DIGITAL LEAGUE
Auvergne-Rhône-Alpes

Les pirates ne dorment jamais.

Et vous ?

édition 2025

Guide Cyber

La Région Auvergne-Rhône-Alpes

CAMPUS RÉGION DU NUMÉRIQUE

EDITO

Les pirates ne dorment jamais. Et vous ?

En 2024, le Club Experts Cybersécurité de Digital League lançait la première édition de ce guide. Son objectif ? Rendre la cybersécurité accessible, pragmatique et surtout en phase avec la réalité terrain des TPE, PME-PMI, ETI, associations et collectivités de notre région.

Un an plus tard, le constat est sans appel !

2025 a vu la cybercriminalité franchir un nouveau cap. Rançongiciels toujours plus agressifs, fuites massives de données, détournement de l'intelligence artificielle générative… Et notre région n'est pas épargnée avec près d'une entreprise sur deux touchée. Derrière les chiffres, du concret : des parcs machines à l'arrêt, des fonctions support revenues au papier-crayon, des pertes financières, une image ternie et parfois même des entreprises qui mettent la clé sous la porte.

Mais 2025 est aussi la preuve que notre grande région sait se mobiliser. De nouveaux prestataires régionaux, des écoles et centres de recherche de rang mondial, un Campus Région du numérique moteur, etc… Autant d'atouts qui font de notre territoire un vrai rempart face aux cybermenaces.

Cette édition 2025 s'inscrit dans cette dynamique. Pas de jargon, pas de grands discours, mais des règles d'or, des bonnes pratiques, des ressources officielles. L'essentiel pour que la cybersécurité devienne un réflexe et non un fardeau.

Ce guide se veut aussi un premier jalon posé par Digital League, au service de l'ambition collective de la Région Auvergne-Rhône-Alpes, et dans la perspective de l'émergence d'un Campus Cyber Territorial fin 2026.

Et ce n'est qu'un début car 2026 amènera son lot de défis : la transposition de NIS2, l'IA générative qui brouillera toujours plus la frontière entre vrai et faux. Des échéances électorales sous haute tension et des cyberattaques plus ciblées que jamais.

Fort heureusement, la cybersécurité est aussi une histoire de rencontres. Entre ceux qui ont un besoin et ceux qui savent y répondre. C'est tout le sens de l'initiative Digital Leads portée par Digital League : créer de vraies opportunités business pour rapprocher experts régionaux et organisations en quête de confiance numérique.

Les pirates ne dorment jamais. Mais bien préparés, vous pourrez dormir l'esprit tranquille.

Laurent PAÏTA
Responsable projets
Référent Club Experts Cyber
Digital League

CLUB EXPERTS CYBERSÉCURITÉ

Dans un monde toujours plus connecté, où les technologies s'imposent au cœur des stratégies d'entreprise et où les cybermenaces gagnent en intensité comme en sophistication, la cybersécurité est devenue un enjeu stratégique. Elle conditionne à la fois la continuité des activités, la protection des données et la confiance des clients comme des partenaires.

Créé par **Digital League**, le Club Experts Cybersécurité fédère et anime les professionnels du secteur en Auvergne-Rhône-Alpes. Son objectif ? Structurer la filière régionale et élever collectivement le niveau de cybersécurité des acteurs économiques, en particulier des TPE, PME-PMI, ETI, associations et collectivités, souvent les plus exposés et les moins armés face à ces menaces.

En 2024, les cyberattaques se sont intensifiées, touchant près d'une entreprise sur deux dans la région. Rançongiciels toujours plus agressifs, fuites massives de données, exploitation de l'IA générative…
Face à cette réalité, le Club a multiplié les initiatives :

- Organiser des sessions de travail et d'échanges entre pairs pour confronter les pratiques
- Favoriser la mise en réseau pour identifier des synergies et renforcer l'offre de services
- Prendre la parole et représenter l'écosystème lors d'événements
- Produire des ressources concrètes, à l'instar de ce guide

En 2025, le Club s'affirme encore davantage comme un lieu de référence :

- Un collectif engagé réunissant experts cyber, offreurs de solutions, écoles, institutions et chercheurs
- Un espace de veille et d'anticipation, en lien avec les grandes orientations régionales, nationales et européennes
- Un accélérateur qui valorise les savoir-faire régionaux et favorise les mises en relation qualifiées

Plus qu'un cercle, le Club Experts Cybersécurité de Digital League est devenu un moteur régional de la résilience numérique, contribuant à la souveraineté et à la sécurité de tout l'écosystème économique et institutionnel de la région.

Les animateurs du Club Experts Cybersécurité

Thierry ROUQUET
Partner
CyGO Entrepreneurs

Garbiel BLANCHARD
Directeur adjoint - Transfert de technologie
Grenoble INP Esisar

Salem NAIT-IDIR
Délégué Général Adjoint
Digital League

Laurent PAÏTA
Responsable projets
Référent Club Experts Cyber
Digital League

DIGITAL LEAGUE

DIGITAL LEAGUE
Auvergne-Rhône-Alpes

Digital League est le cluster des **entreprises de la filière numérique en Auvergne-Rhône-Alpes.** Avec +400 membres, notre objectif est de favoriser la croissance économique et l'emploi en région.

Digital League propose à sa communauté, des actions au service de 3 missions :

Réunir une communauté pour favoriser l'échange d'idées et de bonnes pratiques et **créer des opportunités de collaboration**.

Faire grandir nos adhérents, leurs collaborateurs et l'écosystème en facilitant leur quotidien avec la mise à disposition des **outils essentiels au développement de l'entreprise**.

Engager les entreprises pour avancer plus efficacement sur des **enjeux sociétaux liés aux numérique**.

Au quotidien, Digital League créé du lien entre entrepreneurs, écoles, laboratoires, investisseurs et institutionnels pour faire naître des synergies gagnantes et inscrire les membres de la famille dans une **dynamique durable.** Le tout respectant 4 valeurs : le collectif, la convivialité, la proximité et les compétences.

Vous souhaitez en savoir plus sur Digital League ?
Rendez-vous sur www.digital-league.org

Dans un monde numérique en constante évolution, la cybersécurité est devenue **un enjeu majeur** pour les entreprises de toutes tailles.

Face à **une menace grandissante**, il est impératif de prendre des mesures proactives pour protéger ses actifs numériques.

Le **Club Experts Cybersécurité de Digital League**, qui **fédère les acteurs de la cybersécurité de la région Auvergne Rhône-Alpes**, vous présente ses 10 points clés de la cybersécurité.

De la sensibilisation des collaborateurs à la gestion de crise, ces principes offrent un cadre solide pour sécuriser votre environnement informatique et assurer la continuité de vos activités en toute sécurité.

LES 10 RÈGLES D'OR DE LA CYBERSÉCURITÉ

1 Sensibiliser ses collaborateurs

49% des entreprises françaises ont subi au moins une cyberattaque. La première protection reste vos collaborateurs.

2 Sécuriser ses mots de passe

80% des intrusions impliquent des identifiants volés ou faibles.

3 Maintenir à jour son système d'information

+ 50% des incidents graves proviennent de failles dans des outils non mis à jour.

4 Cloisonner son environnement

20% des cyberattaques finissent par atteindre l'outil de production.

5 Contrôler les accès

33% des incidents graves viennent d'une mauvaise gestion des droits d'accès.

6 Détecter les signaux faibles

Les incidents de sécurité ont augmenté de **15%** en 2024.

7 Protéger ses données stratégiques

En 2024, + de **1 000** fuites de données d'entreprises françaises ont été recensées sur des sites de cybercriminels.

8 Faire des sauvergardes et les tester

60% des PME victimes d'une cyberattaque majeure cessent leur activité dans les 6 mois faute de sauvergardes fiables.

9 Avoir une politique de cybersécurité

68% des PME n'ont pas de politique de cybersécurité formelle.

10 Se préparer au pire

Seulement **38%** des entreprises disposent d'un plan de réponse aux incidents.

LES 10 RÈGLES D'OR DE LA CYBERSÉCURITÉ

1 Sensibiliser ses équipes

Souvent considérés comme le maillon faible, les collaborateurs représentent pourtant la première ligne de défense face aux cyberattaques. Or, la plupart des incidents graves trouvent leur origine dans une erreur humaine : clic sur un mail piégé, ouverture d'une pièce jointe douteuse, utilisation d'un mot de passe faible. La sensibilisation doit donc être régulière et adaptée à la réalité de votre entreprise. Campagnes de faux mails de phishing, exercices de fraude au président ou ateliers autour des deepfakes permettent d'ancrer de bons réflexes. Plus vous intégrerez la culture de la vigilance au sein de votre entreprise, moins elle sera vulnérable aux manipulations des cybercriminels.

