CYBER CERCLE

21 OCTOBRE 2021
LYON

RENCONTRES CYBERSÉCURITÉ
AUVERGNE-RHÔNE-ALPES

#RCYBERARA
#TDFCYBER

RHÔNE
LE DÉPARTEMENT

TOUR DE FRANCE DE LA CYBERSÉCURITÉ

#TDFCYBER

ESPACES DÉMOS
TABLES RONDES
FORMATION
NETWORKING
RECRUTEMENT
ATELIERS

@CyberCercle
@CyberTerritoire

DOSSIER PARTICIPANT

RCyberAra en distanciel 21 OCTOBRE 2021

Edito

Christophe GUILLOTEAU
Président du Département du Rhône

A l'heure du tout numérique, de la dématérialisation des procédures et de la gestion accrue des données personnelles, les systèmes d'informations des entreprises et des collectivités deviennent des cibles récurrentes aux attaques informatiques.

En février 2020, l'Hôpital de Villefranche sur Saône, plus grand centre hospitalier du département du Rhône a ainsi été victime d'une cyberattaque d'ampleur, obligeant pendant quinze jours l'établissement à interrompre l'intégralité ses services informatiques.
Des communes dans le Rhône ont connu le même sort, faute de protection suffisante de leur interface web ou mail.

Ce type d'évènements aux conséquences dramatiques et couteuses n'arrive pas qu'aux autres.

Si le risque zéro est impossible, des solutions aujourd'hui existent tant par le déploiement d'outils de protection que par la formation des usagers aux bons comportements à adopter.

Les collectivités longtemps en retard face à ce risque doivent aujourd'hui prendre leur responsabilité et engager les dépenses nécessaires pour s'équiper en matière de sécurité numérique.

Depuis longtemps impliqué personnellement dans le domaine de la cybersécurité et de la transformation numérique, je suis heureux de pouvoir accueillir pour la deuxième fois à l'Hôtel du Département du Rhône, « les Rencontres Cybersécurité Auvergne-Rhône-Alpes» et le CyberCercle qui vont aborder tous les enjeux de défense face aux menaces du 21ème siècle.

DOSSIER PARTICIPANT

RCyberAra en distanciel 21 OCTOBRE 2021

Crédit photo Alain Zimeray

Bénédicte PILLIET
Présidente du CyberCercle

Edito

Le CyberCercle a fait de la sécurité et la confiance numériques des territoires un des axes forts de son action depuis plusieurs années. Dans le prolongement de nos événements « Cyber et Territoires », nous avons ainsi lancé en 2018 le Tour de France de la Cybersécurité.

Aller au contact des acteurs locaux pour promouvoir la sécurité et la confiance numériques afin d'en faire une vraie force, engager des synergies au sein des écosystèmes, des territoires et entre les territoires, susciter des projets fédérateurs, être force de propositions pour les élus… sont les moteurs de notre action et de notre motivation en région depuis plus de six ans.

Avec la crise de la COVID 19, le recours au numérique, devenu essentiel, a encore accéléré la transformation numérique des organisations, publiques et privées, augmentant d'autant la surface de vulnérabilité face aux cyberattaques qui se multiplient.

Permettre dans ce contexte d'avoir accès à une parole de confiance sur la sécurité numérique et favoriser les échanges constructifs pour avancer ensemble vers des territoires de confiance numérique sont les objectifs de cette troisième édition des Rencontres de la Cybersécurité Auvergne-Rhône-Alpes qui se déroule à Lyon, dans les salons de l'Hôtel du Département du Rhône.

Je tiens à remercier très sincèrement Christophe GUILLOTEAU, le Président du Département du Rhône, de son soutien depuis la création de ces Rencontres.

Cette édition a également lieu alors que le rôle majeur des collectivités, et plus largement des territoires, en matière de cybersécurité est aujourd'hui mis en lumière par le Plan de Relance Cybersécurité et sa dimension Cybersécuriser les territoires. Fort de son expertise sur un sujet où il a été précurseur, le CyberCercle a publié cette année le deuxième ouvrage de sa collection Regards Croisés sur cette thématique de la sécurité numérique des collectivités territoriales.

Cette journée est donc une occasion pour nous, ici, en Auvergne-Rhône-Alpes, de faire un point de situation, d'échanger sur ces sujets majeurs, de travailler ensemble, de mieux connaître les dispositifs nationaux et locaux dans lesquels nous pouvons nous inscrire pour faire de nos territoires des territoires de confiance numérique.

Car la sécurité numérique, au-delà de sa dimension sécurité, est un pilier fondamental aujourd'hui pour le développement économique, l'attractivité des territoires, les relations entre collectivités et citoyens.

