encore fragmenté.

Un besoin de structuration territoriale

Les constats issus du contexte national, des évolutions réglementaires et des ateliers de préfiguration convergent vers un même diagnostic : le territoire ne souffre pas d'une absence d'acteurs ou d'initiatives en matière de cybersécurité, mais d'un manque de structuration, de lisibilité et de coordination.

Les compétences existent. Les expertises sont présentes. Les offres sont multiples. Cependant, elles demeurent dispersées, parfois méconnues, insuffisamment articulées entre elles et difficiles à appréhender pour les organisations, en particulier les PME, les collectivités de petite ou moyenne taille et les structures peu acculturées aux enjeux cyber.

Dans ce contexte, le besoin exprimé par les acteurs du territoire ne consiste pas à créer un prestataire supplémentaire ou à dupliquer des dispositifs existants, mais à :

- offrir un point d'entrée régional clair et identifiable ;
- rendre lisible l'écosystème cyber local ;
- mutualiser certaines ressources et bonnes pratiques ;
- faciliter la coopération entre acteurs publics, privés, académiques et associatifs ;
- accompagner la montée en maturité des dirigeants et décideurs.

Le rôle attendu de CYBERLIG est donc celui d'un tiers de confiance structurant, fédérateur et coordinateur, capable d'agréger et de valoriser les initiatives existantes sans logique de

substitution.

Afin d’assurer l’équilibre de son modèle économique, il pourra être envisagé, à la marge, la facturation de certains services spécifiques. Toutefois, ces prestations auront vocation à compléter et structurer l’offre existante, sans entrer en concurrence avec les prestataires du territoire. Elles s’inscriront dans une logique de mutualisation, d’animation et de mise en capacité, et non de substitution aux acteurs économiques locaux.

Il s’agit ainsi de transformer un écosystème riche mais fragmenté en un réseau organisé, coopératif et accessible, au service de la résilience numérique de l’ensemble du territoire.

Chapitre 2

VISION, MISSION ET AMBITION STRATÉGIQUE

VISION, MISSION ET AMBITION STRATÉGIQUE

Vision à trois ans

À horizon quatre ans, CYBERLIG ambitionnera de :

Renforcer collectivement la résilience numérique des acteurs des territoires ligériens, tout en générant un retour sur investissement concret pour ses membres et partenaires.

Renforcer la résilience numérique du territoire signifie :

- élever le niveau global de maturité cyber ;
- réduire l'isolement des acteurs ;
- favoriser la coopération interorganisationnelle ;
- fédérer les communautés existantes ;
- rendre la cybersécurité accessible, compréhensible et actionnable pour tous.

La cybersécurité représente aujourd'hui un coût subi lorsqu'elle est abordée de manière isolée. À l'inverse, une approche territoriale mutualisée permet de transformer cet enjeu en levier de performance, de confiance et d'attractivité.

La vision de CYBERLIG reposera sur cette logique :
faire de la résilience numérique un avantage compétitif et un facteur de sécurisation durable du tissu économique et institutionnel régional.

Une mission structurante : fédérer, structurer, rendre lisible

La mission de CYBERLIG sera d'être l'acteur régional de référence pour dynamiser la résilience cyber des acteurs économiques et publics des Pays de la Loire.

Pour cela, CYBERLIG aura vocation à :

- structurer et cartographier l'écosystème régional afin de savoir rapidement « qui fait quoi » ;
- faciliter les mises en relation entre acteurs publics, privés, talents et projets ;
- agréger les initiatives existantes et éviter les doublons ;
- donner de la visibilité aux démarches locales et régionales ;
- renforcer la coopération entre communautés ;
- rendre la cybersécurité accessible à toutes les organisations, quel que soit leur taille ou leur niveau de maturité.

CYBERLIG ne se positionnera pas comme un prestataire supplémentaire, mais comme un agrégateur et un facilitateur régional, au service de l'intérêt général et en complémentarité avec les dispositifs existants.

Un retour sur investissement pour chaque catégorie d'acteurs

La participation à CYBERLIG reposera sur un principe fondamental : chaque catégorie d'acteurs — qu'elle soit adhérente ou non — doit retirer une valeur identifiable de son existence.

Pour les professionnels non adhérents (socle de services accessibles à tous)

Dans une logique d'intérêt général, CYBERLIG proposera un socle de services de premier niveau accessible à l'ensemble des professionnels du territoire, qu'ils soient adhérents ou non.

Ce socle comprendra notamment :

- une assistance de premier niveau en cas d'incident (Pays de la Loire Cyber Assistance – CSIRT régional) ;
- un diagnostic initial de maturité ou d'exposition au risque (CyberDépart), ainsi qu'un point de suivi 6 mois plus tard ;
- des actions de sensibilisation et d'acculturation accessibles ;
- une orientation vers les dispositifs et prestataires adaptés ;
- des exercices de crise interentités
- une banque de ressources.

Le retour sur investissement pour ces acteurs se traduira par :

- une réduction immédiate de l'isolement face à un incident ;
- un accès simplifié à des repères fiables ;
- une première montée en maturité sans barrière financière ;
- une amélioration de la capacité de réaction en cas de crise.

Cette approche contribuera à élever le niveau minimal de résilience cyber sur l'ensemble du territoire.

Pour les adhérents

Les adhérents bénéficieront de services mutualisés et d'un accès renforcé à l'écosystème régional :

- mise en relation structurée avec partenaires et experts pour un accompagnement de premier niveau pour la mise en œuvre des réglementations liées à NIS et au CRA ;
- accès privilégié à une veille sur la menace régionalisée ;
- bénéficier d'aide dans le cadre d'une charte de solidarité ;
- participation à des groupes de travail et retours d'expérience.

Le retour sur investissement se mesurera par :

- une réduction du risque cyber ;
- un gain de temps et de lisibilité ;
- un accès facilité aux compétences ;
- une montée en maturité organisationnelle.

Pour les partenaires

Les partenaires bénéficieront :

- d'une visibilité accrue ;
- d'un positionnement comme acteur structurant de l'écosystème ;
- d'opportunités de mise en relation qualifiée ;
- d'un environnement territorial plus mature et structuré.

Le retour sur investissement s'exprimera en notoriété, développement d'opportunités, ancrage territorial et contribution à la structuration du marché régional.

Pour les mécènes

Les mécènes contribueront à un projet stratégique d'intérêt général, participant directement à la sécurisation du tissu économique et institutionnel régional.

Le retour sur investissement se traduira par :

- une valorisation institutionnelle et territoriale ;
- une image d'engagement en faveur de la résilience numérique ;
- une contribution mesurable à la stabilité économique régionale ;
- un alignement avec les priorités nationales et européennes en matière de cybersécurité.

Une ambition collective et contributive

CYBERLIG reposera sur un modèle collaboratif. Les utilisateurs de la structure ne seront pas uniquement des bénéficiaires de services, mais des contributeurs à la dynamique collective.

Chaque communauté — entreprises, collectivités, RSSI, établissements d'enseignement supérieur, associations, entreprises de services numériques — participera à la création de valeur commune par :

- le partage d'expériences et de bonnes pratiques ;
- la mutualisation de ressources ;
- la mise en lumière de démarches réussies ;
- l'animation de groupes de travail et d'événements.

Cette approche permettra de proposer une valeur spécifique à chaque communauté tout en renforçant la cohérence d'ensemble du territoire.

Des valeurs fondatrices au service du territoire

L'action de CYBERLIG s'appuiera sur des valeurs structurantes :

- **création de valeur** : chaque action devra produire un impact concret et mesurable pour les acteurs du territoire ;
- **neutralité** : garantir un positionnement équilibré, non concurrentiel et indépendant des intérêts particuliers ;
- **entraide et partage** : favoriser la coopération et la diffusion des bonnes pratiques ;
- **confiance** : créer un cadre sécurisé permettant l'échange d'informations et de retours d'expérience ;
- **pédagogie** : Adopter un discours adapté aux non-spécialistes, avec une logique d'acculturation et de montée en maturité progressive ;
- **complémentarité** : s'inscrire en cohérence avec les dispositifs existants, sans duplication ;
- **proximité territoriale** : agir au plus près des acteurs locaux ;
- **accessibilité** : proposer des événements régionaux accessibles à tous, y compris en visioconférence, afin de garantir l'inclusion et l'équité territoriale.

Une ambition stratégique régionale

À travers cette vision et cette mission, CYBERLIG visera à devenir :

- le point d'entrée régional de référence en matière de cybersécurité ;
- un catalyseur de coopération public-privé ;
- un amplificateur des initiatives locales ;
- un levier d'attractivité et de montée en compétences pour les Pays de la Loire.

L'ambition ne sera pas uniquement de répondre aux enjeux actuels, mais de structurer durablement un écosystème capable d'anticiper les évolutions technologiques, réglementaires et économiques.

Chapitre 3

POSITIONNEMENT DANS L'ÉCOSYSTEME NATIONAL ET RÉGIONAL

POSITIONNEMENT DANS L'ÉCOSYSTÈME NATIONAL ET RÉGIONAL

Une intégration active au réseau des Campus Cyber régionaux

CYBERLIG s'inscrira pleinement dans le réseau des campus cyber régionaux déployés sur le territoire national, en articulation avec le Campus Cyber National.