2 Sécuriser ses mots de passe

Fini les « 1234 », « admin » ou encore votre date de naissance. Un seul mot de passe compromis peut suffire à bloquer toute une organisation. Il est essentiel d'imposer des mots de passe uniques et robustes. Encouragez l'utilisation de passphrases complexes et d'outils de gestion de mots de passe sécurisés, comme par exemple : « GhT1KwAyiEr! » (ndlr : J'ai acheté un kway hier).
La double authentification (appelée MFA) est désormais incontournable pour sécuriser les accès sensibles : comptes administrateurs, banque, messageries, etc...
Les clés de sécurité physiques ou les passkeys, de plus en plus répandues, offrent une protection renforcée face aux méthodes de vol d'identifiants qui se perfectionnent chaque année.

3 Maintenir à jour son système d'information

Un système non mis à jour est une cible facile. Négliger les mises à jour revient à laisser une porte ouverte. Les pirates exploitent massivement les failles connues et notamment celles qui affectent les équipements de sécurité placés en bordure de l'entreprise (pare-feu, VPN, routeurs). Ces faiblesses techniques sont aujourd'hui à l'origine de la majorité des intrusions graves. Maintenir à jour vos logiciels, systèmes d'exploitation et applications métiers ne suffit plus. Au même titre que vous vérifiez régulièrement votre trousse de secours, faites de même avec l'état de vos équipements de sécurité et appliquez les correctifs dès leur publication.

4 Cloisonner son environnement

Comme les œufs, ne mettez pas tous vos systèmes dans le même panier. Parc machines, bureaux, Wi-Fi invité ou bien encore objets connectés doivent être séparés et isolés les uns des autres. Segmentez vos réseaux (par service, par bâtiment, etc...). Ce cloisonnement limite la propagation d'une attaque. Autrement dit une intrusion sur le Wi-Fi invité ne doit pas permettre d'atteindre les données clients ou de bloquer votre outil de production. Avec la généralisation du télétravail, du cloud et des objets connectés, séparer vos environnements est devenu une mesure simple mais indispensable pour réduire l'impact d'une cyberattaque.

5 Contrôler les accès

Un collaborateur ne doit disposer que des accès nécessaires à sa mission. Donner trop de droits d'accès, c'est multiplier les risques d'abus ou de compromission. Les comptes administrateurs doivent être strictement réservés à des usages précis et surveillés. Lorsqu'un collaborateur change de poste, ses accès doivent être modifiés. Révoquez immédiatement ceux des anciens collaborateurs en élaborant un processus d'offboarding (ie : débarquement).
Ces gestes, souvent considérés comme de simples formalités, évitent pourtant de nombreuses intrusions. Imaginez ce que pourrait faire un ancien collaborateur mécontent.

Détecter les signaux faibles

6

Une cyberattaque ne se traduit pas toujours par un blocage immédiat.
Dans la plupart des cas, les cybercriminels restent discrets, observent et testent vos défenses avant de frapper là où vous ne vous y attendez pas.
Pour y remédier, détectez les signaux faibles : connexions inhabituelles, transferts de données suspects, comportements anormaux. Réduire votre “surface d’attaque” et mettre en place des solutions de surveillance adaptées à la taille de votre entreprise renforcent considérablement votre capacité à réagir vite. Plus tôt une menace est repérée, moins ses conséquences seront lourdes.

Protéger ses données stratégiques

7

Toutes les données n’ont pas la même valeur pour vous comme pour un pirate.
Certaines sont vitales pour la survie de votre entreprise : fichiers clients, données financières, brevets, plans techniques, informations RH. Les pirates le savent et ciblent en priorité ces informations sensibles. Identifiez vos données stratégiques, chiffrez-les, limitez leur accès et évitez de les conserver plus longtemps que nécessaire.
Une donnée bien protégée est une donnée qui ne pourra pas être exploitée ou revendue par un attaquant.

Faire des sauvegardes et les tester

8

Les sauvegardes sont « l’assurance vie numérique » de votre entreprise.
Pourtant, une sauvegarde qui ne peut pas être restaurée ne sert à rien. Appliquez la règle du 3-2-1 : trois copies de vos données, sur deux supports différents, dont une hors ligne.
N’oubliez pas de tester régulièrement vos restaurations y compris pour vos solutions cloud.
En cas de cyberattaque, une sauvegarde fiable peut faire la différence entre une reprise rapide de l’activité et une fermeture définitive de votre entreprise.

Avoir une politique de cybersécurité

9

La cybersécurité ne doit pas reposer uniquement sur la bonne volonté ou l’intuition.
Et encore moins sur le dirigeant d’entreprise. Une politique cyber claire définit les règles à suivre, les rôles de chacun et les moyens alloués. Même simple et adaptée à la taille de votre structure, elle montre à vos collaborateurs, clients et partenaires que la sécurité est prise au sérieux. Avec l’arrivée de nouvelles réglementations comme la directive européenne NIS2, avoir une politique de cybersécurité n’est plus seulement une bonne pratique : c’est une nécessité pour continuer à inspirer confiance.

Se préparer au pire

10

Même avec toutes les protections en place, le risque zéro n’existe pas. Une cyberattaque peut frapper à tout moment et paralyser votre activité. Anticiper, c’est donc aussi prévoir un plan de réponse simple et connu de tous : qui prévenir en interne, qui contacter à l’extérieur (prestataire, assureur, avocat, CNIL, 17Cyber) et comment communiquer avec vos clients et partenaires.
Ce plan doit inclure des processus clairs, comme l’activation d’un Plan de Continuité d’Activité (PCA) ou d’un Plan de Reprise d’Activité (PRA) afin de minimiser l’impact d’une attaque. Réaliser au moins un exercice par an vous permettra de tester vos réactions et de corriger vos faiblesses.
Une entreprise préparée traverse la crise, une entreprise non préparée la subit.

Sources : ANSSI, ComCyber-MI, Cybermalveillance.gouv.fr, CESIN, Auvergne-Rhône-Alpes Entreprises.

JE SUIS VICTIME D'UNE CYBERATTAQUE

Dans un contexte où les cybermenaces sont de plus en plus fréquentes et sophistiquées, il est crucial pour les entreprises de savoir réagir rapidement face à une cyberattaque. Qu'il s'agisse de **limiter les dégâts**, d'**identifier l'origine de l'incident** ou de **communiquer** avec les parties prenantes, **les premières heures qui suivent une attaque sont déterminantes.**
Le Club Experts Cybersécurité de Digital League vous propose les **10 réflexes à adopter** pour contenir efficacement l'attaque et assurer une reprise rapide de vos activités.

QUE DOIS-JE FAIRE ?

#1
☐ Prévenez votre partenaire cyber

#2
☐ Contactez le 17Cyber

#3
☐ Activez un plan de gestion de crise

#4
☐ Identifiez l'origine et la portée de l'attaque

#5
☐ Isolez le système infecté

#6
☐ Prévenez votre assureur cyber

#7
☐ Déposez plainte

#8
☐ Ne payez pas la rançon

#9
☐ Conservez et consignez tout

#10
☐ Communiquez

BONUS : Restez vigilant

Pour plus de détails...

#1

Prévenez votre partenaire cyber

S'il connaît vos systèmes et vos habitudes, il sera le meilleur chef d'orchestre pour gérer la crise, isoler les postes infectés et coordonner les prochaines étapes.

#2

Contactez le 17Cyber

Si vous n'avez pas encore de partenaire identifié, ne perdez pas de temps, rendez-vous sur 17cyber.gouv.fr. Disponible 24h/24 et 7j/7, ce service national d'assistance vous oriente vers les services compétents et acteurs labellisés ExpertCyber proches de chez vous. Certains membres du Club Experts Cybersécurité sont en capacité d'intervenir en cas de cyberattaque. Référez-vous à l'annuaire pour les identifier et les solliciter.

#3

Activer un plan de gestion de crise

Si votre entreprise dispose d'un PCA (Plan de Continuité d'Activité) ou d'un PRA (Plan de Reprise d'Activité), activez-le pour minimiser les interruptions de services, garantir une reprise rapide de vos activités (y compris en mode dégradé) et maîtriser la communication interne comme externe.