Le territoire dans lequel nous sommes est un territoire dynamique, fort d'un écosystème économique riche et diversifié, doté de politiques publiques structurantes sur l'industrie 4.0, l'IA, le numérique, avec en particulier le Campus Région du Numérique. Nous sommes heureux au CyberCercle de contribuer à cette construction d'un territoire de confiance numérique, avec cette journée de Rencontres mais aussi, tout au long de l'année, avec nos matinales bimestrielles.

Je remercie nos partenaires, qui pour certains nous suivent sur l'ensemble du Tour de France de la Cybersécurité depuis sa création comme le Groupe La Poste, Cybermalveillance.gouv.fr et CERTitude NUMERIQUE, des organisations comme Avant de Cliquer, ENEDIS et la Banque des Territoires qui nous ont rejoints cette année.
Je remercie également nos soutiens, collectivités, ministères, écoles, associations, qui s'associent à cet événement dans cet esprit fédérateur qui est le nôtre.

Rappelons-nous que la sécurité numérique demande un effort individuel mais surtout collectif, une dynamique de gouvernance allant bien au-delà de la sphère des experts dans laquelle elle est encore trop souvent enfermée.

« *Agir efficacement ensemble pour construire une culture de sécurité numérique partagée au service des acteurs présents sur les territoires* », telle est la signature du Tour de France de la Cybersécurité.

Cette troisième édition des Rencontres de la Cybersécurité Auvergne-Rhône-Alpes s'inscrit pleinement dans cette dynamique constructive, d'autant plus indispensable pour faire face aux enjeux actuels, qu'ils soient économiques, sécuritaires ou sociétaux.

8h30 ■›› **OUVERTURE DU CAFE D'ACCUEIL**

9h00 ■›› **MOT DE BIENVENUE**

Bénédicte PILLIET, Présidente du CyberCercle

■›› **INTERVENTIONS**

Christophe GUILLOTEAU, Président du Département du Rhône

Renaud PFEFFER, Vice-président en charge de la sécurité de la Région Auvergne-Rhône-Alpes, représentant **Laurent WAUQUIEZ** Président de la Région Auvergne-Rhône-Alpes

9h30 ■›› **TABLE RONDE**

Auvergne-Rhône-Alpes : une région aux nombreux atouts en matière de sécurité numérique

Animatrice : **Bénédicte PILLIET**

Cyril AMPRINO, secrétaire général, CPME Auvergne-Rhône-Alpes

Bruno CHARRAT, adjoint au directeur de la recherche technologique, CEA

Erasmia DUPENLOUP, directrice du développement des entreprises et des territoires, MINALOGIC

David HELY, professeur associé, Grenoble-INP ESISAR

Alix MADET, déléguée à l'information stratégique et à la sécurité économiques pour la région Auvergne-Rhône-Alpes, direction régionale de l'économie, de l'emploi, du travail et des solidarités, Secrétariat général pour les affaires régionales, Préfecture de la région Auvergne-Rhône-Alpes

11h00 ■›› **PAUSE**

11h30 ■›› **KEYNOTES**

➤ Cybermalveillance.gouv.fr : quels outils et services pour les acteurs des territoires

Amandine DEL-AMO, chargée de mission partenariats, cybermalveillance.gouv.fr

➤ L'identité numérique, une brique indispensable de sécurité et de souveraineté numériques

Dr Michel DUBOIS, directeur scientifique et technique, direction de la cybersécurité, Groupe La Poste

➤ RGPD : où en sommes-nous ?

Laurane RAIMONDO, DPO - chercheure associée, Centre Lyonnais d'Etudes de Sécurité Internationale et de Défense, Université Jean Moulin Lyon 3

13h00 ■›› **PAUSE DEJEUNER - cocktail déjeunatoire**

14h30 ■›› CONFERENCES-DEBATS

Les conférences-débats durent deux heures et ont pour objectif de permettre aux participants d'échanger sur des thématiques précises, dans un cadre de confiance - elles sont placées sous les règles de Chatham House. Elles sont ouvertes par un ensemble d'interventions d'une quinzaine de minutes chacune, suivies à l'issue par un dialogue avec les participants qui seront invités à faire part de leur expertise, de leur vécu ou de poser des questions.

➤ CONFERENCE-DEBAT 1 - Collectivités : comment traiter les risques numériques

Les collectivités sont aujourd'hui la cible de cyberattaques de plus en plus nombreuses. Engagées dans des processus de transformation numérique et de e-administration qui en font des cibles privilégiées pour les cyberattaquants, elles se doivent de se doter d'outils, de process et d'une culture interne propres à les aider à faire face à ces menaces, et développer des collaborations sur les territoires.