L'objectif sera double :

- bénéficier des retours d'expérience, outils et travaux déjà réalisés par les autres campus ;
- contribuer aux échanges interrégionaux et à la mutualisation des bonnes pratiques.

Dans cette logique, CYBERLIG veillera à identifier et à déployer, lorsque cela est pertinent, des services déjà expérimentés avec succès dans d'autres régions. Cette approche permettra :

- d'accélérer la montée en puissance de CYBERLIG ;
- de s'appuyer sur des dispositifs éprouvés ;
- d'optimiser les ressources ;
- de réduire les risques liés à l'expérimentation.

Les groupes de travail mis en place au sein de CYBERLIG seront définis en tenant compte des initiatives déjà engagées dans d'autres territoires, afin d'éviter les redondances et de concentrer les efforts sur des thématiques à forte valeur ajoutée pour les Pays de la Loire.

Cette intégration active au réseau national garantira cohérence stratégique, efficacité opérationnelle et capacité d'innovation partagée.

Une coopération structurée avec les associations professionnelles et réseaux d'experts

CYBERLIG développera des partenariats avec les associations nationales et régionales d'experts en cybersécurité, telle que le CESIN ou le CLUSIR, ainsi qu'avec les associations du numérique comme ADN Ouest.

L'objectif est de :

- valoriser les actions déjà portées par ces structures ;
- coordonner les calendriers d'événements ;
- éviter les doublons en matière de sensibilisation ou de groupes de travail ;
- renforcer la visibilité collective de l'écosystème régional.

CYBERLIG se positionne ainsi comme amplificateur et fédérateur, et non comme acteur concurrent.

Un partenariat avec les fédérations professionnelles

Des coopérations seront également développées avec les fédérations et réseaux professionnels tels que le MEDEF, la CPME, le Club des ETI ou encore l'Association des Maires de France.

L'objectif sera de permettre à CYBERLIG d'apporter une contribution d'expertise auprès des adhérents de ces organisations, notamment en matière :

- d'acculturation des dirigeants aux enjeux cyber ;
- de sensibilisation aux évolutions réglementaires (NIS2, Cyber Resilience Act, etc.) ;
- d'identification des risques opérationnels et stratégiques ;
- d'orientation vers des solutions adaptées et proportionnées.

CYBERLIG jouera également un rôle de mise en valeur des dispositifs d'accompagnement existants, qu'ils soient gratuits ou subventionnés, afin de faciliter leur mobilisation par les entreprises et les collectivités. Il s'agira notamment :

- d'identifier les aides financières disponibles pour renforcer la cybersécurité ;
- de valoriser les dispositifs publics d'accompagnement ;
- d'orienter vers les programmes de diagnostic ou de soutien existants ;
- de simplifier l'accès à ces mécanismes souvent méconnus.

Ce positionnement permettra d'accroître l'impact des politiques publiques et des dispositifs d'aide existants, tout en apportant une valeur concrète et immédiate aux adhérents des fédérations professionnelles.

Une coopération étroite avec les pouvoirs publics

CYBERLIG travaillera en lien avec les autorités et acteurs publics impliqués dans la cybersécurité, notamment l'ANSSI et autres services de l'État.

Cette coopération visera à :

- relayer les messages institutionnels de prévention ;
- faciliter la circulation d'informations en cas d'incident ;
- contribuer à la cohérence territoriale des dispositifs de sensibilisation ;
- renforcer la coordination entre sphère publique et acteurs économiques.

Un lien structurant avec les établissements de formation

Un dialogue permanent sera entretenu avec les établissements d'enseignement supérieur et écoles formant aux métiers du numérique et de la cybersécurité.

L'objectif sera de :

- renforcer la visibilité des parcours existants ;
- favoriser les passerelles entre formation et besoins des entreprises ;
- contribuer à la rétention des talents sur le territoire.

CYBERLIG jouera ainsi un rôle de facilitateur entre monde académique et tissu économique.

Un ancrage territorial au plus près des acteurs

Afin d'assurer une proximité effective avec l'ensemble des territoires ligériens, CYBERLIG mettra en place des déclinaisons ou antennes locales dans chaque département des Pays de la Loire.

Ces implantations territoriales n'auront pas vocation à reproduire un modèle unique. Elles pourront prendre des formes adaptées aux spécificités et à la maturité de chaque écosystème local, telles que :

- un collectif d'acteurs cyber départemental ;
- un centre de ressources cyber mutualisé ;
- un réseau d'ambassadeurs ou de référents territoriaux ;
- des groupes de travail ou clubs locaux thématiques ;
- un lieu d'animation ou d'événements ponctuels.

L'objectif sera que chaque déclinaison locale soit construite en cohérence avec les dynamiques existantes, les besoins identifiés et les forces déjà présentes sur le territoire concerné.

Cette approche différenciée permettra :

- d'éviter la duplication de structures existantes ;
- de valoriser les initiatives locales ;
- de renforcer la confiance par la proximité ;
- d'adapter les actions aux réalités économiques et institutionnelles de chaque département.

Ce maillage territorial constituera un élément différenciant fort de CYBERLIG, garantissant une résilience numérique pensée à la fois à l'échelle régionale et au plus près des acteurs locaux.

Chapitre 4

MODÈLE DE SERVICES ET MODALITÉS D'ACCÈS

MODÈLE DE SERVICES ET MODALITÉS D'ACCÈS

Un accès aux services structuré selon le niveau d'engagement

L'offre de services de CYBERLIG reposera sur un principe de différenciation fondé sur la qualité et le niveau d'engagement des acteurs au sein de la structure.

Voici les catégories de bénéficiaires à ce jour identifiées :

- les professionnels (entreprises, collectivités, indépendants, tous secteurs, hors grand public) ;
- les adhérents ;
- les partenaires ;
- les mécènes ;
- les associations et fédérations ;
- les services de l'État.

L'accès aux services sera organisé selon une matrice claire distinguant :

- **les services ouverts**, accessibles gratuitement à l'ensemble des professionnels ;
- **les services à valeur ajoutée**, gratuits pour les adhérents mais facturés aux non-adhérents ;
- **les groupes de travail**, réservés aux membres engagés et animés par les partenaires.

Cette structuration permettra :

- de garantir un socle d'intérêt général accessible à tous ;
- de valoriser l'adhésion par des services à plus forte valeur ajoutée ;
- d'impliquer les partenaires dans l'animation opérationnelle ;
- d'assurer la soutenabilité économique du modèle.

Un socle de services ouverts au service de l'intérêt général

CYBERLIG proposera un ensemble de services ouverts, gratuits et accessibles à l'ensemble des professionnels du territoire — entreprises, collectivités, indépendants — dans une logique d'intérêt général et de montée en maturité collective.

Ce socle constituera le premier niveau d'accompagnement et vise à renforcer la résilience minimale de l'ensemble de l'écosystème régional.

Il comprendra notamment :

- **un annuaire régional structuré**, recensant les événements, prestataires, clubs professionnels, formations et dispositifs d'accompagnement existants, afin de faciliter l'identification rapide des ressources adaptées et de rendre l'écosystème plus lisible ;
- **des actions de sensibilisation et d'acculturation**, destinées aux dirigeants, élus et équipes opérationnelles, visant à rendre la cybersécurité compréhensible, accessible et proportionnée

aux réalités des organisations ;

- **un diagnostic cyber de premier niveau (CyberDépart)**, permettant aux structures de disposer d'une première évaluation de leur niveau de maturité ou d'exposition au risque, et d'identifier les priorités d'action. Il sera possible pour le bénéficiaire de faire un point d'étape 6 mois plus tard ;
- **une information en cas d'alerte ou d'incident (**Pays de la Loire Cyber Assistance), contribuant à diffuser rapidement les messages de prévention, les bonnes pratiques et les orientations vers les dispositifs compétents ;
- **des exercices de crise cyber interstructures** sensibilisant à la nécessité de se préparer à une attaque cyber et aux bienfaits de ce type d'exercice ;
- **une banque de ressources** regroupant des documents modèles (PSSI, charge...) qui sont la base de l'organisation documentaire des démarches de cybersécurité.

Ce socle ouvert répondra directement aux besoins exprimés lors des ateliers de préfiguration : disposer de repères simples, accessibles et non anxiogènes, permettant d'agir sans complexité excessive.

Pour les mécènes, le financement de ce socle ouvert représentera un levier d'impact territorial concret et mesurable. Il permet :

- de soutenir un dispositif bénéficiant à l'ensemble du tissu économique et institutionnel ;
- de contribuer à la sécurisation des chaînes de valeur régionales ;
- d'associer leur image à une démarche d'intérêt général favorisant la résilience numérique collective.

Ainsi, les services ouverts constitueront à la fois un outil de prévention à large échelle et un vecteur de valorisation pour les acteurs engagés dans le soutien de CYBERLIG.

Des services à valeur ajoutée pour les adhérents et partenaires

L'adhésion à CYBERLIG ouvrira l'accès à des services augmentés et à des dispositifs à plus forte valeur stratégique.