#4

Identifiez l'origine et la portée de l'attaque

Avec votre partenaire ou votre équipe IT, qualifiez rapidement le point d'entrée et l'ampleur de l'incident. Dressez une cartographie de l'impact : postes et serveurs concernés, comptes touchés, données et sauvegardes potentiellement affectées, indices d'exfiltration de données, etc...

#5

Isolez le système infecté

Sur la base de ce premier diagnostic, endiguez sans détruire les preuves qui seront utiles aux enquêteurs : déconnectez du réseau les postes et serveurs compromis, désactivez les comptes compromis, évitez tout redémarrage, "nettoyage" ou réinstallation tant que les investigations ne l'exigent pas. Et bien évidemment, sécurisez vos sauvegardes pour prévenir toute nouvelle compromission.

#6

Prévenez votre assureur cyber

Certains contrats imposent une notification immédiate de l'incident pour que la couverture s'applique.
Ne tardez pas à les alerter.

#7

Déposez plainte

Dès la prise de connaissance de la cyberattaque, déposez plainte dans les 72h. La saisine immédiate des autorités permettra de considérer l'infraction comme un « flagrant délit ». Pré-plainte en ligne, Police, Gendarmerie, ReCym, OFAC, Procureur de la République sont vos relais.

#8

Ne payez pas la rançon

Céder au chantage ne garantit pas la restitution de vos données. Payer alimente le modèle économique des cybercriminels et fragilise encore davantage votre organisation.
Ne cédez pas !

#9

Conservez et consignez tout

Ne supprimez rien : e-mails frauduleux, captures d'écran, journaux systèmes, fichiers suspects... Tenez une « main courante » pour consigner ce qui arrive, ce qui a été fait, par qui et quand. Cette traçabilité sera précieuse pour comprendre l'attaque et améliorer votre résilience.

#10

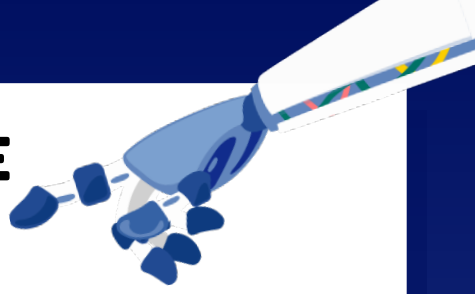
Communiquez

Adoptez une posture de transparence tout en adaptant votre niveau de langage auprès de vos collaborateurs, clients et partenaires. Aujourd'hui, être victime d'une cyberattaque est malheureusement monnaie courante. Expliquer clairement la situation et vos actions correctives devient un gage de confiance.

BONUS : Restez vigilant

Une attaque peut en cacher une autre. Dans les jours qui suivent, attendez-vous à des tentatives de rebond : phishing par e-mail, smishing par SMS, vishing par appels frauduleux, voire exploitation de vos données si elles ont fuité.

MON FOURNISSEUR EST VICTIME D'UNE CYBERATTAQUE



Dans un monde de plus en plus interconnecté, les entreprises dépendent souvent de prestataires de services pour assurer des fonctions clés comme la gestion informatique, les logiciels de production ou l'hébergement des données. Mais que faire lorsque l'un de vos prestataires devient lui-même victime d'une cyberattaque, compromettant ainsi votre capacité à opérer ?

Voici les étapes clés à suivre pour gérer cette situation de manière proactive et limiter l'impact sur votre activité.

QUE DOIS-JE FAIRE ?

#1
- [ ] Évaluer l'impact sur l'activité

#2
- [ ] Maintenir une communication active avec le fournisseur

#3
- [ ] Le dépôt de plainte n'est pas nécessaire

#4
- [ ] Activer le PCA

#5
- [ ] Vérifier les clauses contractuelles

#6
- [ ] Notifier l'assureur

#7
- [ ] Impliquer les parties prenantes

#8
- [ ] Solliciter un conseil juridique

#9
- [ ] Notifier la CNIL

#10
- [ ] Documenter et protéger

Pour plus de détails...

#1

☐ Évaluer l'impact sur l'activité

Avant toute chose, évaluez comment l'attaque **affecte vos opérations.**

L'interruption touche-t-elle des services critiques comme la production, la gestion des commandes ou la relation client ?
Quels systèmes ou logiciels sont concernés ?
Ce premier état des lieux vous permettra de prioriser les actions à mener.

#2

☐ Maintenir une communication active avec le fournisseur

Une fois l'impact identifié, prenez immédiatement contact avec votre fournisseur affecté pour **obtenir des informations détaillées.** Posez les questions suivantes :

1. Quelle est la nature de l'attaque dont ils sont victimes ?
2. Quelles mesures prennent-ils pour remédier à la situation et rétablir les services ?
3. Quel est le délai estimé de reprise de leurs activités ?
4. Existe-t-il une solution de contournement ou une alternative temporaire pour restaurer vos services critiques ?

Maintenir une **communication constante** avec votre fournisseur tout au long de la crise vous permettra d'**adapter votre propre gestion de crise**. N'accablez pas votre prestataire qui est tout autant sous pression. Vous verrez en temps voulu s'il est nécessaire de poursuivre ou non votre collaboration.

#3

☐ Le dépôt de plainte n'est pas nécessaire

Contrairement à une entreprise directement ciblée par une cyberattaque, en tant que victime collatérale, **vous n'êtes pas concerné par le dépôt de plainte.** En effet, l'attaque n'est pas dirigée directement contre votre organisation, mais contre celle de votre prestataire.
L'interruption de service relève alors d'un **litige commercial.**

#4

☐ Activer le PCA

Si votre prestataire est victime d'une attaque et que vous subissez des interruptions de services, activez votre Plan de Continuité d'Activité (PCA). Ce plan doit inclure des **solutions de repli en cas d'indisponibilité d'un prestataire**. Par exemple, cela pourrait impliquer le recours à un fournisseur de secours, l'utilisation de solutions cloud alternatives, ou la réallocation temporaire des tâches externalisées à des services internes.

La robustesse de votre PCA est cruciale pour **minimiser l'impact** de la situation sur vos propres clients et maintenir la continuité de vos opérations autant que possible. En dernier recours, il vous reste les bons vieux Monsieur Papier et Madame Stylo.

#5

☐ Vérifier les clauses contractuelles

Votre contrat avec votre prestataire inclut probablement des **accords de niveau de service** (SLA : Service Level Agreement) ainsi que des clauses contractuelles définissant les obligations et responsabilités de chaque partie en cas d'interruption de service.
Vérifiez attentivement ces documents pour comprendre :

- Les **garanties de continuité d'activité** en cas d'incident cyber affectant le prestataire
- Les **pénalités** prévues pour les manquements aux SLA
- Les **recours disponibles** pour obtenir des compensations ou des solutions alternatives si l'interruption se prolonge

Ces clauses sont essentielles pour faire valoir vos droits et **limiter l'impact sur votre activité**. Si des clauses de redondance existent, votre fournisseur devrait être en mesure de proposer des **services de secours** pour réduire la durée de l'interruption.

Pour plus de détails...

#6

☐ Notifier l'assureur

Même si vous n'êtes pas la cible directe de l'attaque, il est important d'**avertir immédiatement votre assureur** pour vérifier vos clauses de couverture en cas de défaillance de fournisseurs critiques. Votre assureur pourrait vous indiquer les démarches à suivre ou vous aider à **réduire l'impact financier de la crise.**

Si votre assureur réagit mal ou refuse de prendre en compte votre situation, vous saurez qu'il est peut-être temps de réévaluer votre contrat et de choisir un autre assureur plus adapté à vos besoins.

#7

☐ Impliquer les parties prenantes

Dans une telle situation, il est essentiel d'impliquer rapidement les bonnes parties prenantes, tant internes qu'externes :

Internes : Alertez immédiatement votre direction, vos équipes IT, et vos départements concernés (production, relation client) afin qu'ils se préparent à gérer les impacts opérationnels et techniques de l'interruption. Assurez-vous que tous les collaborateurs comprennent la situation et savent quelles actions sont à entreprendre.

Externes : Informez vos clients et partenaires de l'impact potentiel sur vos services. Adoptez une communication transparente, notamment si des retards de livraison ou des interruptions de service sont à prévoir. Une gestion proactive de la communication permet souvent de préserver la confiance et d'éviter de nouvelles tensions.

#8

☐ Solliciter un conseil juridique

Impliquez immédiatement votre conseil juridique afin qu'il vous aide à comprendre les **obligations contractuelles** de votre fournisseur ainsi que vos propres obligations envers vos clients et partenaires. Il vous conseillera également sur les démarches à entreprendre pour **minimiser les risques légaux**, notamment si la crise affecte gravement la continuité de vos services ou entraîne des répercussions contractuelles.

