CYBERSÉCURITÉ :
LES GESTES QUI SAUVENT

Découvrez les piliers pour protéger votre entreprise.
Adoptez les bons réflexes pour éviter le pire.

DIGITAL LEAGUE
Auvergne-Rhône-Alpes

Un e-livret en collaboration avec :

La Région Auvergne-Rhône-Alpes

La Région Auvergne-Rhône-Alpes ENTREPRISES

ONLYNNOV
L'ASSURANCE DES ENTREPRISES TECH

CAMPUS RÉGION DU NUMÉRIQUE

EDITO

CLUB EXPERTS CYBERSÉCURITÉ

Dans un monde toujours plus connecté, où les nouvelles technologies occupent une place centrale dans la stratégie des entreprises, et face à des risques toujours plus sophistiqués, la cybersécurité est devenue un enjeu stratégique pour assurer la continuité des activités, la protection des données et la préservation de la confiance des clients.

Le Club Experts Cybersécurité du Cluster Digital League Auvergne Rhône-Alpes, s'emploie à **animer, fédérer et organiser la filière cybersécurité régionale**.

Fort de l'expertise de ses membres, le Club vous propose à travers ce livre blanc des solutions concrètes. Il est avant tout un guide pragmatique à mettre en œuvre pour sécuriser vos infrastructures numériques comme pour réagir en cas de cyberattaque.

Il recense également la liste des membres experts cyber qui s'engagent et œuvrent de manière collective à la protection comme à la résilience des entreprises de la Région Auvergne Rhône-Alpes.

La cybersécurité n'est plus une option : elle est l'affaire de toutes et tous pour garantir la pérennité de nos organisations !

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
Resp. animation et rel. adhérent
Référent Club Experts Cyber
Digital League

DIGITAL LEAGUE

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

95% des cyberattaques réussissent à cause d'erreurs humaines.

2 Sécuriser ses mots de passe

80% des violations de données sont liées à des mots de passe faibles.

3 Maintenir son système d'information à jour

60% des attaques exploitent des failles déjà connues.

4 Maîtriser ses réseaux

40% des cyberattaques proviennent d'un accès non autorisé aux réseaux internes.

5 Contrôler les accès

58% des entreprises ne révoquent pas immédiatement les accès des anciens employés.

6 Prendre conscience des vulnérabilités

Les audits de sécurité réguliers réduisent de **70%** les risques de failles non détectées.

7 Prendre soin de ses informations « clés »

43% des cyberattaques visent directement les petites entreprises.

8 Faire des sauvegardes

93% des entreprises ayant subi une perte de données sans sauvegarde ferment dans les 5 ans.

9 Avoir une politique de cybersécurité

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

10 Se préparer à la crise

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

LES 10 RÈGLES D'OR DE LA CYBERSÉCURITÉ

Sensibiliser ses collaborateurs

La cybersécurité débute par une sensibilisation efficace des collaborateurs, qui deviennent alors la **première ligne de défense**. Former régulièrement votre équipe aux bonnes pratiques de sécurité est essentiel pour identifier les signaux d'alerte et éviter les erreurs humaines. Ces formations doivent couvrir des aspects tels que l'identification des emails suspects, l'usage sécurisé des mots de passe ou bien encore l'utilisation des wifi non sécurisés. Une sensibilisation continue permet d'**ancrer les réflexes** de sécurité nécessaires.

Sécuriser ses mots de passe

L'utilisation de **mots de passe forts et uniques** est l'une des bases de la cybersécurité. Des combinaisons comme «1234» ou «admin» facilitent l'accès aux systèmes par des pirates, rendant votre organisation vulnérable. 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). De plus, l'implémentation de l'**authentification multi-facteurs** (MFA) renforce considérablement la sécurité. Cette approche proactive réduit les risques liés aux vols d'identifiants et aux intrusions malveillantes.

Maintenir son système d'information à jour

Les mises à jour logicielles et matériels jouent un rôle crucial dans la sécurité des systèmes informatiques. Elles corrigent des failles de sécurité et préviennent leur exploitation par les cybercriminels. Négliger les **mises à jour** revient à laisser une porte ouverte. Il est donc essentiel d'automatiser et de suivre rigoureusement les mises à jour sur tous vos logiciels, systèmes et objets connectés. Une maintenance proactive réduit les risques et assure une protection continue contre les nouvelles menaces.

Maîtriser ses réseaux

La sécurisation des réseaux est un pilier de la cybersécurité. Pour protéger efficacement votre infrastructure, **segmentez vos réseaux** (par service, par bâtiment, etc.) pour limiter l'impact d'une compromission. Sécurisez également vos connexions Wi-Fi avec des mots de passe robustes. Bien évidemment, **distinguez vos Wi-Fi professionnels et invités**. La surveillance active des connexions permet de détecter rapidement toute activité suspecte, tandis qu'une gestion rigoureuse des accès assure que seules les personnes autorisées peuvent y accéder. Une maîtrise rigoureuse des réseaux limite les surfaces d'attaque.