Ces services apporteront un retour sur investissement renforcé :

- accès privilégié aux groupes de travail ;
- participation active à la gouvernance ;
- ressources mutualisées réservées ;
- visibilité accrue au sein de l'écosystème.

Les partenaires joueront un rôle clé dans l'animation de ces services : ils interviendront dans les groupes de travail, contribueront aux événements et pourront fournir certains services spécialisés dans un cadre structuré et non concurrentiel.

Ainsi, la valeur apportée sera différenciée selon le niveau d'engagement, tout en maintenant un équilibre entre intérêt général et modèle économique.

Une montée en puissance progressive des services

L’offre de services de CYBERLIG sera déployée de manière progressive, en cohérence avec les ressources disponibles et la montée en puissance du modèle économique. Cette trajectoire vise à garantir un haut niveau de qualité dans la délivrance des services, tout en maîtrisant les charges et en sécurisant le démarrage opérationnel.

Phase 1 – Lancement : sensibilisation, accompagnement et premiers groupes de travail prioritaires

Dès le lancement, au-delà du socle de services ouverts, CYBERLIG concentrera ses actions sur des thématiques prioritaires, traitées sous forme de sensibilisation, d’accompagnement et de groupes de travail, afin de répondre rapidement aux besoins les plus structurants du territoire :

- **prise en compte de la réglementation** (notamment NIS2 et Cyber Resilience Act), pour aider les organisations à comprendre les impacts, clarifier les obligations et identifier des trajectoires de mise en conformité proportionnées ;
- **gestion de crise cyber**, afin de renforcer la capacité de préparation et de réaction des organisations, via des contenus pédagogiques, des retours d’expérience et des exercices adaptés aux réalités des PME, ETI et collectivités ;
- **sécurisation de la chaîne de sous-traitance**, enjeu majeur pour la continuité d’activité, visant à diffuser des pratiques simples de maîtrise des risques fournisseurs et à renforcer la confiance dans les écosystèmes numériques.

Phase 2 – Consolidation : élargissement progressif de l’offre

Dans une seconde phase, à mesure que les ressources humaines et financières se consolideront, CYBERLIG développera de nouveaux services et formats (outils mutualisés, dispositifs d’accompagnement renforcés, événements à plus forte intensité opérationnelle), en cohérence avec les retours d’usage et les besoins exprimés par les communautés.

Cette montée en puissance progressive garantit :

- une cohérence entre ambition et capacité opérationnelle ;
- une trajectoire financière maîtrisée ;
- un déploiement guidé par l’impact et les besoins réels du territoire.

Chapitre 5

OFFRE DE SERVICES DETAILLÉE

OFFRE DE SERVICES DETAILLÉE

L'offre de services de CYBERLIG vise à répondre aux besoins exprimés par les acteurs du territoire en combinant intérêt général, montée en maturité collective et création de valeur pour les membres engagés.

Elle s'articule autour :

- d'un socle accessible à tous les professionnels ;
- de services à valeur ajoutée pour les membres ;
- de dispositifs spécialisés en complémentarité avec les partenaires.

Un socle d'intérêt général accessible à tous

Annuaire régional et cartographie de l'écosystème

Plateforme numérique recensant :

- calendrier des événements cyber sur la région ;
- les clubs et réseaux ayant une thématique cyber ;
- les prestataires et éditeurs cyber ayant un site sur la région ;
- les formations cyber sur la région ;
- les dispositifs d'accompagnement et aides disponibles.

Proposition de valeur :

- lisibilité accrue de l'écosystème régional ;
- réduction du temps de recherche pour les organisations ;
- mise en relation facilitée ;
- visibilité renforcée pour les acteurs référencés ;
- impact territorial large pour les mécènes.

Sensibilisation et acculturation (NIS2, CRA, enjeux cyber)

Organisation de sensibilisations sur l'ensemble du territoire, animés en partenariat avec les centres de ressources cyber, des experts partenaires et les services de l'État.

Proposition de valeur :

- acculturation des dirigeants et élus ;
- anticipation des obligations réglementaires ;
- positionnement des partenaires comme contributeurs experts.

Diagnostic cyber de premier niveau

CYBERLIG facilitera l'accès au dispositif **CyberDépart**, porté par l'ANSSI, qui permet aux organisations de bénéficier d'un premier niveau d'évaluation de leur exposition aux risques cyber.

CYBERLIG assurera :

- la promotion active du dispositif sur le territoire ;
- la facilitation de l'inscription et de l'orientation des structures ;
- l'accompagnement dans l'interprétation des premiers résultats ;
- la mise en relation avec des acteurs compétents pour les étapes suivantes.

Les partenaires ou adhérents de CYBERLIG pourront, lorsqu'ils remplissent les conditions requises, devenir « aidants » dans le cadre du dispositif CyberDépart, contribuant ainsi à son déploiement territorial.

Proposition de valeur :

- accès simplifié à un dispositif national reconnu ;
- première évaluation structurée sans complexité excessive ;
- orientation claire vers les priorités d'action ;
- renforcement du rôle du territoire dans la diffusion d'un dispositif d'État ;
- opportunité pour les partenaires de s'inscrire dans une dynamique nationale tout en contribuant localement.

Point de suivi CyberDépart

CYBERLIG permettra aux bénéficiaires du diagnostic **CyberDépart** de réaliser, s'il le souhaite, d'un point de suivi 6 mois après leur diagnostic.

CYBERLIG assurera :

- la proposition de diagnostic auprès des bénéficiaires ;
- la mise en relation avec un aidant ;

Information et appui en cas d'alerte ou d'incident

CYBERLIG facilitera l'accès au dispositif **Pays de la Loire Cyber Assistance**, centre régional de réponse aux incidents de sécurité informatique et de cyberattaques soutenu par l'ANSSI et porté par Gigalis. Ce service existe déjà et constitue une offre opérationnelle de premier niveau pour aider les organisations victimes de cyberattaques ou confrontées à un incident informatique.

Pays de la Loire Cyber Assistance s'adresse aux associations, PME, ETI et collectivités territoriales intermédiaires ayant un établissement dans la région. Il comprend notamment :

- des interventions d'urgence en cas de cyberattaque ;
- la mise en relation 24h/24 et 7j/7 avec des prestataires labellisés pour une assistance rapide ;
- des actions de sensibilisation et de prévention ;
- la diffusion des recommandations de l'ANSSI et de Cybermalveillance.gouv.fr.

CYBERLIG s'assurera que les organisations régionales identifient facilement ce service, en

facilitera la promotion et l'orientation des structures vers ce dispositif, et pourra encourager ses partenaires et adhérents à devenir des relais ou aidants pour orienter les victimes vers l'assistance adaptée.

Proposition de valeur :

- mise à disposition d'un dispositif opérationnel déjà existant et reconnu ;
- réduction immédiate de l'isolement en cas d'incident grave ;
- accès structuré à une assistance 24/7, avec mise en relation vers des prestataires compétents ;
- augmentation de la résilience numérique collective du territoire ;
- visibilité positive pour les mécènes de CYBERLIG, car leur soutien contribue à un service de protection concret et accessible à tous.

Exercice de crise inter-structure

CYBERLIG organisera des exercices de gestion de crise cyber interstructures, inspirés de l'exercice national Rempar25 conduit par l'ANSSI, et s'appuyant sur le kit méthodologique en cours de conception par le Campus Cyber National.

Ces exercices permettront à des professionnels de diverses structures (entreprises, collectivités, établissements publics) de se confronter à un scénario de crise cyber simulée et de tester collectivement :

- les dispositifs nécessaires à la de gestion de crise ;
- la coordination interne (direction, IT, communication, juridique) ;
- les mécanismes de décision ;
- l'articulation avec les partenaires et autorités compétentes.

Un réseau régional d'animateurs sera constitué à partir de professionnels volontaires, de collaborateurs issus des partenaires ou des mécènes de CYBERLIG. Formés à l'utilisation du kit national, ils contribueront à diffuser une culture opérationnelle de gestion de crise sur l'ensemble du territoire.

Proposition de valeur :

- sensibiliser concrètement les dirigeants à l'ampleur et à la réalité d'une crise cyber ;
- mettre en évidence les écarts entre procédures théoriques et capacité réelle de réaction ;
- développer des réflexes collectifs et une culture de préparation ;
- réduire le temps de réaction en cas d'attaque réelle ;
- renforcer la coopération territoriale face à un incident majeur.

Participer à ce type d'exercice constituera un levier puissant d'acculturation et de préparation : l'expérience immersive permettra de transformer la perception du risque en action concrète.

Banque de ressources mutualisées

La création d'une banque de ressources mutualisées répondra directement à une demande forte exprimée lors des ateliers de préfiguration : mettre en commun un certain nombre de documents structurants afin d'éviter que chaque organisation ne produise isolément les mêmes livrables.

Les participants ont notamment souligné le besoin de disposer de modèles opérationnels et pragmatiques, adaptés aux réalités des PME et des collectivités.

Cette banque de ressources comprendra notamment :

- des modèles de politique de sécurité des systèmes d'information (PSSI) ;
- des stratégies cyber simplifiées ;
- des chartes utilisateurs ;
- des clauses contractuelles types (notamment en matière de sous-traitance) ;
- des trames de gestion de crise ;
- des supports de sensibilisation.