Votre conseil juridique pourra également vous guider sur les actions à entreprendre si la situation devient critique, notamment en termes de réclamations, de ruptures de contrat ou de responsabilités partagées. Si votre conseil est dépassé, demandez-lui de vous orienter vers un confrère expérimenté dans ce type de situation.

#9

☐ Notifier la CNIL

Si l'interruption de service causée par votre fournisseur a entraîné une **violation des données personnelles** de vos clients ou de vos employés, vous avez **l'obligation légale de notifier cet incident à la CNIL** (Commission Nationale de l'Informatique et des Libertés) dans un délai maximal de 72 heures. Cette notification est cruciale pour respecter la conformité avec le RGPD et éviter d'éventuelles sanctions.

Assurez-vous de bien **documenter** tous les détails de l'incident, y compris les actions entreprises par votre fournisseur pour contenir l'attaque afin de pouvoir fournir des informations complètes à la CNIL.

#10

☐ Documenter et protéger

Pendant toute la gestion de la crise, il est impératif de documenter chaque action, chaque communication et chaque décision prise. Cela comprend les échanges avec votre fournisseur, les notifications à la CNIL, les décisions internes ainsi que toutes les actions de remédiation.

De plus, si votre fournisseur détient des données sensibles ou gère des infrastructures critiques pour votre entreprise, vérifiez auprès de lui que vos données n'ont pas été compromises dans l'attaque. Si nécessaire, **demandez une confirmation formelle et écrite de la sécurité des informations qui vous concernent.** Par ailleurs, il peut être judicieux d'isoler temporairement certains flux de données ou de systèmes jusqu'à ce que la situation soit sous contrôle.

Cette documentation sera précieuse en cas d'audit, de réclamations légales, ou de discussions avec vos assureurs et partenaires. Elle servira aussi à analyser la situation a posteriori pour **renforcer vos processus internes** et ajuster vos contrats.

Les idées reçues sur la cybersécurité et l'assurance cyber

Les petites et moyennes entreprises pensent souvent qu'elles ne sont pas des cibles parce qu'elles ne sont pas des géants de la tech.

Faux. Les cyberattaques ne ciblent pas que les grands groupes. En 2024, TPE et PME sont les principales victimes des cyberattaques en France, représentant 60% des cyberattaques.

La complexité de certaines offres freine la souscription.

Vrai. 0,3% des TPE et PME sont équipées d'une assurance cyber. En réponse, nous avons développé un parcours de souscription ultra-pédagogique avec des conseils à chaque étape.

Le coût de l'assurance cyber est très élevé.

Faux. Nous avons conçu une assurance cyber à partir de 29€/mois et ultra-personnalisée avec +10 critères de personnalisation.

Faut-il payer ou non la rançon ?

Chez Onlynnov, notre réponse est double.

« D'un côté, il ne faut pas payer. Céder à une demande de rançon, c'est alimenter les finances du crime organisé et encourager la répétition de ces attaques.
Mais de l'autre, nous ne pouvons pas non plus dire à un chef d'entreprise de laisser mourir sa société, ses emplois, son outil de travail, au nom d'un principe.

C'est pourquoi, chez Onlynnov, nous défendons une approche pragmatique et responsable :
- **Renforcer la résilience du système d'information**, avec des sauvegardes fiables, applicatives et données, sur des périodes longues. Et surtout, tester régulièrement le plan de continuité d'activité pour s'assurer que ces sauvegardes sont réellement exploitables.
- **Déposer plainte dans les 72h**, comme l'exige la réglementation, pour permettre aux forces de l'ordre d'enquêter et, si possible, de démanteler les réseaux criminels.
- **Prévoir en dernier recours une garantie de paiement de rançon dans le contrat d'assurance**.
Si toutes les autres options échouent, cette garantie permet d'obtenir une clé de déchiffrement et de sauver l'entreprise.

Cette approche permet de protéger efficacement les entreprises, tout en limitant au maximum le recours au paiement. Elle est d'ailleurs alignée avec la position du législateur français.

En tant que dirigeant, je crois qu'il faut sortir des postures idéologiques pour proposer des solutions concrètes, équilibrées et responsables. »

Guillaume SANTIAGO, CEO d'Onlynnov

ASSURANCE CYBER

ONLYNNOV
L'ASSURANCE DES **ENTREPRISES TECH**

L'assurance cyber sur-mesure et performante d'Onlynnov

Protégez-vous des risques numériques avec une assurance cyber puissante.
Piratage informatique, cyber risques, violation de données, ransomware : l'assurance sur-mesure adaptée à votre métier et votre chiffre d'affaires.

À partir de 29€/mois	**Jusqu'à 5 millions d'euros de garanties**	**Cyberprotection dans le monde entier**	**Assistance 24h/24 et 7j/7**

L'audit de votre assurance cyber a pour objectif d'identifier les lacunes, d'évaluer les risques spécifiques et garantir que votre politique d'assurance cyber est adaptée.
Profitez d'un audit complet de votre cyber assurance pour optimiser **le coût de votre assurance.**

Qui est Onlynnov ?

Onlynnov est l'assurance des entreprises tech. Nous faisons de votre assurance un vrai atout pour votre business. Numérique, santé et électronique, nous concevons +20 contrats d'assurance sur-mesure pour vous accompagner à chaque étape de votre croissance.

Pourquoi être partenaire Digital League ?

Editeurs de logiciel, agence web, entreprise des services numériques, consultant et audit cyber : c'est parce que nous comprenons votre métier que nous assurons le bon risque.

Être partenaire historique de Digital League nous place au cœur de l'écosystème tout en nous permettant de rester connecté aux innovations du secteur du numérique.

RC Pro, Responsabilité des Dirigeants, Cybersécurité ou encore Multirisque :
comprendre et intégrer les technologies des adhérents de Digital League est la garantie de toujours proposer la bonne assurance adaptée aux étapes de croissance de votre entreprise.

Retour d'expérience EFALIA

Début juillet 2024, EFALIA finalise, à l'issue d'un audit, la souscription d'une assurance cyber adaptée à ses risques métiers. Le 31 juillet à 9 h, un ransomware paralyse serveurs et système de facturation. Les bons réflexes techniques s'enchaînent, puis la gestion de crise s'organise. En 1h30, l'assistance prévue au contrat mobilise les experts (réponse à incident, forensic), le juridique (plainte, CNIL) avec un plan de reprise structuré pour éviter toute ré-infection. La communication de crise, quant à elle, est gérée par les équipes d'EFALIA tout en la faisant valider par l'assureur.

Dans cette séquence, le rôle d'Onlynnov ne s'est pas limité à déclarer le sinistre : le courtier a orchestré la coordination, suivi chaque décision avec la direction/DSI et porté les intérêts d'EFALIA auprès de l'assureur. A la clôture de l'incident, une offre d'indemnisation initiale de 70 % a été négociée à 85 %.

En 90 jours, l'activité est repartie, avec un cloisonnement renforcé, des sauvegardes mieux segmentées et testées mais aussi des procédures de réponse réajustées. Sans couverture ni assistance, l'entreprise estime au moins à six mois la période d'interruption, avec un risque de défaillance. L'assurance achète du temps critique, structure la décision et accélère la reconstruction.

« Ce qu'on prévoyait de faire en un an, on l'a fait en trois mois. » Pascal Charrier, EFALIA

Retrouvez l'étude de cas complète ici : https://onlynnov.com/cybersecurite/etude-de-cas-efalia/

Cyberattaque : qui paie les dégâts ?

Parler d'argent, c'est parler de responsabilités partagées. En cas de cyberattaque, l'entreprise reste responsable devant ses clients et la loi au regard de la protection des données comme de la continuité de service.

Autour, deux types de prestataires peuvent entrer en scène : **d'abord le fournisseur d'outils (logiciel SaaS, hébergeur), ensuite le prestataire cyber/infogéreur.**

Le fournisseur d'outils.
Il doit livrer un service sûr (correctifs, surveillance, notification d'incident) et tenir ses engagements de continuité comme de disponibilité. Mais l'entreprise garde la main sur ses choix et ses paramètres : droits d'accès, sauvegardes, journalisation, plan de continuité en cas d'arrêt. Un défaut de configuration côté entreprise ou l'absence de sauvegardes reste à la charge de ce dernier.