Animateur : **Christian DAVIOT**, senior advisor, CyberCercle
Daniel COISSARD, directeur des usages numériques, Département du Rhône
Amandine DEL-AMO, chargée de mission partenariats, Cybermalveillance.gouv.fr
Astrid FROIDURE, chargée des relations publiques, Avant de Cliquer
Adjudante Malika WAVELET, conceptrice en planification et gestion de crise, conseillère en sécurité économique, Etat-major de la Région de Gendarmerie Auvergne-Rhône-Alpes

➤ CONFERENCE-DEBAT 2 - La place des femmes dans la cybersécurité : des formations et des métiers d'avenir

La filière cybersécurité souffre aujourd'hui d'un manque de ressources humaines qualifiées et formées. Près de 10 000 postes seraient à pourvoir en France... et les besoins vont encore augmenter. Dans ce contexte, les femmes ne représentent aujourd'hui que 10% des professionnels de la cybersécurité. Cette conférence a pour objectif de présenter les métiers de la cybersécurité, les formations, de montrer que les femmes ont toute leur place dans ce secteur et de favoriser le développement de cette filière RH en Auvergne-Rhône-Alpes.

Animatrice : **Béatrice BERARD**, officier de sécurité sur les systèmes d'information, Hospices Civils de Lyon - membre, Cercle des Femmes de la Cybersécurité (CEFCYS)
Clara FOUCHER, membre, CEFCYS
Gaëlle PICARD-ABEZIS, directrice des Relations extérieures, DOCAPOSTE
Séverine MARTINS, directrice de projets, Fondation LDigital
Emmanuel RUAUD, référent filière Informatique, Lyon YNOV Campus

➤ CONFERENCE-DEBAT 3 - Comment favoriser l'innovation en cybersécurité

La cybersécurité est aujourd'hui un enjeu majeur pour l'économie et la souveraineté. Rôle des grands donneurs d'ordre, soutien des acteurs du développement local, plan de financement au niveau national, relations entre recherche fondamentale et recherche applicative, relations entre grands groupes et pmi-pmi, soutien aux start-up... autant de sujets qui seront abordés au service du développement des entreprises du numérique et de la cybersécurité d'Auvergne-Rhône-Alpes.

Animateur : **Dr Michel DUBOIS**, directeur scientifique et technique, direction de la cybersécurité, Groupe La Poste
Adrien BRESSON, directeur de projets réseaux et sécurité, Direction Générale des Entreprises, ministère de l'Economie, des Finances et de la Relance
Philippe SIRAUDIN, co-animateur du groupe cybersécurité, ADIRA
Assia TRIA, responsable scientifique du service sécurité, CEA-Leti

16h00 ■›› FIN DES ATELIERS - CAFE DE CLOTURE

Les intervenants

Christophe GUILLOTEAU

Président
Département du Rhône

Christophe GUILLOTEAU est né le 18 juin 1958 à Lyon. Après avoir été assistant parlementaire puis Chef de cabinet à la mairie de Tarare de 1988 à 1994, il est devenu attaché territorial et collaborateur du Vice-président du Conseil Régional de Rhône-Alpes. Elu en 1998 Conseiller régional et Conseiller municipal de Vaugneray, il a été de 2008 à 2015, Conseiller général du Rhône et Vice-président du SDIS. Il est depuis mars 2015 le Président du Conseil départemental du Rhône.
Elu député du Rhône en 2003, il a été réélu en 2007 et en 2012.
Christophe GUILLOTEAU a été nommé en juillet 2012 membre titulaire de la Commission chargée de l'élaboration du Livre blanc sur la Défense et la Sécurité nationale. Membre de la Commission de la Défense nationale et des Forces armées sein de l'Assemblée Nationale, il en a été le vice-président, rapporteur pour le Budget Air et Président du Groupe d'étude Industrie de Défense, développant une expertise sur les sujets de Défense et de Sécurité Nationale.
Il est depuis avril 2015 Président du Département du Rhône.
Christophe GUILLOTEAU est Chevalier de l'Ordre National du Mérite et Chevalier du Mérite agricole, Capitaine de vaisseau dans la Réserve citoyenne de la Marine, et membre de la Réserve Citoyenne Cyberdéfense.

Bénédicte PILLIET

Présidente
CyberCercle

Crédit photo Alain Zimeray

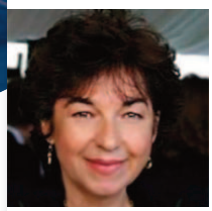
Bénédicte Pilliet est depuis 2011 la Présidente fondatrice du CyberCercle, cercle de réflexion, d'échanges et de rencontres sur la sécurité et la confiance numériques, placé sous la dynamique des parlementaires et des élus locaux. Diplômée de Sciences Po Paris, elle bénéficie de quinze ans d'expérience de relations institutionnelles et parlementaires sur les sujets de Défense et de Sécurité Nationale.
Elle est responsable pédagogique et créatrice du Certificat « Conformité Numérique, données personnelles et cybersécurité » à l'Université Paris-Dauphine, responsable du séminaire "Politiques publiques de cybersécurité et Relations internationales" au sein du M2 "Politiques de Défense-Sécurité et Relations internationales" à l'Université de Toulouse 1 Capitole, et intervient dans plusieurs cursus - Université Catholique de Lyon, Institut Leonard de Vinci.
Membre fondateur du Cercle K2, membre du Cercle des Experts de la Sécurité de l'Information et du Numérique (CESIN), membre du conseil d'administration du Cercle des Femmes de la Cybersécurité (CEFCYS) et de la Fédération Française de la Cybersécurité (FFCYBER) , Bénédicte Pilliet est depuis 2007 Lieutenant-colonel de réserve (citoyenne) dans l'armée de Terre et a rejoint à sa création en 2012, le réseau de la Réserve Citoyenne de Cyberdéfense, où elle a été en charge du rayonnement et de la communication jusqu'en 2017.
Elle est titulaire de la Médaille de la Défense nationale, échelon or, agrafe cyber, et de la Médaille des Services Militaires Volontaires, échelon bronze.