Ces documents seront produits, enrichis et validés dans le cadre des groupes de travail de CYBERLIG, garantissant leur pertinence et leur adaptation au contexte régional.

Proposition de valeur :

- mutualisation des efforts et réduction des coûts de production documentaire ;
- accès à des modèles éprouvés et validés collectivement ;
- accélération de la mise en conformité et de la structuration interne ;
- harmonisation des pratiques à l'échelle régionale ;
- réponse concrète aux besoins exprimés par les acteurs lors de la phase de préfiguration.

Ce service incarnera pleinement la logique collaborative et contributive de CYBERLIG : transformer une demande partagée en ressource collective au bénéfice de l'ensemble du territoire.

Des services à valeur ajoutée pour les membres engagés

Parcours consulting réglementaire (NIS2 / CRA)

CYBERLIG proposera un dispositif de **parcours consulting réglementaire**, inspiré du principe du permettant aux organisations d'échanger de manière ciblée avec des experts sur les enjeux liés à la directive NIS2 et au Cyber Resilience Act (CRA).

Le format reposera sur 4 créneaux d'une heure durant lesquels une organisation adhérente pourra poser des questions précises et obtenir un premier éclairage sur :

- ses obligations réglementaires et les impacts juridiques ;
- les implications organisationnelles ;
- les exigences techniques ;
- les enjeux liés à la sous-traitance et aux fournisseurs.

Les experts mobilisés (partenaires de CYBERLIG) pourront être :

- des juristes spécialisés en réglementation cyber ;
- des consultants en organisation et gouvernance ;
- des experts techniques ou RSSI expérimentés.

Ces sessions seront organisées régulièrement et déployées sur l'ensemble des territoires ligériens,

afin de garantir une proximité géographique et une accessibilité équitable.

Proposition de valeur :

- accès rapide et simplifié à une expertise qualifiée ;
- clarification immédiate d'un point bloquant ;
- réduction du risque de mauvaise interprétation réglementaire ;
- aide à la priorisation des actions ;
- format accessible et peu engageant, facilitant la prise de décision.

Ce dispositif permettra de rendre la réglementation compréhensible et actionnable auprès des adhérents, sans imposer d'audit lourd ou d'engagement financier disproportionné.

Observatoire régional de la menace

La création d'un observatoire régional de la menace cyber répondra à une demande explicite formulée lors des ateliers de préfiguration : disposer d'une vision territoriale consolidée des incidents, des tendances et des vulnérabilités affectant les organisations ligériennes.

Cet observatoire se matérialisera par plusieurs dispositifs complémentaires :

Newsletter régionale

Diffusion régulière d'une newsletter dédiée :

- aux attaques cyber rencontrées par des organismes de la région (avec anonymisation systématique) ;
- aux vulnérabilités observées ;
- aux retours d'expérience partagés ;
- à l'actualité cyber régionale (événements, initiatives partenaires, évolutions réglementaires).

La newsletter sera alimentée notamment par **Pays de la Loire Cyber Assistance**, dispositif régional d'appui en cas d'incident, ainsi que par les partenaires de CYBERLIG, qui pourront contribuer à la diffusion d'analyses, de retours d'expérience ou de signaux faibles observés sur le territoire.

L'objectif sera de contextualiser la menace au niveau régional, afin de rendre le risque plus concret, plus proche et plus actionnable pour les organisations locales.

Système d'alerte ciblé

Les adhérents de CYBERLIG pourront bénéficier d'une information spécifique en cas d'alerte majeure, notamment lors de la découverte d'une vulnérabilité critique ou d'une campagne d'attaque significative.

Ce dispositif visera à renforcer la capacité d'anticipation et de réaction des organisations engagées dans la démarche de CYBERLIG.

Enquête annuelle régionale

Une enquête régionale sera conduite chaque année afin de :

- mesurer l'évolution de la menace sur le territoire ;

- identifier les typologies d'incidents rencontrés ;
- analyser les impacts organisationnels et économiques ;
- produire des indicateurs (nombre de structures victimes, types d'attaques, délais de détection, etc.).

Les résultats feront l'objet d'une restitution synthétique permettant d'objectiver la réalité de la menace et d'orienter les priorités d'action de CYBERLIG.

Proposition de valeur :

- transformation d'une menace abstraite en réalité territoriale mesurable ;
- aide à la priorisation des investissements cyber ;
- renforcement de la culture du retour d'expérience ;
- source d'information fiable, contextualisée et neutre ;
- production d'indicateurs utiles pour les décideurs publics et économiques ;
- valorisation de l'impact territorial de CYBERLIG auprès des mécènes et partenaires.

Groupes de travail thématiques

Les groupes de travail constitueront un pilier structurant de l'action de CYBERLIG. Ils ont vocation à produire des livrables concrets et opérationnels répondant aux besoins identifiés par les acteurs du territoire.

Les thématiques abordées seront définies dans le cadre de la gouvernance de la structure, en cohérence avec les priorités stratégiques régionales. Les premiers thèmes ont émergé lors des ateliers de préfiguration et portent notamment sur :

- la prise en compte des évolutions réglementaires (NIS2, CRA) ;
- la gestion de crise cyber ;
- la sécurisation de la chaîne de sous-traitance ;
- l'organisation et la gouvernance de la cybersécurité.

Modalités de fonctionnement

Afin de garantir une production saine, indépendante de toute arrière-pensée commerciale, les groupes de travail seront ouverts exclusivement aux adhérents qui ne sont pas des entreprises de services numériques.

Ce choix vise à :

- favoriser l'expression libre des besoins ;
- éviter toute logique de prospection commerciale ;
- garantir un climat de confiance et de coopération.

Les partenaires pourront toutefois :

- animer les groupes de travail ;
- accueillir les réunions ;
- apporter leur expertise technique ou réglementaire.

CYBERLIG se portera garant de la neutralité des échanges et veillera à ce que les interventions

des partenaires s'inscrivent dans une logique d'intérêt collectif et non promotionnelle.

Production et diffusion des livrables

Les groupes de travail auront pour objectif de produire :

- des synthèses ;
- des recommandations pratiques ;
- des modèles ou trames documentaires ;
- des retours d'expérience anonymisés.

Une partie de ces productions (synthèses, recommandations générales) sera mise à disposition de l'ensemble des professionnels du territoire afin de contribuer à l'intérêt général.

Les documents les plus détaillés ou opérationnels seront réservés aux adhérents, constituant ainsi un levier de valeur ajoutée et un bénéfice concret lié à l'engagement au sein de la structure.

Proposition de valeur :

- Intelligence collective territoriale structurée ;
- Production de livrables adaptés aux réalités locales ;
- Garantie de neutralité et d'absence de démarchage commercial ;
- Mutualisation des réflexions et des outils ;
- Création d'un espace de confiance entre pairs ;
- Diffusion élargie des bonnes pratiques au bénéfice du territoire.

Analyses technologiques et ateliers pratiques

Ce service complètera les groupes de travail en proposant un format plus descendant, centré sur le partage d'expertise et la diffusion de connaissances techniques ou organisationnelles.

Il s'agira d'ateliers animés par :

- des partenaires de CYBERLIG disposant d'une expertise reconnue ;
- ou des experts nationaux invités pour partager leur analyse sur une thématique spécifique.

Les sujets pourront notamment porter sur :

- les évolutions technologiques (intelligence artificielle appliquée à la cybersécurité, segmentation réseau, durcissement des systèmes, etc.) ;
- les bonnes pratiques opérationnelles (PCA/PRA, gestion des vulnérabilités, sécurisation des environnements cloud) ;
- les retours d'expérience sur des incidents ou projets structurants.

Ces ateliers auront pour objectif de :

- éclairer les adhérents sur des enjeux émergents ;
- vulgariser des sujets techniques complexes ;
- permettre aux décideurs de mieux comprendre les implications stratégiques et opérationnelles ;
- accélérer la montée en compétences des équipes.

Un effort particulier sera porté sur la couverture territoriale : ces ateliers seront organisés sur l'ensemble des départements ligériens afin de garantir un accès équitable et une proximité réelle avec les acteurs locaux.

CYBERLIG veillera à la neutralité des contenus présentés et à l'absence de promotion commerciale directe.

Solidarité entre adhérents en cas d'attaque

En accord avec Nantes Métropole, une version adaptée de leur charte de solidarité pourra être proposée aux adhérents du Campus Cyber

Chapitre 6

GOUVERNANCE ET GARANTIES DE NEUTRALITÉ

GOUVERNANCE ET GARANTIES DE NEUTRALITÉ

La gouvernance de CYBERLIG sera conçue pour garantir un équilibre durable entre les différentes parties prenantes, assurer la neutralité des actions menées et préserver l'intérêt général du projet.

Elle reposera sur une organisation collégiale, une représentation équilibrée au sein du conseil d'administration et la mise en place de mécanismes spécifiques de prévention des conflits d'intérêts.

Une organisation en collèges représentatifs

Afin d'assurer une représentation équilibrée des parties prenantes, CYBERLIG sera structuré en quatre collèges :

Collège des adhérents

Ce collège regroupera des représentants des six communautés identifiées dans le projet :

- entreprises ;
- collectivités ;
- établissements académiques ;
- associations ;
- professionnels de la cybersécurité ;
- entreprises de services numériques.