Prestataire cyber/infogéreur.
C'est un « sachant » ayant une obligation de conseil, d'alerte et d'exécution conforme à l'état de l'art. Ne pas signaler un risque évident ou tarder à corriger peut engager sa responsabilité. Néanmoins, l'entreprise décide, arbitre les priorités, valide les budgets et doit appliquer les recommandations. Ignorer un avis critique ou repousser indéfiniment une mise à jour pèse alors sur elle.

La clé de voûte.
Des contrats clairs (qui fait quoi, délais de remise en service, quantité de données qu'on accepte de perdre, preuves à conserver, pénalités et limites) et une assurance alignée (pré-requis, exclusions, articulation avec celle du prestataire). Une prévention bien documentée déterminera, le jour J, qui paie quoi. Pour y voir plus clair, n'hésitez pas à prendre attache auprès d'un avocat spécialisé en droit du numérique. Pour cela, regardez parmi les partenaires juridiques de Digital League, sélectionnés entre autre, pour cette compétence.

Par où commencer ?

Dirigeant, l'enjeu n'est pas de tout transformer d'un coup, mais de faire une photo à l'instant T, puis d'avancer par petites touches avec des objectifs atteignables.
Ce parcours en 5 étapes vous aidera à insuffler le mouvement sans tout révolutionner : diagnostiquer, désigner un pilote, poser les gestes qui sauvent, préparer votre plan de continuité et enfin mettre en place un processus d'amélioration continue alignée sur votre réalité terrain.

1. Comprendre où vous en êtes

Faites une photo à l'instant T de votre exposition (outils, données, partenaires, faiblesses).
Pas besoin d'un audit lourd : **l'objectif est de prioriser vite et bien**.

CONCRÈTEMENT :
- Recensez vos actifs critiques (production, ERP, messagerie, données clients…)
- Notez vos incidents passés et vos "points de douleur"
- Passez un test simple de maturité pour objectiver le point de départ (prise de conscience)

4. Préparer vos équipes et votre plan de réaction

Transformez la prise de conscience en réflexes ; préparez un PCA (Plan de Continuité d'Activité) simple pour gagner de précieuses heures le jour J.

CONCRÈTEMENT :
- Sensibilisez aux pièges courants (phishing, faux support, pièces jointes)
- Ecrivez une fiche réflexe : qui alerter, quoi isoler, où sont les sauvegardes
- Tenez à jour la liste des contacts utiles (contacts des salariés, prestataire, 17Cyber, assurances, police/gendarmerie, DPO/CNIL)

5. Tester et se renforcer chaque année

Un rendez-vous annuel pour tester, mesurer, ajuster et progresser :
c'est votre moteur d'amélioration continue.

CONCRÈTEMENT :
- Refaire un test de maturité pour voir les progrès.
- Mettre à jour votre plan (priorités, budgets, conformité…).
- Capitaliser sur les retours d'expérience (incidents, exercices, audits).

2. Désigner un pilote de la cybersécurité

Insufflez le mouvement en désignant un référent (interne ou externe) qui centralise, coordonne, et vous alerte.
Pas de révolution interne : **juste un point de contact clair**.

CONCRÈTEMENT :
- Nommez un référent (cadre, DSI, prestataire de confiance)
- Donnez-lui mandat, moyens et disponibilité
- Alignez la cyber sur vos objectifs métier (continuité, délais, image, conformité)

3. Mettre en place les protections de base

Commencez par petites touches avec les gestes qui sauvent : ils répondent déjà à l'essentiel, sans tout bouleverser.

CONCRÈTEMENT :
- Sauvegardes régulières testées
- Mises à jour automatiques
- Mots de passe robustes + MFA (double authentification)
- Protection des postes & emails
- Gestion des droits d'accès

Ressources

Pour faciliter votre parcours, nous avons sélectionné pour vous des ressources officielles, francophones, classées par étape et pertinentes pour un décideur.

Etape 1 : Comprendre où vous en êtes

Identifiez dans ce guide les membres du Club Experts Cybersécurité répondant à la catégorie « **Gouvernance** » pouvant réaliser des audits, tests d'intrusion.

- **ANSSI** - Test de maturité cyber en ligne : https://messervices.cyber.gouv.fr/test-maturite/

- **France Num** - Test de maturité cyber en ligne : https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/test-cybersecurite-etes-vous

- **MonAideCyber** - Diagnostic de 1er niveau gratuit avec un ambassadeur : https://monaide.cyber.gouv.fr/

- **Gendarmerie Nationale** – Pré-diagnostic avec un cyber-gendarme : https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/avec-diagonal-le-pre-diagnostic

Etape 2 : Désigner un pilote

Identifiez dans ce guide les membres du Club Experts Cybersécurité répondant à la catégorie « **Gouvernance** » pouvant vous accompagner dans votre stratégie cyber.

- **Auvergne-Rhône-Alpes Entreprises** – Panorama des acteurs cyber : https://plateforme-iet.auvergnerhonealpes-entreprises.fr/informations-economiques/publications/panorama-des-acteurs-de-la-cybersecurite-en-auvergne-rhone-alpes

- **ANSSI** – Guide de bonnes pratiques : https://cyber.gouv.fr/guides-essentiels-et-bonnes-pratiques-de-cybersecurite-par-ou-commencer

- **Cybermalveillance** – Fiches réflexes : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/liste-des-ressources-mises-a-disposition

- **Cybermalveillance** – Se faire accompagner par un prestataire labellisé ExpertCyber : https://www.cybermalveillance.gouv.fr/label-expertcyber

Etape 3 : Mettre en place les protections de base

Identifiez dans ce guide les membres du Club Experts Cybersécurité répondant aux catégories « **Protection** » et « **Défense** » pouvant vous aider à réduire votre exposition et les attaques du quotidien

- **ANSSI** – Guide d'hygiène informatique : https://cyber.gouv.fr/publications/guide-dhygiene-informatique

- **ANSSI** – Recommandations relatives aux mots de passe : https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe

- **Cybermalveillance** – Comment bien gérer ses sauvegardes : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

- **CERT-FR** – Suivre les alertes & correctifs critiques : https://www.cert.ssi.gouv.fr

Etape 4 : Préparer vos équipes & votre plan de réaction

Identifiez dans ce guide les membres du Club Experts Cybersécurité répondant aux catégories « **Gouvernance** », « **Défense** » et « **Résilience** » pour vous aider à vous préparer.
Participez et faites participer vos salariés à des sessions de sensibilisation organisées par les pôles & clusters de la région, agences Auvergne-Rhône-Alpes Entreprises, ENE, CCI, Campus Région du numérique, organisations syndicales et patronales, etc...

- **SecNumAcadémie** – formation en ligne gratuite : https://secnumacademie.gouv.fr/

- **ANSSI** – Anticiper et gérer une crise cyber : https://cyber.gouv.fr/anticiper-et-gerer-une-crise-cyber

- **CNIL** – Violation de données : que faire ? : https://www.cnil.fr/fr/cybersecurite/les-violations-de-donnees-personnelles

Etape 5 : Tester et se renforcer chaque année

Identifiez dans ce guide les membres du Club Experts Cybersécurité répondant aux catégories « **Gouvernance** », « **Défense** » et « **Résilience** » pour vous tester, vous entraîner et réagir en cas de cyberattaque.

- **ComCyber-MI** – Rapport annuel sur la cybercriminalité : https://www.interieur.gouv.fr/actualites/communiques-de-presse/publication-du-rapport-annuel-relatif-a-cybercriminalite

- **Cybermalveillance** – Initiation à la gestion de crise pour les TPE/PME : https://www.cybermalveillance.gouv.fr/gestion-de-crise/sency-crise

- **ANSSI** – Organiser un exercice de gestion de crise : https://cyber.gouv.fr/publications/organiser-un-exercice-de-gestion-de-crise-cyber

- **17Cyber** - Guichet unique d'alerte & d'assistance : https://17cyber.gouv.fr/

COMMENT BIEN CHOISIR SON PARTENAIRE CYBER ?

Choisir un prestataire cyber, c'est comme choisir un copilote : il doit être compétent, fiable, réactif... mais aussi comprendre votre métier et parler votre langage. Dans un marché foisonnant, il est parfois difficile de s'y retrouver. Voici les **10 critères incontournables** pour avancer en confiance.

1) Reconnaissance officielle

Privilégiez les prestataires disposant de labels, certifications ou qualifications reconnues : ISO27001, PASSI, SecNumCloud, PRIS, etc... Ces repères attestent d'un socle de qualité et de conformité.

2) Réputation et références sectorielles

Un bon partenaire a déjà accompagné des entreprises comparables à la vôtre : TPE, PME, ETI, collectivités ou acteurs d'un secteur spécifique (santé, industrie, services...).
C'est la garantie qu'il connaît vos réalités.