Renaud PFEFFER

Vice-président en charge de la sécurité
région Auvergne-Rhône-Alpes

Erasmia DUPENLOUP

Directrice du développement des entreprises
Pôle de compétitivité Minalogic



Avant de rejoinder Minalogic, Erasmia a occupé le poste d'administrateur au Lycée Français la Pérouse à San Francisco (Chair of the North American College Preparation Task Force, member of the Nominating Committee and of the Governance Committee).
De 2000 à 2002, Mme Dupenloup a occupé le poste d'ingénieur d'application chez Hewlett-Packard à Cupertino, Californie. Elle était détachée chez Cadence Design Systems, en charge du support des équipes R&D, de la promotion de HP à l'intérieur de Cadence et du renforcement des relations entre les deux sociétés.
De 1987 à 1989, elle a travaillé à Paris en tant qu'ingénieur développement logiciel, dans l'équipe de développement du compilateur ADA, chez Alsys la startup fondée par l'inventeur du langage ADA.
De 1982 à 1986, elle a occupé le poste d'ingénieur R&D au Laboratoire de recherche IMAG, Grenoble dans l'équipe de recherche développant de nouvelles approches de test fonctionnel de circuits intégrés. Elle a testé divers microprocesseurs utilisés dans des applications critiques pour IBM, la SNCF et l'Agence Spatiale européenne.

Cyril AMPRINO

Secrétaire général
CPME Auvergne-Rhône-Alpes

Diplômé de Sciences Po Lyon, titulaire d'une maîtrise de droit des affaires, Cyril AMPRINO est Secrétaire Général de la CPME Auvergne-Rhône-Alpes depuis janvier 2001.
La CPME (Confédération des Petites et Moyennes Entreprises) est la seule organisation patronale interprofessionnelle qui assure la représentation et la défense des TPE-PME, start-up, artisans, commerçants.
« *Être aux côtés et au service de nos 12 000 TPE/PME adhérentes* », c'est ce qui anime depuis bientôt deux décennies Cyril AMPRINO, secrétaire général à la CPME Auvergne-Rhône-Alpes, et son équipe.
Un rôle sur-mesure pour Cyril AMPRINO qui, au cours de sa première expérience au sein de la ville de Lyon était chargé de mission auprès de l'association Lyon Insertion avec pour but d'insérer les jeunes par l'économie ! C'est d'ailleurs à cette période qu'il tape dans l'œil de son futur président, François TURCAS, convaincu par la capacité de Cyril « à bâtir des projets et endosser une fonction d'opérationnel ».
Depuis le couple Président/Secrétaire Général est inséparable : « *Cette complicité est indispensable pour le bon fonctionnement d'une structure comme la nôtre mais j'avoue une affection toute particulière pour mon président* », confie Cyril AMPRINO.
Cyril AMPRINO est Chevalier dans l'Ordre National du Mérite.

David HELY

Professeur associé
Grenoble INP-ESISAR

Diplômé de l'INSA Lyon en 2002, David HELY a obtenu son doctorat en microélectronique en 2005 de l'Université Montpellier II, ses travaux de thèses réalisés dans la division Smartcard de STMicroelectronics avec le LIRMM concernant la sécurité des systèmes sur puce. Après plusieurs expériences industrielles sur la conception et l'évaluation de systèmes sécurisés chez STMicroelectronics et Ingenico, il est depuis 2010 maître de conférences à Grenoble INP Esisar et au laboratoire de recherche LCIS. Il a également effectué plusieurs longs séjours de recherche dans les instituts de cybersécurité des universités américaines NYU et NAU. Ses activités d'enseignement, de recherche et de transfert de technologies concernent la sécurité des systèmes embarqués.