Il garantira que les bénéficiaires directs des services participent activement à l'orientation stratégique de CYBERLIG.

Collège des partenaires

Ce collège rassemblera les partenaires contribuant à l'animation, à l'expertise et au développement des services de CYBERLIG.

Il permettra d'associer les acteurs économiques spécialisés dans un cadre structuré, tout en préservant la neutralité du dispositif.

Collège des mécènes

Ce collège réunira les représentants des organisations apportant un soutien financier au projet dans une logique d'intérêt général.

Il garantira une visibilité institutionnelle aux mécènes tout en maintenant une séparation claire entre financement et orientation opérationnelle.

Collège des centres de ressources cyber

Ce collège regroupera des représentants des centres de ressources cyber déployés dans chaque département des Pays de la Loire.

Ces centres constitueront les déclinaisons territoriales de CYBERLIG. Leur organisation et leur statut pourront varier selon les spécificités locales (collectif d'acteurs, dispositif porté par une structure existante, centre mutualisé, etc.).

Ils auront pour missions principales :

- de valoriser et déployer localement les services de la structure ;
- d'assurer un relais de proximité auprès des acteurs économiques et publics ;
- d'animer la dynamique cyber à l'échelle départementale.

Ils pourront également conduire leurs propres actions, telles que :

- des groupes de travail locaux ;
- des ateliers thématiques ;
- des actions de sensibilisation adaptées aux besoins du territoire.

Les productions et travaux réalisés au niveau départemental seront mutualisés et mis à disposition des autres centres de ressources cyber, contribuant ainsi à une dynamique régionale coordonnée et à un partage structuré des bonnes pratiques.

Un Conseil d'Administration garant de l'intérêt général

Le Conseil d'Administration sera composé :

- de représentants des quatre collèges ;
- d'un représentant de l'État, notamment l'ANSSI ;
- d'un représentant de la Région des Pays de la Loire ;
- d'un représentant du Gigalis, porteur du projet de préfiguration.

Cette composition assurera :

- un ancrage institutionnel fort ;
- une cohérence avec la stratégie nationale ;
- un équilibre entre acteurs publics et privés.

Le Conseil d'Administration définira les orientations stratégiques, validera le programme d'actions annuel et veillera au respect des principes de neutralité et d'intérêt général.

Des comités thématiques pour structurer l'action

Afin de préparer les orientations stratégiques et d'impliquer les parties prenantes dans la vie de CYBERLIG, plusieurs comités pourront être mis en place.

Les membres des collèges pourront y participer.

Comités envisagés :

- **comité thématique** : en charge du choix des sujets des groupes de travail et des ateliers ;
- **comité prospective et innovation** : identification des nouveaux services et des évolutions à intégrer ;
- **comité neutralité et éthique** : garant du respect des équilibres, de la prévention des conflits d'intérêts et du traitement des situations sensibles ;
- **comité communication** : valorisation des actions de CYBERLIG et cohérence des messages.

Cette organisation favorisera la participation active tout en structurant les décisions.

Le rôle du GIP Gigalis

Le Gigalis, porteur du projet de préfiguration dans le cadre de sa mission d'intérêt public, apportera un soutien structurant à CYBERLIG, notamment par :

- la mise à disposition de locaux ;
- l'accès à des services généraux ;
- l'appui de personnels, notamment via Pays de la Loire Cyber Assistance.

Ce soutien permettra d'amorcer le projet dans des conditions maîtrisées.

À mesure que CYBERLIG atteindra son équilibre économique grâce à l'augmentation des adhésions, des partenariats et du mécénat, cette dépendance opérationnelle sera progressivement réduite, renforçant son autonomie.

Une équipe opérationnelle dédiée

Une équipe opérationnelle dédiée assurera l'animation quotidienne de la structure.

Son dimensionnement évoluera en fonction du développement du projet.

Les missions envisagées incluront :

- alimentation et animation du site internet ;
- organisation et suivi des actions ;
- animation territoriale ;
- coordination avec les autres Campus Cyber et réseaux partenaires ;
- appui à la diffusion des dispositifs d'assistance cyber ;
- communication et valorisation des actions ;

- autres missions structurantes à définir.

Cette équipe constituera le moteur opérationnel du dispositif.

Garantie de neutralité opérationnelle et de distribution équitable des missions

Afin de prévenir toute perception de concurrence ou de favoritisme, CYBERLIG formalisera un principe clair de neutralité opérationnelle dans la mise en relation entre les organisations bénéficiaires et les partenaires.

CYBERLIG n'a pas vocation à produire en propre des prestations d'expertise technique, juridique ou organisationnelle concurrentes des acteurs du territoire. Son rôle est d'orienter, de structurer et de coordonner, sans se substituer aux entreprises spécialisées.

Lorsqu'un service impliquera l'intervention de partenaires (diagnostics, packs d'accompagnement, exercices personnalisés), les principes suivants s'appliquent :

- transparence des modalités d'intervention, validées par le Conseil d'Administration ;
- constitution des équipes d'intervention sur la base de critères objectifs (compétences, disponibilité, adéquation sectorielle) ;
- rotation équitable des partenaires lorsque plusieurs acteurs disposent de compétences similaires.

CYBERLIG ne désignera pas un partenaire de manière unilatérale.

Un reporting annuel synthétique pourra être présenté au Conseil d'Administration afin de garantir l'équilibre des interventions et la transparence du fonctionnement.

Cette garantie constituera un pilier de la confiance entre CYBERLIG et l'écosystème régional des entreprises de services numériques.

Une charte d'impartialité

Afin de garantir la neutralité des échanges et prévenir toute dérive commerciale ou conflit d'intérêts, une charte d'impartialité sera formalisée.

Elle encadrera notamment :

- les modalités d'intervention des partenaires ;
- la gestion des prises de parole ;
- la production des livrables des groupes de travail ;
- les règles de communication.

Cette charte constituera un engagement formel en faveur de la transparence, de l'équité et de la confiance.

Chapitre 7

MODÈLE ÉCONOMIQUE ET TRAJECTOIRE FINANCIÈRE

MODÈLE ÉCONOMIQUE ET TRAJECTOIRE FINANCIÈRE

Les principes du modèle économique de CYBERLIG ont été imaginés dès l'origine pour garantir sa soutenabilité et son indépendance financière progressive.

L'objectif est de construire un dispositif structurant pour le territoire, reposant majoritairement sur l'engagement des acteurs bénéficiaires et partenaires, plutôt que sur une dépendance aux subventions publiques.

Les hypothèses financières détaillées figurent dans le budget prévisionnel annexé au présent document.

Une structure de recettes fondée sur l'engagement des acteurs

Le modèle repose principalement sur 3 sources de recettes :

1. Les adhésions

Les cotisations des adhérents constitueront le socle du financement.

Le montant des cotisations sera :

- Unitaire pour les adhésions individuelles
- proportionnel au chiffre d'affaires de la structure pour les entreprises ;
- proportionnel au nombre d'habitants pour les collectivités territoriales.

Les cotisations seront capées

Ce principe garantira :

- une équité contributive ;
- une accessibilité pour les petites structures ;
- une contribution plus significative des grandes organisations.

Les associations, ordres professionnels, syndicats et chambres consulaires seront exonérés de cotisation afin de favoriser l'élargissement de l'écosystème et la dynamique collective.

2. Les partenariats

Deux niveaux de partenariat seront accessibles (normal et gold). Le niveau Gold permettra au partenaire d'avoir une mise en valeur supplémentaire décrite dans la matrice R.O.I en annexe.

Au-delà de la contribution financière, chaque partenaire s'engagera à mobiliser des ressources internes pour contribuer à l'animation de la structure (groupes de travail, ateliers, expertises)

Ce double engagement :

- d'impliquer activement les partenaires ;
- de valoriser leur expertise ;
- de limiter les charges opérationnelles directes de CYBERLIG.

3. Recettes complémentaires

En complément des adhésions et partenariats, des services facturés seront proposés.

Ces services resteront encadrés afin de préserver la complémentarité avec les entreprises de services numériques et éviter toute situation de concurrence. Ainsi :

- ces services doivent s'adresser à plusieurs entités simultanément ;
- ces services doivent impliquer plusieurs partenaires gold ;
- ces services ne doivent pas être proposés à l'échelle d'un territoire.

4. Le mécénat

Le mécénat annuel sera fixé à un montant minimum égale au niveau de partenariat gold.

Il s'inscrira dans une logique d'intérêt général et de soutien à la résilience numérique du territoire.

Le mécénat contribuera principalement au financement :

- du socle de services ouverts ;
- des actions de sensibilisation ;
- des dispositifs à fort impact territorial.

Une structure de dépenses maîtrisée

Les principales catégories de dépenses concerneront :

- l'animation de CYBERLIG et la coordination des actions ;
- le développement et la maintenance du site internet et des outils numériques ;
- l'organisation des événements ;
- la communication.

Les charges liées aux ressources humaines évolueront progressivement en fonction du développement du nombre d'adhérents et de partenaires.