3) Compréhension de vos besoins métiers

La cybersécurité n'est pas une fin en soi, mais un moyen de protéger votre activité. Votre partenaire doit partir de vos priorités (continuité de service, protection de données sensibles, télétravail, conformité) et non d'une solution pré-formatée. Il connaît donc votre terrain de jeu.

4) Clareté du langage et pédagogie

La cybersécurité regorge d'acronymes (EDR, SOC, XDR, SASE...). Un bon prestataire doit savoir traduire ces termes en bénéfices clairs pour votre entreprise, et vous parler simplement.
C'est à lui de s'adapter à vous, pas l'inverse.

5) Clarté du périmètre et intégration dans l'écosystème

Un expert cyber peut être spécialisé (pentest, RSSI à temps partagé, sensibilisation, matériel) ou plus généraliste. L'essentiel est qu'il soit transparent sur son champ d'action et qu'il sache mobiliser un écosystème reconnu pour compléter ses compétences.
A l'instar des membres du Club Experts Cybersécurité présents dans ce guide qui s'emploient à travailler dans une logique de réseau pour toujours mieux répondre à vos besoins.

6) Réactivité et rôle de prescripteur

En cas d'incident, la rapidité d'intervention est cruciale. Mais si le prestataire atteint ses limites, vous mesurerez sa vraie valeur : sa capacité à activer immédiatement ses partenaires de confiance.
Comme un médecin, il intervient directement dans son champ et prescrit les bons spécialistes ou solutions (assurance cyber, conformité réglementaire, recyclage sécurisé du matériel...).

7) Transparence contractuelle et financière

Un contrat clair inspire confiance : délais d'intervention, responsabilités, coûts cachés... Demandez des engagements lisibles et comparables, pour éviter les mauvaises surprises.

8) Capacité d'évolution et d'adaptation

Votre organisation évolue : croissance, internationalisation, nouveaux outils. Votre partenaire doit proposer des solutions évolutives, capables de s'adapter à vos changements sans vous enfermer.

9) Respect des réglementations et souveraineté des données

Un partenaire sérieux maîtrise les obligations légales (RGPD, NIS2, Cyber Resilience Act...) et garantit que vos données restent hébergées en France ou en Europe, dans le respect de la souveraineté numérique.

10) Pérennité et solidité

La cybersécurité est une relation de long terme. Choisissez un prestataire stable financièrement, durablement implanté, et reconnu dans l'écosystème comme ceux du Club Experts Cybersécurité de Digital League.

La checklist du dirigeant

Avant de signer, posez-vous ces questions ?

- ☐ *« Est-il reconnu par un label ou une certification officielle ? »*
- ☐ *« A-t-il déjà accompagné des entreprises comparables à la mienne ? »*
- ☐ *« Comprend-il mes priorités métier ? »*
- ☐ *« Me parle-t-il simplement, sans jargon inutile ? »*
- ☐ *« Est-il clair sur ce qu'il couvre et bien intégré dans un écosystème comme Digital League ? »*
- ☐ *« Peut-il intervenir vite et prescrire les bons spécialistes si besoin ? »*
- ☐ *« Son contrat est-il transparent, sans frais cachés ? »*
- ☐ *« Ses solutions évolueront-elles avec mon entreprise ? »*
- ☐ *« Mes données resteront-elles protégées et souveraines ? »*
- ☐ *« Est-il solide et présent dans la durée ? »*

En résumé

Un bon partenaire cyber n'est pas forcément « expert en tout ».
C'est un **allié stratégique** de votre entreprise, compétent dans son domaine, capable de vous expliquer clairement les enjeux, et de s'appuyer sur un réseau solide pour couvrir l'ensemble de vos besoins.

Digital Leads

Trouver le bon prestataire, sans perdre de temps

Trouver les bons partenaires métiers dont vous avez besoin pour répondre à vos projets numérique (dont cyber) et donner un coup d'accélérateur à votre activité ?

C'est ce que propose **Digital Leads**, un service facilitant la mise en relation entre les entreprises du secteur numérique de la Région, avec pour objectif de **favoriser la création de collaborations locales.**

Que vous soyez à la recherche de spécialistes en cybersécurité, en logiciel de gestion, en communication digitale ou bien encore en solution d'intelligence artificielle, **Digital Leads est là pour simplifier vos recherches de partenaires qualifiés**, grâce à l'écosystème Digital League composé d'entreprises expertes dans le numérique.

Comment ça marche (simple, rapide et gratuit) :

1) **Rendez-vous** sur https://digital-league.org/digital-leads

2) **Exprimez votre besoin** grâce au formulaire dédié.

3) **Votre besoin est partagé de manière anonyme** aux adhérents du réseau Digital League.

4) Nous faisons une **short-list des adhérents** candidats pertinents.

5) Une mise en relation est faite et **c'est alors à vous d'échanger**, comparer, décider.

Panorama des acteurs cyber en région

A l'initiative de la Région, l'Agence Auvergne-Rhône-Alpes Entreprises, en partenariat avec les pôles et cluster régionaux, dont Digital League, a réalisé ce panorama.

Régulièrement mis à jour, ce document souligne la richesse des expertises en cybersécurité présentes en Région avec notamment une capacité de réponse complète des acteurs régionaux pour accompagner les entreprises régionales face à la montée en puissance et aux méthodes d'intrusion de plus en plus ingénieuses des cyberattaquants.

Découvrez dans ce panorama les principales caractéristiques et compétences des acteurs régionaux positionnés sur les quatre grandes compétences de la cybersécurité : **Gouvernance, Protection, Défense et Résilience/Remédiation**.

URL : https://plateforme-iet.auvergnerhonealpes-entreprises.fr/informations-sectorielles/cartes-et-annuaires/carte-dynamique-des-acteurs-de-la-cybersecurite-en-auvergne-rhone-alpes

La Région
Auvergne-Rhône-Alpes
ENTREPRISES

Description des catégories d'expertises CYBER

GOUVERNANCE

Il s'agit de **mettre de l'ordre et de la méthode.**
On identifie les risques, on fixe des règles simples (qui fait quoi, avec quels accès), on cartographie les données importantes et on sensibilise les équipes.

- Assurance
- Audit organisationnel
- Audit technique
- Juridique
- Exercice de crise
- Cartographie
- Analyse des risques
- Politique de sécurité
- Audit organisationnel
- Analyse de la surface d'attaque
- Ordonnancement / planification
- Classification de la donnée
- Veille sur la menace / CTI

Objectif :

Prendre des décisions claires, établir des priorités et engager un processus d'amélioration continue.

PROTECTION

Il s'agit de **fermer les « portes et fenêtres » de vos actifs.**
On protège vos postes, serveurs, mobiles, réseaux, comptes et données (politique mots de passe, mises à jour, configurations, sauvegardes, segmentation, protection des données stratégiques).

- Audit de code source
- Exercice de PRI / PCI
- Protection des terminaux mobiles
- Solution de chiffrement
- Protection de la donnée
- Protection des produits
- Solution de chiffrement
- Protection des postes de travail
- Veille e-réputation et fuite des données
- Protection des infrastructures
- Protection des services
- Communication / sensibilisation
- Protection des communications
- Gestion des identités

Objectif :

Réduire fortement l'exposition et les attaques du quotidien.

Description des catégories d'expertises CYBER

DÉFENSE

Il s'agit de **surveiller et agir** quand quelque chose cloche. Surveillance continue, détection d'anomalies, alerte, réponse rapide en cas d'incident et tests réguliers pour vérifier la solidité.

SOC | SIEM | SecDevops | Dashboards sécurité | Réponse à un incident

Analyse forensiques | Patch Management | MCO | Service de sécurité infogérés

Cloud de confiance | Chiffrement | Blockchain | Archivage | Pentest

Exercice de crise | Exercice de PRI / PCI | Bugbounty

Objectif :

Raccourcir le délai entre l'attaque et l'action pour limiter l'impact.

RÉSILIENCE

Il s'agit de **redémarrer vite et en toute confiance**.
Plans de continuité et de reprise (PCA/PRA), organisation de la gestion de crise, sauvegardes vérifiées et restauration testée, collecte des éléments utiles après incident.

Forensique | Conversation de la preuve | Pilotage PRA / PCA | Réponse à un incident

Procédure UDRP USR | IAAS sécurisée

Gestion de crise

Objectif :

Transformer un incident en contretemps maîtrisé et non en catastrophe.