Contrôler les accès

Limiter les accès aux informations sensibles est crucial pour minimiser les risques de compromission. Chaque utilisateur ne doit disposer que des **droits strictement nécessaires à ses tâches**. Révisez régulièrement les droits d'accès et révoquez immédiatement ceux des anciens collaborateurs en élaborant un **processus d'offboarding** (ie : débarquement). Une politique de gestion des accès efficace permet de limiter les menaces internes, mais aussi de restreindre l'ampleur des attaques externes, assurant une protection renforcée des données sensibles de l'entreprise.

Prendre conscience des vulnérabilités

L'arrivée de nouveaux salariés, l'achat d'une nouvelle machine connectée, etc... la cybersécurité repose sur une **évaluation continue** des vulnérabilités. Il est primordial de réaliser des audits réguliers pour identifier les points faibles de votre infrastructure, qu'il s'agisse de failles logicielles, d'erreurs humaines ou de configurations réseaux. En comprenant mieux la « **surface d'attaque** » de votre système, vous pouvez mettre en place des mesures préventives et réagir de manière plus efficace aux menaces avant qu'elles n'arrivent. Une évaluation proactive permet de renforcer durablement votre résilience.

Prendre soin de ses informations « clés »

Il vous sera impossible de tout sécuriser. Toutes les informations ne nécessitent pas le même niveau de protection, mais les données critiques de votre entreprise doivent être protégées de manière prioritaire. Identifiez les **informations les plus sensibles** et appliquez des mesures de sécurité spécifiques telles que le chiffrement ou la gestion stricte des accès. En concentrant vos efforts sur la protection des **éléments stratégiques**, vous minimisez l'impact des incidents sur votre activité. Ce focus sur les informations clés garantit la continuité et la résilience de votre organisation.

Faire des sauvegardes

Les **sauvegardes régulières** de vos données sont essentielles pour garantir la continuité de vos opérations en cas de cyberattaque ou de défaillance technique. Mettez en place une stratégie de sauvegarde qui inclut des copies stockées en plusieurs lieux sécurisés, dont certaines hors ligne dites «à froid». **Testez ces sauvegardes** régulièrement pour vous assurer de leur bon fonctionnement. En cas d'attaque, ces sauvegardes vous permettront de restaurer vos systèmes rapidement, minimisant ainsi l'impact sur vos activités et assurant une reprise rapide.

Avoir une politique de cybersécurité

Elaborer une politique de cybersécurité structurée est essentiel pour protéger efficacement votre organisation. Cette politique doit inclure une répartition claire des responsabilités, des budgets adaptés et des **procédures à suivre en cas d'incident**. Désigner un responsable de la cybersécurité (interne à l'entreprise ou externalisé) garantit que la politique est suivie et régulièrement mise à jour pour **s'adapter aux nouvelles menaces**. Un cadre bien défini permet de prévenir les incidents et de réagir efficacement.

Se préparer à la crise

C'est un fait, toute entreprise, quelle que soit sa taille, sera tôt ou tard victime d'une cyberattaque. Il est donc crucial de mettre en place un plan de réponse aux incidents. 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. Un volet communication, interne et externe, doit aussi être prévu pour informer rapidement les parties prenantes tout en rassurant les clients. Être prêt à gérer une crise permet de réagir rapidement, efficacement et de limiter les dommages.

Sources : ANSSI, Cybermalveillance.gouv.fr, Eurostat, Verizon, Digital Shadows, Microsoft, IBM, Symantec.

JE SUIS VICTIME D'UNE CYBERATTAQUE

QUE DOIS-JE FAIRE ?

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.**

#1 **Isoler le système infecté**
Dès les premiers signes d'une cyberattaque, **isolez** le(s) système(s) et matériel(s) compromis du réseau pour limiter la propagation de l'attaque. Cela inclut la **déconnexion des équipements infectés, des serveurs et des réseaux locaux**.

#2 **Identifier l'origine et la portée de l'attaque**
Mobilisez votre équipe informatique, votre prestataire de services cyber ou votre infogéreur pour **identifier la nature de l'attaque** (phishing, ransomware, etc.), évaluer l'étendue des dégâts et surtout quels systèmes et/ou données ont été affectés.

#3 **Alerter les parties prenantes**
Informez immédiatement les parties prenantes internes (dirigeants, équipe informatique), externes (juridique, assurance) et si nécessaire vos partenaires (clients, fournisseurs, régulateurs) afin de **coordonner une réponse adéquate**.

#4 **Saisir les autorités**
Dès la prise de connaissance de la cyberattaque, vous disposez de **72h pour déposer plainte**. La saisie immédiate des autorités permettra de considérer l'infraction comme un « flagrant délit ». Police, Gendarmerie, ReCym, OFAC, Procureur de la République sont vos relais.

#5 **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 des opérations critiques et maîtriser la communication interne comme externe.