Dans la phase de lancement, le Gigalis apportera un soutien structurant (locaux, services généraux, ressources humaines mutualisées), ce qui :

- réduit fortement les coûts fixes initiaux ;
- sécurise la phase d'amorçage ;
- permet un développement progressif sans déséquilibre financier.

Ce soutien sera amené à diminuer à mesure que les recettes propres augmentent.

Une trajectoire financière progressive et équilibrée

La trajectoire financière reposera sur :

- une croissance progressive des adhésions ;
- la stabilisation d'un nombre cible de partenaires ;
- l'engagement structurant des mécènes ;
- une augmentation corrélée des ressources humaines.

Le principe retenu est clair. L'équilibre financier sera recherché chaque année, avec un pilotage budgétaire prudent et une adaptation progressive du dimensionnement des équipes.

Le modèle visera à atteindre une autonomie opérationnelle durable, fondée sur :

- la fidélisation des membres ;
- la qualité des services ;
- la valeur perçue par les parties prenantes.

Chapitre 8

PLAN DE DÉPLOIEMENT ET FEUILLE DE ROUTE

PLAN DE DÉPLOIEMENT ET FEUILLE DE ROUTE

Le déploiement de CYBERLIG sera structuré sur une trajectoire pluriannuelle progressive, visant à sécuriser la phase d'amorçage, consolider l'écosystème régional, puis atteindre une pleine maturité opérationnelle.

La montée en puissance de CYBERLIG sera directement corrélée :

- à la sécurisation des ressources financières ;
- à la structuration des centres de ressources départementaux ;
- à l'augmentation du nombre d'adhérents, partenaires et mécènes.

Année 1 – 2026 : Structuration et lancement

L'année 2026 constituera la phase d'amorçage et de structuration institutionnelle.

Juin – Juillet 2026 : sécurisation du modèle

Une consultation préalable est lancée afin de vérifier la concordance du projet avec les aspirations des territoires ligériens

Le business plan est présenté au comité exécutif (Région Pays de la Loire, Préfecture de la Région Pays de la Loire, Gigalis, ANSSI) avec un objectif clair : atteindre le socle minimal de financement prévu dans le budget prévisionnel, à savoir :

- 10 adhésions individuelles ;
- 10 entreprises PME/TPE
- 10 entreprises ETI/Groupe ;
- 5 collectivités territoriales ;
- 13 partenaires dont 3 gold ;
- 2 mécènes.

Cette étape conditionne le lancement opérationnel du projet.

Septembre – Novembre 2026 : mise en place opérationnelle

- Recrutement d'un chef de projet à temps plein pour définir en détails les services, organisation, statuts, finances, staffing de la CYBERLIG ;
- Lancement des premiers travaux et services :
- liste des prestataires ;
- liste des clubs et associations régionaux ;
- liste des formations ;
- Préparation de la journée officielle de lancement.

Décembre 2026 : lancement institutionnel

- validation et dépôt des statuts de l'association ;
- organisation de la journée de lancement officielle ;
- signature des conventions avec les centres de ressources cyber départementaux, associations et fédérations ;
- organisation de 5 événements départementaux (sensibilisation, exercice de gestion de crise…) ;
- Construction des parcours réglementaires ;
- réalisation de la première enquête de l'Observatoire régional de la menace.

Objectif de fin d'année : une structure opérationnelle, structurée juridiquement, visible territorialement et dotée de premiers livrables.

Année 2 – 2027 : Consolidation et montée en puissance

L'année 2027 visera à structurer l'offre et renforcer l'ancrage territorial.

Déploiement territorial renforcé

- organisation de 2 événements par département (soit 10 au total) ;
- organisation d'une journée cyber régionale ;
- structuration des centres de ressources cyber manquants.

Développement des services

- mise en place effective des services à valeur ajoutée ;
- lancement des ateliers thématiques ;
- mise en place d'un second groupe de travail ;
- déploiement des parcours d'accompagnement NIS2 et CRA ;
- mise à jour du site internet avec fonctionnalités avancées :
- espace adhérent ;
- plateforme Talents & Compétences.

Pilotage et amélioration continue

- deuxième enquête de l'Observatoire régional de la menace ;
- enquête de satisfaction auprès des adhérents, partenaires et mécènes ;
- campagne active de promotion pour élargir la base d'adhésion.

Objectif : atteindre un seuil de stabilisation financière et opérationnelle.

Année 3 – 2028 : Maturité et élargissement

L'année 2028 marquera l'entrée de CYBERLIG dans une phase de maturité.

Intensification des actions

- organisation de 4 événements par département (soit 20) ;
- organisation d'une journée cyber régionale ;
- développement des services à valeur ajoutée ;
- déploiement des premiers services spécialisés facturés.

Renforcement opérationnel

- renforcement de la coordination avec Pays de la Loire Cyber Assistance et cofinancement de fonctions mutualisées ;
- financement d'une étude de recherche et développement ;
- troisième enquête de l'Observatoire régional de la menace.

Développement stratégique

- poursuite de la croissance des adhésions, partenariats et mécénat ;
- nouvelle enquête de satisfaction.

Objectif : consolider l'autonomie financière et renforcer la valeur ajoutée de la structure.

Année 4 – 2029 : Rayonnement et optimisation

L'année 2029 visera à amplifier l'impact régional et optimiser les outils.

Déploiement territorial intensif

- organisation de 6 événements par département (soit 30) ;
- organisation d'une journée cyber régionale.

Optimisation des services

- développement continu des services à valeur ajoutée et spécialisés facturés ;
- refonte du site internet pour accompagner la montée en charge.

Pilotage stratégique

- quatrième enquête de l'Observatoire régional de la menace ;
- enquête annuelle de satisfaction ;
- poursuite de la dynamique d'adhésion.

Objectif : positionner CYBERLIG comme acteur régional de référence pleinement stabilisé.

Synthèse de la trajectoire

Année	Priorité	Niveau de maturité
2026	Structuration & lancement	Amorçage
2027	Consolidation	Stabilisation
2028	Maturité	Autonomie renforcée
2029	Rayonnement	Optimisation

Chapitre 9

STRATÉGIE DE MOBILISATION ET D'ACQUISITION

STRATÉGIE DE MOBILISATION ET D'ACQUISITION

La réussite de CYBERLIG reposera sur sa capacité à mobiliser progressivement les acteurs du territoire et à les inscrire dans un parcours d'engagement structuré.

L'objectif ne sera pas d'adopter une logique de prospection commerciale classique, mais de positionner la structure comme un tiers de confiance territorial, facilitateur et agrégateur.

La stratégie de mobilisation visera à répondre à trois besoins identifiés lors des ateliers :

- élever la maturité des organisations les moins avancées, en particulier les dirigeants ;
- apporter un premier niveau d'accompagnement face aux nouvelles exigences réglementaires ;
- structurer une information aujourd'hui dispersée

Cibles prioritaires (2026–2028)

Au cours des deux à trois premières années, les efforts seront concentrés sur :

- les dirigeants de TPE/PME peu matures ;
- les collectivités territoriales ;
- les RSSI et responsables numériques du territoire.

Quatre offres constitueront les principales portes d'entrée :

- le site internet et son annuaire structuré ;
- le diagnostic CyberDépart ;
- les exercices de gestion de crise ;
- le speed consulting réglementaire.

Mobilisation via les réseaux relais

Le premier levier d'acquisition reposera sur des réseaux déjà légitimes auprès des publics cibles :

- chambres consulaires ;
- associations d'élus ;
- clusters et réseaux numériques ;
- établissements d'enseignement supérieur.

L'objectif sera de crédibiliser la démarche et de toucher des publics déjà en confiance, grâce à des intermédiaires reconnus. Concrètement, cela se traduira par :

- la co-organisation de webinaires et ateliers de premier niveau (par exemple : « Cyber : par où commencer quand on est une TPE/PME ou une collectivité ? ») ;
- des interventions de CYBERLIG dans les instances existantes de ces réseaux (commissions,

clubs, réunions d'élus, réseaux d'entreprises…) ;
- l'intégration progressive de CYBERLIG comme « guichet unique cyber » dans leurs communications (newsletters, sites, plaquettes).

Ces actions permettront de présenter la proposition de valeur de la structure, de faire connaître les diagnostics CyberDépart et les parcours d'accompagnement, et de générer des premiers contacts qualifiés.

Animation territoriale et événements

Les événements organisés dans les départements constitueront un levier majeur de mobilisation :

- ateliers de sensibilisation ;
- exercices de crise interstructures ;
- retours d'expérience ;
- participation à des salons et forums territoriaux.

Chaque événement sera conçu comme une étape dans un parcours progressif :

1. Prise de conscience des risques ;
2. Orientation vers un diagnostic ou un exercice ;
3. Engagement dans une démarche plus structurée.

Prospection directe ciblée, en appui

La prospection directe viendra en **complément** des réseaux et des événements, dans une logique de relation plutôt que de démarchage massif.

Elle se concentrera sur :

- les contacts qualifiés issus des ateliers, webinaires et événements ;
- les organisations signalées par les réseaux relais (entreprises ou collectivités en difficulté, ou en questionnement sur la cybersécurité) ;
- quelques profils clés (dirigeants, DGS, responsables numériques, responsables formation) identifiés via LinkedIn ou bases partenaires.