LES MEMBRES DU CLUB EXPERTS CYBERSÉCURITÉ (1/5)

Ad Confirma

Ad Confirma est un cabinet de conseil et d'audit en cybersécurité spécialisé en gouvernance, risques et conformité. Nos experts vous accompagnent sur la mise en œuvre, le contrôle et l'audit des normes et règlements en lien avec la cybersécurité.

https://www.adconfirma.com

Gouvernance | Résilience

Agaetis

https://agaetis.tech/

Agora Calycé

Chez Agora Calycé, la cybersécurité est au cœur de notre ADN. Nous ne sommes pas qu'un prestataire technique : nous sommes des conseillers de confiance. Chaque projet Cloud/Infrastructure est une occasion pour nous d'accompagner et conseiller.

https://www.agoracalyce.com/

Gouvernance | Protection | Défense | Résilience

AIoTrust

AIoTrust développe des systèmes intelligents destinés à fournir aux industriels des données de confiance afin d'analyser les performances de leur installation et de détecter des anomalies pouvant provenir de cyber-attaques ou de déviations naturelles.

www.aiotrust.io

Protection | Résilience

Akant

Akant, cabinet de conseil où la conformité cyber devient un levier de confiance.
ISO, SOC2, NIS2, DORA, IA Act... Nos experts passent du stratégique à l'opérationnel, de l'audit au RSSI externalisé, avec une approche concrète et une authenticité assumée.

https://www.akant.fr/

Gouvernance

Akenatech

Akenatech est un prestataire de services en cybersécurité industrielle OT/IoT :
- Conseil : NIS2, Cyber Resilience Act, marquage CE, ISO 27001, IEC 62443.
- Solutions : intégrateur de logiciels et matériel de cybersécurité.
- Services : RSSI à temps partagé.

www.akenatech.com

Gouvernance | Protection

Aldene

ALDENE, certifié ExpertCyber, protège vos organisations face aux cybermenaces.
De la détection à la remédiation, nous sécurisons vos données, vos usages et vos infrastructures pour une confiance numérique durable.

www.aldene.fr

Gouvernance | Protection | Défense | Résilience

Algosecure

Entreprise indépendante de cybersécurité basée à Lyon, AlgoSecure aide les entreprises et organismes publics à sécuriser leur système d'information : audit, conseil, surveillance (EASM) et réponse aux incidents.
Qualifié PASSI par l'ANSSI & certifié ISO 27001.

https://www.algosecure.fr

Gouvernance | Protection | Défense | Résilience

Amiltone

Sécurité applicative intégrée au cycle de dev : audits de code SAST/SCA/DAST, remédiations et coaching d'équipes.
Objectif : livrer des applications web/mobile plus robustes, conformes et performantes, en détectant les vulnérabilités au plus tôt.

https://appsec.amiltone.com/

Défense

AntemetA

AntemetA déploie une offre de cyber-résilience basée sur le risque comprenant : cybersécurité (assets & identités), protection des données (backup & S3 immuable) et continuité (PRA). Son offre Sanctuaire garantit une protection souveraine et cohérente à 360°.

www.antemeta.fr

Protection | Défense | Résilience

Aphelio

Aphelio est une société française de cybersécurité, basée à Valence et Grenoble. Nous proposons à la fois des prestations cyber (audits, conseil, intégration, sécurisation, accompagnement ISO 27001...) et des logiciels pour sécuriser vos infrastructures.

https://aphelio.fr/

Gouvernance | Protection | Défense

Apitech

Apitech, éditeur français d'open solutions, propose des outils collaboratifs souverains (chat, visio, mail, drive) hébergés en France.
Sa solution Krisalee isolée du SI permet d'assurer la communication avant, pendant et après une crise cyber.

https://apitech.fr

Résilience

LES MEMBRES DU CLUB EXPERTS CYBERSÉCURITÉ (2/5)

Arsium

ARSIUM accompagne les industries et organisations dans la mise en œuvre de solutions IT fiables, sécurisées et sur-mesure. Nous intervenons à travers quatre domaines clés : Cybersécurité, Infrastructure & Réseaux, Développement, Support IT.

https://www.arsium.fr/

Gouvernance | Protection | Défense | Résilience

Artecys

Artecys est un cabinet de conseil et d'audit en cybersécurité qui vous accompagne dans toute la France. Nos experts évaluent vos risques, vous conseillent pour renforcer vos défenses et bâtir une culture de sécurité alignée sur vos objectifs métier.

https://www.artecys.com/

Gouvernance | Défense

ASC2SI

ASC2SI sécurise vos systèmes d'information : audits, gouvernance cybersécurité, conformité RGPD et formations sur mesure.
Un partenaire de confiance pour anticiper les menaces et garantir la protection de vos données.

https://asc2si.fr

Gouvernance

ATN Groupe

ATN GROUPE, le partenaire cyber des PME et ETI : une plateforme de management et des solutions innovantes alliant Gouvernance, Protection, Défense et Résilience. Dirigeant, DSI et Experts unis pour une cybersécurité pragmatique et en amélioration continue.

www.atngroupe.fr

Gouvernance | Protection | Défense | Résilience

Avangarde Cyber Sécurité

Avangarde Cyber Sécurité est un pure «Player» Cyber (basé à Lyon 3e), proposant des services de conseils, d'audit/pentest ainsi qu'un centre de cyber défense (SOC - CERT - CTI) répondant à vos enjeux de conformités règlementaires et défis techniques.

https://www.avangardecyber.fr/

Gouvernance | Protection | Défense | Résilience

Axess

Axess vous accompagne dans vos enjeux de cybersécurité. Nous renforçons la résilience de vos SI grâce à une surveillance continue, des audits avancés, la sensibilisation de vos collaborateurs et une défense active face aux menaces les plus critiques.

https://www.axess.fr/

Gouvernance | Protection | Défense | Résilience

BPR Security

Cabinet cyber IT/OT. Audits et feuilles de route, gouvernance ISO 27001, sécurité opérationnelle et réponse à incident.
Exercices de crise et priorisation des actions pour renforcer vos défenses et la continuité d'activité, du terrain au comité de direction.

https://www.bprsecurity.fr

Gouvernance | Protection | Défense | Résilience

CPE Lyon

CPE Lyon est une école d'ingénieurs qui dispense des formations dans 3 domaines : «chimie», «biotechnologies» et «sciences et technologies du numérique». Un diplôme et des spécialisations dans plusieurs autres programmes sont dédiés à la cybersécurité.

https://www.cpe.fr/

Gouvernance | Protection | Défense | Résilience

CSB.School

CSB.school, fondée par des experts en cybersécurité, forme les talents de demain avec un Bachelor (Bac+3) et un Mastère (Bac+5) labellisés SecNumEdu par l'ANSSI. Basée au Campus Région du numérique, son modèle allie technique, management et besoins du marché.

https://www.csb.school/

Gouvernance | Protection | Défense | Résilience

Cybalgoris

Cybalgoris propose Cybernoe®, le premier assistant Secure by Design. Une plateforme complète pour intégrer la sécurité dès la conception : règles de sécurité par tâche, formation au fil des besoins, suivi des process et traçabilité de la sécurité, conformités.

https://cybernoe.fr/

Gouvernance

CyberNetDefense Intelligence

CyberNetDefense Intelligence est une société spécialisée en expertise de sécurité numérique accompagnant les entreprises dans la protection de leurs actifs critiques, en identifiant les risques juridiques, techniques et opérationnels liés à leurs contrats.

https://cndi.pro

Gouvernance | Protection | Défense | Résilience

CyGO Entrepreneurs

Premier startup studio européen dédié à la cybersécurité, nous bâtissons des startups nées en Europe et à l'ambition mondiale. Nous concevons et développons ces startups en tant que co-fondateurs, équipes opérationnelles et investisseurs.

https://cygo-entrepreneurs.com/

Protection

LES MEMBRES DU CLUB EXPERTS CYBERSÉCURITÉ (3/5)

Devensys Cybersecurity

Devensys : Pure player_: pentest/Red Team, SOC 24/7 (<30 min), CERT/IR et formation. Détection rapide, gestion de crise et remédiations guidées pour limiter l'arrêt d'activité. Une couverture offensive et défensive adaptée aux PME, ETI et acteurs publics.

https://www.devensys.com/

Gouvernance | Protection | Défense | Résilience

Dstny

Dstny Entreprises accompagne et conseille les PME et ETI pour collaborer efficacement, partout et en toute sécurité, grâce à son expertise et à ses solutions de cybersécurité, de Cloud, d'UCaaS et de connectivité. Support 24/7 et proximité garantis.