Bruno CHARRAT

Adjoint au directeur de la recherche technologique
CEA

De formation initiale d'ingénieur complétée d'un doctorat en microélectronique, Bruno CHARRAT a occupé plusieurs fonctions d'encadrement dans des groupes industriels avec de rejoindre le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) en 2012. En tant que chef du service Sécurité de l'institut CEA-Leti, il s'est impliqué dans le lancement et la conduite de plusieurs collaborations avec des acteurs nationaux et internationaux en cybersécurité. Depuis 2019, à la direction de la recherche technologique du CEA, il est en charge du programme Cybersécurité qui coordonne le travail de plus de 180 chercheurs et ingénieurs, afin de développer de nouveaux outils d'analyse de la sécurité et des technologies permettant aux systèmes de mieux résister aux cyberattaques.
Il représente le CEA dans plusieurs initiatives nationales comme le Campus Cyber, le Programmes et Equipements Prioritaires de Recherche (PEPR) de la stratégie nationale d'accélération cybersécurité et le groupe de travail cybersécurité du comité stratégique de filière Nouveaux Systèmes Energétiques (CSF NSE).
Il est auditeur de la 3ème session nationale « Souveraineté Numérique et Cybersécurité » de l'Institut des Hautes Etudes de Défense Nationale (IHEDN).

Alix MADET

Déléguée à l'information stratégique et à la sécurité économiques pour la région Auvergne-Rhône-Alpes
DREETS Auvergne-Rhône-Alpes

Nommée par le Secrétaire à l'Information Stratégique du ministère de l'économie, Alix Madet a pris ses fonctions de Déléguée à l'Information Stratégique et à la Sécurité Economique (DISSE), le 2 mai 2019, poste rattaché à la DIRECCTE au côté de Pascal Brocard. Avocate et attachée principale d'administration des finances, elle est titulaire d'un master 2 de droit civil, et est auditrice de l'IHEDN. Elle débute sa carrière en 1996 dans un cabinet d'avocats parisien, spécialisé en droit de l'aviation, où elle gère les dossiers de responsabilité civile ou pénale. En 1997, elle choisit d'entrer dans l'administration, grâce au concours d'entrée à l'Institut Régional d'Administration de Lille, d'où elle sort attachée d'administration au Ministère des Finances. Elle assume des missions de contentieux en droit de la concurrence au sein de la DGCCRF, plaidant au nom du Ministre des finances devant la Cour d'appel de Paris, pour les recours contre les décisions du Conseil de la concurrence. En 2001, elle est nommée à la DRIRE Rhône-Alpes, en tant que chef de subdivision en développement industriel pour le département de la Loire. Elle restera dans ce service déconcentré de l'Etat jusqu'en 2010, date à laquelle elle intègre la DIRECCTE Rhône-Alpes, en tant que chargée de mission en développement économique. Là elle participe à l'application de la politique industrielle de l'Etat et accompagne les filières industrielles de la Région, celle du textile d'abord, puis du luxe et du design, enfin la filière de la mécanique et son pôle de compétitivité Viameca.

Les intervenants

Amandine DEL-AMO

Chargée de mission partenariats
Cybermalveillance.gouv.fr

Amandine DEL-AMO est Chargée de mission partenariats au sein du dispositif national Cybermalveillance.gouv.fr. Forte d'une expérience de plus de 10 ans dans l'écosystème de la sécurité et des systèmes d'informations, elle a notamment été responsable commerciale chez DG Consultants (Groupe Comexposium) où elle a contribué à développer l'événement "les Assises de la Sécurité" à Monaco et à fédérer la communauté des professionnels du secteur. Après une expérience au sein d'un distributeur à valeur ajoutée Exclusive Networks, en charge du développement de la marque Palo Alto Networks, elle a souhaité mettre son expérience au service d'un organisme d'intérêt général en rejoignant en septembre 2019 le dispositif d'assistance aux victimes d'actes de cybermalveillance et de sensibilisation aux risques numériques.

Dr Michel DUBOIS

Directeur scientifique et technique
Direction de la cybersécurité
GROUPE LA POSTE

Michel DUBOIS est chef du pôle expertise cybersécurité au sein de la direction de la cybersécurité du Groupe La Poste. Ingénieur en informatique, titulaire d'un mastère spécialisé en Sécurité des Systèmes d'information et docteur en cryptologie, Michel a exercé pendant près de trente ans des fonctions de responsable de la SSI au sein du Ministère des Armées.
Il est, par ailleurs enseignant chercheur au sein du laboratoire de Cryptologie et de Virologie Opérationnelles de l'ESIEA à Laval. Il est membre du club des experts de la sécurité de l'information et du numérique (CESIN), du club de la sécurité de l'information français (CLUSIF) et de l'association des réservistes du chiffre et de la sécurité de l'information (ARCSI).