Au même titre que vous êtes un professionnel de votre domaine d'activité, en matière de cybersécurité, **entourez-vous des meilleurs !**

#6 **Évaluer les dommages**
Procédez à une analyse profonde (dite forensique) pour **comprendre l'origine**, le vecteur de l'attaque et l'impact exact. Cela permettra de déterminer les systèmes compromis, les données volées ou altérées et de prendre les mesures appropriées.

#7 **Mettre en place les solutions correctives**
Appliquez les correctifs nécessaires pour **éliminer les vulnérabilités identifiées**. Cela inclut les mises à jour de sécurité, le changement de mots de passe, la réinstallation de systèmes compromis, et la mise en œuvre de correctifs logiciels.

#8 **Communiquer**
Communiquez rapidement et **avec transparence** auprès de vos clients, partenaires et employés, en précisant les mesures prises pour sécuriser leurs données et rétablir les services. Les entreprises victimes de cyberattaques communicant de manière structurée et transparente renvoient une image « professionnelle » et accroissent bien souvent le sentiment de « partenaire de confiance ».

#9 **Recourir à l'assurance cyber**
Si votre entreprise dispose d'une assurance cyber, contactez immédiatement votre assureur pour entamer le processus de réclamation et obtenir des conseils sur les **actions à entreprendre.** Votre assureur à tout intérêt à vous accompagner pour éviter les surcoûts.

#10 **Améliorer les mesures de sécurité**
Après l'incident, effectuez une évaluation pour **identifier les faiblesses dans vos systèmes et vos processus de sécurité.** Renforcez les mesures de prévention, notamment en sensibilisant les collaborateurs, en améliorant la protection des données et en renforçant les systèmes de détection des menaces.

ASSURANCE CYBER

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 2023, 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.

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.

MON FOURNISSEUR EST VICTIME D'UNE CYBERATTAQUE QUE DOIS-JE FAIRE ?

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.

#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 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 plan de gestion de crise

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.

#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.

DIGITAL LEAGUE Auvergne-Rhône-Alpes

LES MEMBRES DU CLUB EXPERTS CYBERSÉCURITÉ

Abelionni
contact@abelionni.com
abelionni.com

Adista
mfonta@adista.fr
adista.com

Agaetis
claire.avedikian@agaetis.fr
agaetis.fr

AIoTrust
frederic.breussin@aiotrust.io
aiotrust.io

Akant
gestion@akant.fr
akant.fr

AlgoSecure
commercial@algosecure.fr
algosecure.fr

Apitech
apitech@apitech.fr
apitech.fr

Artecys
clecomte@artecys.com
artecys.com

ATN Groupe
commercial@atngroupe.fr
atngroupe.fr

Avangarde Consulting
christine.lamour@avangarde-consulting.com
avangarde-consulting.com

Axess
jacques.verdier@axess.fr
axess.fr

BPR Security
contact@bprsecurity.fr
bprsecurity.fr

CPE Lyon
isabelle.favre@cpe.fr
cpe.fr

Cybalgoris
contact@cybalgoris.com
cybalgoris.com

Cyberenity
fpriou@cyberenity.com
cyberenity.com

Cyberprotect
dnassar@cyberprotect.one
cyberprotect.one

CyGO Entrepreneurs
contact@cygo-entrepreneurs.com
cygo-entrepreneurs.com

Elysium Security
quentin.hugon@elysium-security.com
elysium-security.com

Evicys
contact@evicys.com
evicys.com

Grenoble INP Esisar
relations.entreprises@esisar.grenoble-inp.fr
esisar.grenoble-inp.fr

Groupe Gardeners
pmaison@agencegardeners.com
lp.agencegardeners.com

Hackuity
psamson@hackuity.io
hackuity.io

IP Garde
lnoury@ipgarde.com
ipgarde.com

Linphone
elisa.nectoux@belledonne-communications.com
linphone.org

My MSP
info@my-msp.fr
my-msp.com

Neyrial Informatique
scalandry@neyrial.com
neyrial.com

OpenStudio
jnicaise@openstudio.fr
openstudio.fr

Piirates
sg@piirates.fr
piirates.fr

RAI Consulting
fmarquez@consultant.com

Serenicity
commercial@serenicity.fr
serenicity.fr

Stormshield
vincent.nicaise@stormshield.eu
stormshield.com

Strat&Si
contact@strat-et-si.fr
strat-et-si.fr

Tenacy
baptiste.david@tenacy.io
tenacy.io

Vaadata
contact@vaadata.com
vaadata.com

ENGAGÉS POUR LA RÉSILIENCE EN RÉGION AUVERGNE-RHÔNE-ALPES

PANORAMA DES ACTEURS CYBER DE LA RÉGION AUVERGNE-RHÔNE-ALPES

À 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.

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.

Je consulte le panorama

CYBERSÉCURITÉ :
LES GESTES QUI SAUVENT

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

DIGITAL LEAGUE
Auvergne-Rhône-Alpes

Octobre 2024

Un livret cybersécurité rédigé par Digital League à l'occasion du cybermois