https://www.dstny.fr/

Gouvernance | Protection | Défense | Résilience

Elysium Security

Expertise technique, formations et solutions souveraines autour de la protection des systèmes d'information pour accompagner des organisations de tous types. Une approche unifiée pour réduire le risque et optimiser les coûts d'exploitation.

https://www.elysium-security.com/

Gouvernance | Protection | Défense | Résilience

Esynov

Esynov forme et audite les entreprises dans leur maîtrise de la cybersécurité des produits et SI. Notre mission: sécuriser vos développements, anticiper les risques et renforcer les compétences de vos équipes.

https://www.esynov.fr/

Gouvernance | Protection | Défense | Résilience

Evicys

Evicys – Votre cybersécurité sur mesure : Diagnostic, Conseil, RSSI à temps partagé, VOC, Conformité et Cyber OT. Une expertise opérationnelle et stratégique pour protéger vos données, anticiper les menaces et garantir votre cybersécurité au quotidien.

https://www.evicys.com/

Gouvernance | Protection | Défense | Résilience

Excube

EXCUBE, cabinet de conseil indépendant lyonnais de 35 consultants, accompagne les PME, ETI et Grands Groupes sur leurs besoins de CyberGouvernance (GRC), de CyberDéfense (Cadrage et AMO SOC et outillage, besoins SECOP), de CyberRésilience et d'audits/pentests.

https://www.excube.fr/

Gouvernance | Protection | Défense | Résilience

Gardeners - Cyber.Stories

Du jamais vu. Les dispositifs de sensibilisation à la cyber «Cyber.Stories» ce sont : des histoires façon série Netflix, des personnages captivants, un contenu pédagogique validé par des experts, un engagement et un impact sur vos équipes incomparables...

https://cyberstories.fr/

Protection

Grenoble INP - Esisar, UGA

Les entreprises engagent des collaborations avec les experts Esisar et les élèves ingénieurs pour intégrer des briques de sécurité dans leurs produits et/ou services. Une opportunité pour les entreprises de former les talents de demain et d'innover ensemble.

https://esisar.grenoble-inp.fr/

Gouvernance Protection Défense

Groupe Althays

Le Groupe Althays est le partenaire des PME et ETI françaises pour la digitalisation des processus de gestion d'entreprise : ERP, Comptabilité, Paie, Ressources Humaines, Infrastructures informatique et Cybersécurité.

https://groupe-althays.com/

Gouvernance Protection Résilience

Guardis

Certifiée Hébergement de Données de Santé et ISO27001, Guardis propose des services managés, d'infogérance, de télécommunications et de cyberdéfense. Un interlocuteur unique pour sécuriser l'hébergement, le transport, le traitement par IA vos données sensibles.

www.guardis.ch

Défense Résilience

Hardis Group

https://www.hardis-group.com/tech/cybersecurite/

iConseilsPro

iConseilsPro se positionne comme partenaire des TPE/PME en proposant des services de conseil et de DSI externalisée. Notre expertise s'étend sur l'ensemble du système d'information, avec une spécialisation dans les technologies Apple.

www.iconseilspro.com

Gouvernance Protection

LES MEMBRES DU CLUB EXPERTS CYBERSÉCURITÉ (4/5)

IndustriOT

IndustriOT est une société d'ingénierie en infrastructures numériques et cybersécurité industrielle. Passionnés de l'industrie et du numérique. La souveraineté et la protection de l'outil de production des industriels est notre moteur.

https://industriot.com/

Gouvernance | Protection | Défense | Résilience

IPgarde

Hébergeur & cloud_: infrastructures haute disponibilité, sécurité des données, sauvegarde/externalisation et PRA. Supervision et SIEM pour mieux détecter. Des services proches des PME pour protéger vos informations et assurer la continuité.

https://www.ipgarde.com/

Protection

Mines Saint-Étienne

Mines Saint-Etienne est au service du développement des entreprises de son territoire. L'école laccompagne la transformation industrielle en mobilisant l'expertise technique des centres d'enseignement et de recherche, secondé par un réseau d'industriels.

https://www.mines-stetienne.fr/formation/mastere-specialise-manager-de-la-cybersecurite-industrielle/

Protection

Neptune Internet Services

Acteur grenoblois de la Tech depuis plus de 30 ans, nous cultivons la proximité, l'engagement et l'esprit d'équipe. Nos expertises se situent à la croisée de trois univers complémentaires : Opérateur WiFi & Fibre, Agence Web 360° et Infogérance & Cybersécurité.

https://www.neptune.fr/

Gouvernance | Protection | Résilience

Nettic

Intégrateur régional_: cybersécurité, infrastructures et services managés. Protection périmétrique et poste, sauvegarde/PRA, télécoms et support. Objectif_: continuité et productivité des PME avec des solutions éprouvées et un suivi de proximité.

https://www.nettic.fr/

Gouvernance | Protection | Défense

Neyrial

Notre métier s'articule autour de l'infogérance, l'intégration de matériels, logiciels, cybersécurité, hébergement, maintien en condition opérationnelle d'infrastructures informatiques de pointe, réseaux et parc. Nous sommes certifiés Iso27001 et HDS.

https://www.neyrial.com/

Protection | Défense | Résilience

Open Studio

ESN web/IA & e_commerce.
Sécurité intégrée : tests d'intrusion, durcissement des applicatifs, des pratiques de dev et supervision. Des plateformes sur-mesure pensées pour réduire la surface d'attaque sans brider l'expérience utilisateur.

https://www.openstudio.fr/

Protection Défense

Ovide

Ovide propose des formations immersives et participatives qui rendent chaque collaborateur acteur de la sécurité. Elles reposent sur des mises en situation réalistes, des scénarios issus du quotidien et une approche ludique pour un apprentissage durable.

https://ovide.org/

Protection

Phénix Privacy

Phénix Privacy aide les organismes de toute taille à protéger et valoriser les données qu'elles exploitent tout en respectant les contraintes réglementaires. Nos deux chants d'intervention sont la protection des données personnelles et les IA de confiance.

www.phenix-privacy.com

Gouvernance Protection

Piirates

PIIRATES est un cabinet d'audit en cybersécurité à vocation résolument offensive. Nous accompagnons les organisations dans leur gestion du risque cyber. Nous avons développé trois offres permettant d'adresser les multiples dimensions de ce nouveau risque.

https://www.piirates.fr

Défense

Root Me Pro

Plateforme pro d'apprentissage à la cybersécurité : labs, challenges et événements pour sensibiliser, renforcer les compétences, évaluer les acquis et animer.
Un levier concret pour découvrir, s'orienter et progresser dans un cadre ludique.

http://www.root-me.pro/

Protection Défense

Scafe

SCAFE, votre partenaire pour une transformation numérique sécurisée.
Nos 30 experts certifiés conçoivent, déploient et pilotent vos infrastructures IT ainsi que vos dispositifs de cybersécurité.

https://scafe.io/

Gouvernance Protection Défense

Résilience

LES MEMBRES DU CLUB EXPERTS CYBERSÉCURITÉ (5/5)

Stormshield

Éditeur européen : firewalls SNS qualifiés par l'ANSSI, endpoint SES et chiffrement SDS. Protection des réseaux, postes et données, y compris en environnements industriels. Un accompagnement partenaires pour un déploiement maîtrisé et pérenne.

https://www.stormshield.com/fr/

Protection | Défense

Tenacy

Structurer votre cybersécurité pour plus de productivité. La Plateforme GRC Cyber pour centraliser et piloter les organisations complexes. Gouvernance multi-entités, collaboration et efficacité, multi-conformité optimisée, Reporting instantané.

https://www.tenacy.io/

Gouvernance

Vaadata

Vaadata est une entreprise lyonnaise de 30 personnes hautement spécialisées en sécurité offensive : tests d'intrusion et audits red team. Nous travaillons avec plus de 600 clients, basés en France, Allemagne, Benelux, Suisse, UK et USA.

https://www.vaadata.com/fr/

Défense

Wavestone

Conseil & CERT-Wavestone 24/7 : stratégie, gouvernance, tests d'intrusion, détection et réponse, forensique et gestion de crise. Benchmarks et retours d'expérience pour élever la maturité, sécuriser vos projets et renforcer durablement la résilience.

https://www.wavestone.com/fr/nos-expertises/cybersecurite/

Gouvernance | Défense | Résilience

MERCI

pour votre lecture !

DIGITAL LEAGUE
contact@digital-league.org
digital-league.org

DIGITAL LEAGUE
Auvergne-Rhône-Alpes