Christian DAVIOT

Senior Advisor
CyberCercle

Après un troisième cycle de communication et la co-fondation d'une entreprise conseil en stratégie et lobbying, Christian DAVIOT a effectué une partie de sa carrière en cabinets ministériels, notamment ceux de Jean Arthuis, au Plan et au ministère de l'Economie et des Finances où il a été conseiller technique en charge de l'intelligence économique, de l'expansion économique et des TIC. Spécialiste de l'Intelligence économique, il a coordonné la rédaction de deux rapports au Premier ministre, et a créé la Fondation d'entreprises bi-partisane Prometheus dont il a été directeur général. Il a rejoint l'ANSSI en 2009 où il a été le conseiller stratégie du directeur général jusqu'en 2020. Il est aujourd'hui le président fondateur du cabinet de conseil CDStrat et senior advisor du CyberCercle.

Laurane RAIMONDO

DPO
Chercheure associée
Centre Lyonnais d'Etudes de Sécurité Internationale et de Défense

En 2014 d'abord, puis en 2016, pendant ses études, Laurane RAIMONDO travaille pour la data unit du Conseil de l'Europe. En 2018, ses travaux mêlent la protection des données, le cyber et la question de la militarisation et l'arsenalisation de l'espace extra-atmosphérique. Ses recherches sur ce dernier sujet sont primées par le prix du Gouverneur militaire de Lyon. Exerçant dans le même temps comme data protection officer auprès d'un organisme traitant des données sensibles de personnes vulnérables, elle développe l'enseignement cyber dans le Master Relations Internationales à la Faculté de Droit à l'Université Jean Moulin Lyon 3 et celui des données personnelles dans le parcours Expertise et Risques Internationaux.
Auteure de l'ouvrage La protection des données personnelles en 100 questions-réponses à paraître chez Ellipses début 2021, elle écrit pour la série Stories of Conflict d'Arte, le magazine Sécurité & Défense et entend poursuivre l'écriture à destination du grand public ainsi que l'enseignement. Deux axes visant à rendre le cyber accessible à tous pour développer la confiance dans l'espace numérique.

Astrid FROIDURE

Chargée de Relations Publiques
Avant de Cliquer

Astrid FROIDURE a été élue pendant deux mandats à Caen en Normandie et s'est particulièrement investie sur l'aspect stratégique RH des collectivités territoriales en participant activement en tant que jury des concours A et A + de la Fonction Publique Territoriale.
Investie dans une association d'accompagnement économique du territoire Normand, elle est membre du Comité d'Intelligence Économique Territorial qu'avait créé Madame BUCCIO alors Préfète de Normandie.
A la demande des entreprises comme des collectivités, elle coordonne un groupe de travail avec le soutien des services de l'Etat (SISSE, DGSI, ANSSI, Conseiller Diplomatique rejoint par Cybermalveillance et la DRSD) ainsi que des acteurs importants Normandie AéroEspace qui regroupe plus de 400 entreprises et Normandie Université. Ce groupe élabore depuis plus de 4 ans un programme de sensibilisation à la sécurité économique et numérique à l'intention des lycéens dans l'objectif de créer une Attestation de sécurité économique et numérique avant l'entrée en stage, alternance, ou vie active.
Parallèlement, Astrid FROIDURE travaille avec le Centre de Gestion du Calvados afin d'initier un programme d'actions sur le cybersécurité vers les collectivités du Calvados. Avant de Cliquer étant partenaire de cette action, c'est assez naturellement qu'Astrid FROIDURE a rejoint cette société spécialisée dans la sensibilisation des utilisateurs face au phishing, en tant que chargée des Relations Publiques.

Gaëlle PICARD-ABEZIS

Directrice des Relations extérieures
DOCAPOSTE

Femme d'engagement, Gaëlle Picard-Abezis est depuis janvier 2019, Directrice des relations extérieures de Docaposte, filiale du Groupe La Poste experte de la transformation digitale des entreprises et des institutions, engagée, en B to B, sur l'innovation et l'inclusion.
« Serial influenceuse et experte des sujets IT ", Gaëlle a en charge chez Docaposte, en transverse, aussi bien le pilotage des écosystèmes IT , les analystes, les référencements internes et partenariats institutionnels... Elle défend à l'extérieur les valeurs d'innovation de son entreprise, fervente ambassadrice des valeurs d'usages du numérique ; à travers elle, Docaposte participe à de nombreuses interventions expertes et à des référencements experts (Truffle 100, TOP 250, TOP ESN, ...) permettant de valoriser les métiers et savoir-faire de l'entreprise.
Depuis 3 ans, Gaëlle a pour mission d'accélérer la présence de Docaposte dans les écosystèmes métiers et IT dans les domaines stratégiques de Docaposte.
Au-delà de ses missions chez Docaposte, l'engagement de Gaëlle se traduit à travers sa participation aux conseils d'administration du CINOV Numérique (Syndicat des TPE – Pme du Numérique) et de l'ACN (Alliance de la Confiance Numérique), CEFCYS (association de la Femmes Cyber) et co-présidente de la Commission Data et Confiance de l'ACSEL.
Elle anime ou participe également activement à des cercles de réflexion et d'influence dans le numérique dans différents périmètres entrepreneuriaux avec l'ACSEL, NUMEUM, Cinov Numérique, France Digital ou encore auprès d'institutions d'enseignement supérieur.
Femme de conviction, Gaëlle Picard-Abezis s'est tout naturellement engagée dans la stratégie Parité insufflée par Docaposte et pilote aujourd'hui le plan d'actions de son entreprises et ses filiales en faveur de l'accompagnement des femmes dans les métiers du numérique.