Les actions menées seront :

- des emails structurés, pédagogiques et personnalisés ;
- des appels téléphoniques visant à qualifier la situation et proposer un premier pas adapté (diagnostic flash, rendez-vous de cadrage) ;
- des prises de contact ciblées sur LinkedIn lorsque pertinentes.

L'objectif sera de transformer l'intérêt en passage à l'action, tout en restant cohérent avec le positionnement de tiers de confiance (pas de démarchage agressif, mais une proposition d'accompagnement progressive).

Parcours d’engagement par typologie d’acteurs

Parcours type pour une TPE / PME

1. Le dirigeant participe à un atelier de sensibilisation organisé avec une CCI, un cluster ou un réseau entrepreneurial.
2. À l’issue de l’atelier, il est invité à réaliser un diagnostic CyberDépart, présenté comme un point de départ simple et non technique et qui permet de prioriser les actions.
3. Une fois la feuille de route établie, CYBERLIG oriente vers des prestataires locaux pour la mise en œuvre technique, tout en proposant un suivi annuel léger pour ajuster la trajectoire.

Ce parcours illustre une logique d’accompagnement progressif, où chaque étape prépare la suivante et renforce la confiance.

Parcours type pour une collectivité ou un établissement public

1. La collectivité est invitée, via un réseau d’élus ou une association de collectivités, a un exercice de crise avec d’autres collectivités.
2. À l’issue de cette première sensibilisation, la collectivité souhaite organiser en son sein un exercice standard.
3. 12 mois après l’exercice interne, elle refait un exercice personnalisé par un partenaire de CYBERLIG.

Là encore, la démarche reposera sur un parcours structuré, avec CYBERLIG en tiers de confiance pour sécuriser les décisions et assurer la cohérence globale.

Parcours type pour une RSSI

1. Un RSSI se connecte sur le site internet pour voir les prochains événements cyber à côté de chez lui.
2. Sur le site, il voit s’abonne pour recevoir la newsletter hebdomadaire de l’état de la menace.
3. Il contribue à alimenter l’état de la menace par les alertes reçues en interne de sa structure.

Parcours type pour une ETI assujettie pas NIS2

1. Une PME est informée par sa fédération qu’elle est assujettie à NIS2.
2. Le DSI participe à un événement de présentation de NIS2.
3. Le parcours NIS2 est proposé pour poursuivre l’accompagnement.

Messages clés

La stratégie d'attaque s'appuiera sur quelques messages centraux :

- « Vous n'êtes pas seuls et vous n'avez pas besoin d'être expert » : CYBERLIG aide à comprendre, prioriser et trouver les bons relais.

La cybersécurité sera présentée non comme un sujet purement technique, mais comme un enjeu de continuité d'activité, de service public et de crédibilité.

CYBERLIG se positionnera clairement comme un tiers de confiance territorial, neutre vis-à-vis des prestataires, et complémentaire des dispositifs nationaux.

Le ton sera volontairement pédagogique, non anxiogène, mais clair sur les enjeux. La différenciation se fera par :

- la neutralité (adossement à des acteurs publics et parapublics) ;
- l'articulation avec l'écosystème existant (et non la concurrence frontale) ;
- la construction d'un parcours progressif, adapté à la taille et au niveau de maturité de chaque organisation.

Cette stratégie d'attaque visera ainsi à concentrer les efforts sur les leviers qui génèrent le plus de valeur pour le territoire : la montée en maturité des organisations, la structuration d'une demande éclairée et l'orientation vers les compétences cyber locales.

Chapitre 10

INDICATEURS DE PERFORMANCE ET MESURE D'IMPACT

INDICATEURS DE PERFORMANCE ET MESURE D'IMPACT

Le pilotage de CYBERLIG reposera sur des indicateurs quantitatifs et qualitatifs permettant de mesurer :

- la dynamique d'adhésion ;
- l'intensité de l'activité ;
- l'impact territorial ;
- la satisfaction des parties prenantes.

Ces indicateurs feront l'objet d'un suivi annuel et d'une restitution au Conseil d'Administration.

Dynamique d'adhésion et solidité du modèle

Nombre d'adhérents

Le nombre d'adhérents constituera un indicateur structurant du modèle économique et de la légitimité de la structure.

Les objectifs d'adhésion seront définis de manière progressive dans le budget prévisionnel et conditionneront la montée en puissance des ressources humaines et des services.

Taux de renouvellement

Un taux de renouvellement cible de **90 %** est retenu.

Cet indicateur reflètera :

- la valeur perçue des services ;
- la fidélisation des membres ;
- la soutenabilité financière du modèle.

Indicateurs d'impact opérationnel

Ces indicateurs mesureront l'intensité des actions menées et leur diffusion territoriale.

Exercices de crise inter-structure

À partir de 2027 :

- **2 exercices inter-structure par an et par département**

Soit 10 exercices annuels à l'échelle régionale (5 départements).

Diagnostics CyberDépart facilités

En moyenne :

- **30 diagnostics par an et par département**

Soit 150 diagnostics annuels à l'échelle régionale.

Engagement des partenaires

Chaque partenaire s'engagera à participer, intervenir ou co-animer :

- **au minimum 4 événements, ateliers, GT par an**

Cet indicateur garantira :

- l'implication opérationnelle des partenaires ;
- la vitalité de l'écosystème.

Une partie significative de l'animation repose sur les partenaires et centres de ressources cyber départementaux.

Indicateurs issus de l'Observatoire régional

L'Observatoire régional de la menace permettra de mesurer :

- l'évolution du nombre d'incidents déclarés ;
- les typologies d'attaques rencontrées ;
- les délais de détection et de réaction ;
- la proportion de structures victimes.

Ces indicateurs permettront d'objectiver l'évolution de la menace et d'adapter les priorités stratégiques de CYBERLIG.

Newsletter Etat de la menace

- **1 newsletter hebdomadaire**

Soit environ 50 éditions par an.

Indicateurs qualitatifs et satisfaction

Un indicateur clé de réussite sera le taux de satisfaction des membres.

Objectif cible :

- **90 % de satisfaction**

Une enquête annuelle sera réalisée auprès :

- des adhérents ;
- des partenaires ;
- des mécènes.

Les résultats permettront d’ajuster les services et d’orienter les priorités.

Chapitre 11

ANALYSE DES RISQUES ET MESURES D'ATTÉNUATION

ANALYSE DES RISQUES ET MESURES D'ATTÉNUATION

Le projet CYBERLIG s'inscrit dans un environnement économique et institutionnel en évolution. Sa réussite reposera sur une anticipation lucide des risques potentiels et la mise en place de mécanismes d'atténuation adaptés.

Risque d'insuffisance d'adhésion

Bien que les ateliers de préfiguration aient démontré un intérêt réel pour la création d'un campus cyber régional, le contexte économique demeure incertain. Les organisations peuvent arbitrer leurs dépenses, notamment en matière de cotisation associative.

Une insuffisance d'adhésion pourrait fragiliser l'équilibre financier du projet.

Impact potentiel

- recettes inférieures aux prévisions ;
- ralentissement du déploiement des services ;
- retard dans le recrutement de l'équipe opérationnelle.

Mesures d'atténuation prévues

- ajustement possible de la politique tarifaire après le premier tour de table ;
- révision annuelle des grilles tarifaires si nécessaire ;
- adaptation progressive de l'offre de services au niveau réel de recettes ;
- pilotage budgétaire prudent avec équilibre recherché chaque année.

Mesures complémentaires proposées

- développement d'une stratégie de cooptation par territoire ;
- mise en place d'un suivi trimestriel des adhésions avec plan d'action correctif ;
- renforcement des actions de communication ciblée par filière.

Risque de déséquilibre entre partenaires et neutralité

La neutralité constituera un pilier du projet. Les partenaires, qui contribueront financièrement et opérationnellement, pourront légitimement rechercher un retour sur investissement. Ce double objectif pourra générer une tension entre visibilité commerciale et impartialité.

Impact potentiel

- perception de favoritisme ;
- rerte de confiance des adhérents ;
- fragilisation de la gouvernance.

Mesures d’atténuation prévues

- organisation en collèges garantissant un équilibre décisionnel ;
- comité neutralité dédié ;
- charte d’impartialité formalisée ;
- distinction claire entre services d’intérêt général et services valorisant les partenaires ;
- transparence sur les modalités de participation des partenaires.

Mesures complémentaires proposées

- rotation équitable des partenaires intervenants ;
- publication annuelle d’un rapport de neutralité ;
- mise en place d’un mécanisme de signalement interne en cas de conflit d’intérêts ;
- séparation explicite des espaces de communication institutionnelle et promotionnelle.

Risque de concurrence perçue par les ESN

La facturation de certains services (exercices personnalisés, dispositifs spécifiques) pourrait être perçue comme une concurrence par les entreprises de services numériques régionales.

Impact potentiel

- tensions dans l’écosystème ;
- retrait ou non-adhésion de partenaires ;
- perte de crédibilité collaborative.

Mesures d’atténuation prévues

- positionnement clair de complémentarité ;
- limitation des services spécialisés facturés aux besoins non couverts ou mutualisés ;
- mise en place d’un comité dédié à l’examen des nouveaux services ;
- forte représentation du collège partenaires dans ce comité.