Adjudante Malika WAVELET

Conceptrice en planification et gestion de crise, conseillère en sécurité économique
Etat-major de la Région de Gendarmerie Auvergne-Rhône-Alpes

Après avoir intégré l'école de gendarmerie de Montluçon en 1999, Malika WAVELET été affectée à la brigade de Vienne (38) unité rurale en 2000, puis à la brigade de l'Isle d'Abeau en 2006, unité péri-urbaine.
Elle a rejoint le centre d'opérations et de renseignements du Rhône en 2009 en tant qu'opératrice de quart opérationnel.
Formée comme référent sûreté en prévention technique de la malveillance et vidéoprotection en 2017, elle a ensuite été affectée à l'état major de la région de gendarmerie Auvergne-Rhône-Alpes. Actuellement au bureau conduite planification plans, où elle a pu bénéficier du cycle d'expertise en intelligence économique de l'INHESJ.

Séverine MARTINS

Directrice de projets
Fondation LDigital

Après 20 ans en société de conseil et d'ingénierie numérique, à des fonctions de développement du business et des compétences des hommes et des femmes du numérique, elle prend son envol en mettant le pied à l'étrier de l'entreprenariat et fonde en 2021 SEVEL CONSEIL, pour accompagner le développement des entreprises, notamment dans l'IT.
En tant que Directrice de projet chez LDIGITAL, elle œuvre pour plus de mixité dans les métiers du numérique et pour la féminisation de la filière, en allant auprès des jeunes filles et des femmes pour les acculturer à la pluralité des métiers qui existe, comme la Cybersécurité et déconstruire les stéréotypes et biais de genre qui y sont associés.

Daniel COISSARD

Directeur des Usages Numériques
Département du Rhône

Après avoir dirigé le GIP Maximilien (2017-2021), première plateforme d'e-administration, et développé la plateforme e-bourgogne, la toute première plateforme de marchés publics (2008-2016), Daniel COISSARD a rejoint, courant septembre 2021, le département du Rhône, en tant que Directeur des Usages Numériques. Fort de 30 ans d'expérience dans le domaine informatique (développement de jeux dans les années 80, formation, réseaux-télécommunication et gestion de projets de dématérialisation de procédures administratives et facturation), son travail est toujours axé sur :
• L'organisation, la coordination et la conduite de projets ouverts et innovants.
• La relation et la satisfaction de mes clients (internes ou externes).
• La sécurité des biens, des données et des personnes.
Ses motivations au quotidien :
• définir une stratégie, la décliner en plans d'action et piloter sa mise en œuvre,
• créer de nouveaux services numériques sécurisés répondant à un besoin ou une évolution réglementaire,
• optimiser le fonctionnement de l'organisation et coordonner l'action des développeurs, des chefs de projets et des clients,
• innover dans la recherche de solutions et l'optimisation de résultats,
• construire en commun une dynamique d'équipe et contribuer à développer le potentiel de chacun.

Béatrice BERARD

Officier de sécurité au sein des HCL
Membre du CEFCYS

Après avoir œuvré au sein des équipes informatiques du CHU de Nancy en tant que responsable des infrastructures systèmes et animé les premiers projets de sécurisation des SI tels que la gestion des identités et la sécurisation des infrastructures techniques, c'est en 2014 que Béatrice Bérard rejoint les Hospices Civils de Lyon en tant qu'Officier de Sécurité sur les Systèmes d'Information.
Nourrissant une passion pour la fonction publique hospitalière, elle œuvre, au nom de la cybersécurité et avec son équipe, à améliorer la gouvernance dans ce domaine, mener des projets de conformité tels que les certifications HDS et ISO 27001, animer une démarche d'appréciation du risque numériques au sein de son organisation.
Convaincue par la nécessité d'une meilleure visibilité centrale du niveau de maturité cyber des hôpitaux, elle contribue à plusieurs travaux nationaux dont le projet d'identification des professionnels de santé et le projet MATURIN-H.
Depuis 2019, elle met à disposition de la justice son expertise en systèmes d'information, cybersécurité et médiation. Elle est inscrite sur la liste des experts en justice de la Cour d'appel de Lyon.
Cefcysienne récente, elle milite sur la nécessité de mieux communiquer au sujet de la diversité des métiers de la cyber auprès de tous et des jeunes femmes en particulier.