Mesures complémentaires proposées

- mécanismes précis de neutralité opérationnelle et de distribution transparente des missions sont détaillés au chapitre Gouvernance ;
- cartographie annuelle des offres existantes avant lancement d’un nouveau service ;
- consultation préalable des partenaires concernés ;
- priorité donnée à l’externalisation vers des prestataires régionaux ;
- transparence sur la tarification et la justification des services spécialisés facturés.

Risque de dépendance excessive à un nombre limité de mécènes

Les mécènes constituent une ressource financière significative mais peu nombreuse. Une dépendance excessive pourrait fragiliser le modèle en cas de retrait.

Impact potentiel

- déséquilibre budgétaire ;
- réduction des services ouverts ;
- instabilité financière.

Mesures d'atténuation prévues

- diversification progressive des sources de financement ;
- communication régulière sur l'impact territorial ;
- valorisation institutionnelle des mécènes.

Mesures complémentaires proposées

- mise en place d'un plan de diversification du mécénat ;
- développement d'une offre de mécénat à plusieurs niveaux ;
- constitution d'un fonds de réserve en cas d'excédent ;
- plan de continuité budgétaire en cas de perte d'un mécène.

Risque de difficulté d'animation territoriale

Des acteurs seront identifiés pour participer aux centres de ressources cyber départementaux, mais leurs capacités d'animation pourraient être limitées.

Impact potentiel

- dynamique territoriale inégale ;
- érosion de l'engagement local ;
- concentration excessive des actions au niveau régional.

Mesures d'atténuation prévues

- structuration progressive des centres de ressources ;
- appui renforcé de l'équipe régionale ;
- mutualisation des travaux entre départements.

Mesures complémentaires proposées

- déploiement d'indicateurs spécifiques par département ;
- organisation annuelle d'une rencontre des centres départementaux ;
- reconnaissance officielle du rôle d'ambassadeur territorial.

Synthèse

L’analyse des risques montre que les principaux enjeux du projet sont :

- financiers (adhésion et mécénat) ;
- institutionnels (neutralité) ;
- écosystémiques (non-concurrence) ;
- territoriaux (animation locale).

La gouvernance collégiale, la progressivité du modèle économique et la structuration territoriale constitueront les principaux leviers de réduction des risques.

Chapitre 12

FACTEURS CLÉS DE SUCCÈS

FACTEURS CLÉS DE SUCCÈS

Le succès de CYBERLIG reposera sur un ensemble de facteurs structurants, déjà réunis ou en cours de consolidation, qui garantira la crédibilité, la pertinence et la soutenabilité du projet.

Un besoin territorial clairement identifié

Les ateliers de préfiguration ont confirmé :

- l'existence d'un besoin réel de structuration ;
- la volonté des acteurs de coopérer ;
- l'attente d'un tiers de confiance neutre ;
- la nécessité d'une meilleure lisibilité de l'écosystème.

Le projet ne répondra donc pas à une logique descendante, mais à une demande exprimée par les acteurs eux-mêmes.

Un ancrage institutionnel solide

Le portage initial par le Gigalis, dans le cadre de sa mission d'intérêt public, constituera un facteur de sécurisation majeur.

Les implications de la Région des Pays de la Loire, de l'ANSSI, des collectifs/centres de ressources cyber départementaux garantiront une cohérence avec la stratégie nationale et un ancrage territorial fort.

Une gouvernance équilibrée et neutre

La structuration en collèges, la représentation au Conseil d'Administration et la mise en place d'une charte d'impartialité constitueront des garanties concrètes :

- prévention des conflits d'intérêts ;
- équilibre entre acteurs publics et privés ;
- transparence des décisions.

La neutralité sera inscrite dans l'architecture même du projet.

Un modèle économique responsable et progressif

Le choix d'un modèle principalement financé par les adhésions, les partenariats, le mécénat et des services spécialisés facturés renforcera l'autonomie et la responsabilisation des acteurs bénéficiaires.

La montée en puissance progressive des services et des ressources humaines limitera le risque financier et garantira l'adéquation entre ambition et moyens.

Une approche territoriale différenciante

Le déploiement de centres de ressources cyber départementaux permettra :

- une proximité avec les acteurs locaux ;
- une adaptation aux spécificités territoriales ;
- une dynamique ascendante (bottom-up).

Cette architecture régionale constituera un élément différenciant fort par rapport à des dispositifs centralisés.

Une complémentarité assumée avec l'écosystème existant

CYBERLIG ne se positionnera pas comme un prestataire concurrent, mais comme un agrégateur et un coordinateur.

L'articulation avec les associations professionnelles, les fédérations économiques, les établissements de formation et le réseau national des campus cyber constituera un levier majeur de réussite.

Une logique contributive et collaborative

Le modèle reposera sur une implication active des partenaires et des adhérents :

- animation de groupes de travail ;
- contribution à l'Observatoire ;
- participation aux exercices de crise ;
- partage de ressources.

Cette dynamique collaborative renforcera la résilience collective et favorise l'appropriation du projet par l'écosystème.

Une mesure d'impact structurée

Le pilotage par indicateurs (adhésions, exercices, diagnostics, satisfaction, évolution de la menace) permettra:

- une évaluation annuelle ;
- un ajustement continu ;
- une démonstration tangible de la valeur créée.

Chapitre 13

CONCLUSION

CONCLUSION

La cybersécurité n'est plus un sujet technique réservé aux experts.
Elle constitue aujourd'hui un enjeu stratégique pour la continuité d'activité des organisations, la confiance numérique, l'attractivité économique et la souveraineté territoriale.

Les Pays de la Loire disposent :

- d'un tissu économique dense et diversifié ;
- d'acteurs publics et privés engagés ;
- d'experts en cybersécurité ;
- d'un dispositif régional d'assistance déjà opérationnel.

Cependant, l'écosystème reste fragmenté et insuffisamment structuré.

CYBERLIG propose une réponse pragmatique, progressive et équilibrée :

- fédérer dans une logique d'articulation territoriale ;
- structurer sans concurrencer ;
- accompagner sans imposer.

Le modèle retenu repose sur une logique de responsabilité partagée :

- les adhérents s'engagent pour renforcer leur résilience ;
- les partenaires contribuent à l'animation et à la montée en compétences ;
- les mécènes soutiennent un dispositif d'intérêt général à fort impact territorial ;
- les pouvoirs publics assurent la cohérence stratégique.

Investir dans CYBERLIG, c'est :

- contribuer à la sécurisation durable du tissu économique régional ;
- renforcer la capacité de réaction des organisations ;
- structurer un écosystème coopératif et résilient ;
- associer son image à un projet stratégique et d'intérêt général.

La trajectoire proposée est maîtrisée, progressive et fondée sur des indicateurs mesurables. La gouvernance garantit la neutralité et l'équilibre des intérêts. Le modèle économique vise l'autonomie et la soutenabilité.

CYBERLIG représente une opportunité unique de doter les Pays de la Loire d'un outil structurant, au service de la résilience numérique collective.

Il s'agit désormais de transformer l'intérêt exprimé lors des ateliers en engagement concret.

Le succès de CYBERLIG reposera sur la mobilisation de ses financeurs et partenaires fondateurs.

En rejoignant CYBERLIG dès sa phase de lancement, ils contribueront à structurer durablement la cybersécurité régionale et à inscrire les Pays de la Loire parmi les territoires de référence en matière de résilience numérique.

Chapitre 14

ANNEXE FINANCIÈRE

ANNEXE R.O.I

Service	Type de service	Difficulté de mise en place	Le territoire	Adhérent	Partenaire	Partenaire Gold	Associations/Fédération
Annuaire régional cyber	Intérêt général	3	Lisibilité de l'écosystème	-	-	Mise en valeur par bandeau de pub	Mise en valeur de leurs activités
Sensibilisation	Intérêt général	2	Acculturation des dirigeants (entre autre)	Information push	Animation	Accueil évènement	Co-organisation
Diag Cyber	Intérêt général	1	Augmentation de la résilience du territoire	Possibilité d'être aidant	Possibilité d'être aidant	-	-
Suivi Post CyberDépart	Intérêt général	2	Augmentation de la résilience du territoire		Possibilité de faire le suivi 6 mois plus tard		-
Pays de la Loire Cyberassistance	Intérêt général	1	Augmentation de la résilience du territoire	-	-	-	-
Exercice de crise inter-structure	Intérêt général	1	Augmentation de la résilience du territoire	-	Animation	Accueil évènement	-
Banque de ressources mutualisés	Intérêt général	1	Demande forte de la communauté	-	-	-	Co portage ou mise en avant de production déjà réalisée par l'association
Parcours NIS2	Service à V.A.	2	-	Accès à de l'expertise pour démarrage ou précision	-	Mise en valeur de leur expertise	-
Veille menace régionale	Service à V.A.	1	-	Transformation d'une menace abstraite en réalité territoriale	Mise en valeur de leur expertise	-	-
GT Thématique	Service à V.A.	1	-	Demande forte de la communauté	-	Accueil et production du livrable	-
Charte solidarité	Service à V.A.	3	-	accès à de l'expertise et partage d'expérience	-	-	-