Clara FOUCHER

Membre du CEFCYS

Clara FOUCHER est titulaire d'une licence de droit privé de l'Université de Lyon 3 et d'un DU de transformation numérique de l'Université de Lyon. En parallèle de son Master, elle est sous contrat CAPE avec Explorys (incubateur) pour mon activité de consultante RGPD : elle traite ces questions sous forme de Legal Design et accompagne à la mise en oeuvre du RGPD pour les petites entreprises n'ayant pas forcément un budget conséquent pour ce type de questions. Elle est membre du CEFCYS.

Les intervenants

Emmanuel RUAUD

Référent informatique
LYON YNOV CAMPUS

Propulsé par ses passions, Emmanuel RUAUD devient ingénieur en simulation acoustique en 2012, pour poursuivre dans le développement logiciel puis la formation. Aujourd'hui il organise et développe le parcours des formations en informatique à Lyon Ynov Campus. Il est le garant de l'adéquation entre les formations et les métiers auxquelles elles préparent, tant au niveau du contenu que des méthodes pédagogiques employées. Emmanuel RUAUD conserve avec ferveur cette passion pour l'univers du numérique et s'emploie à la transmettre aux générations futures.

Adrien BRESSON

Directeur de projets réseaux et sécurité
DGE – ministère l'Economie, des Finances et de la Relance

Adrien BRESSON est ingénieur des Mines, diplômé de l'école Polytechnique et de l'école des Mines de Paris. Il débute sa carrière en 2016 au sein de la direction régionale de l'environnement, de l'aménagement et du logement de la région Normandie, en tant que chef du service en charge de la prévention des risques industriels et naturels. Il rejoint ensuite en 2019 la direction générale des entreprises au ministère de l'économie, des finances et de la relance, en tant que directeur de projets réseaux et sécurité. Il est en charge de l'élaboration et la mise en œuvre des mesures de politiques industrielles dans le secteur de la cybersécurité et des équipements télécoms, et a notamment piloté l'élaboration de la stratégie d'accélération cybersécurité du plan de relance.

Assia TRIA

Responsable scientifique, service sécurité des systèmes embarqués et composants
CEA-Leti

Après un début de carrière chez Gemplus où elle a passé 9 ans, Assia TRIA a rejoint en octobre 2005 le CEA-LETI pour mettre en place et diriger l'équipe de recherche commune entre le CEA et l'école nationale supérieure des mines de Saint-Étienne : « Systèmes et Architectures sécurisés ». De 2013 à 2019, elle a été chargée d'affaires, avec pour mission de diffuser les technologies clés génériques (KET) du CEA-TECH dans de multiples champs industriels principalement aux PME et ETI de la région PACA puis de la région Occitanie.
Depuis septembre 2019 elle est responsable scientifique au sein du service sécurité des systèmes embarqués et composants, en charge de l'animation scientifique, du ressourcement, des montages de projets collaboratifs et référente Europe pour le volet sécurité. Elle est auteur ou co-auteur de plus de 80 actes dans des conférences et autres revues, dans le domaine de la sécurité matérielle, cryptographie et biométrie. Elle est Co-chair du WG6.4 (Basic and Disruptive Technologies) au sein de l'ECSO (European Cyber Security Organisation), experte pour la Commission Européenne sur les calls cyber H2020 et FP7. De 2012-2017 elle a été membre élue du conseil d'administration du pôle de compétitivité « Solution Communicantes Sécurisées (SCS) ».
Assis TRIA est titulaire d'un doctorat (1994) de l'université de Montpellier, en électronique, optronique et systèmes et d'une HDR (2009) en science de l'ingénieur de l'université Jean Monnet de Saint-Étienne.

Philippe SIRAUDIN

Co-animateur du groupe Cybersécurité
ADIRA

Après une première carrière comme Officier dans l'Armée de Terre, Philippe SIRAUDIN s'est reconverti dans l'informatique en 1992. Il a alors occupé des fonctions managériales dans des directions de systèmes d'information en France et chez des grands constructeurs en Irlande (IBM et Dell).
Installé en région lyonnaise depuis 2008, il a travaillé comme Consultant pour des ESN régionales, occupé des postes de Direction de Systèmes d'Information en management de transition (secteur industriel lié à la Défense, secteur bancaire et secteur des transports publics), tout en occupant des fonctions d'Officier Supérieur de Réserve, expert Cyber, au sein du Ministère des Armées.
Philippe SIRAUDIN a quitté ses fonctions d'Officier de Réserve en 2018 en intégrant comme Directeur Commercial une ESN de premier plan, qu'il a quitté en 2020 pour créer Aiakos, société de Conseil en Cybersécurité.
Philippe est Breveté Officier des Armes, et est titulaire d'un Msc in Computing, du Dublin Institute of Technology. Il est membre de l'Adira (Association pour le Digital en Région Auvergne Rhone-Alpes), qu'il représente au Conseil Pédagogique de Sup la Mache, ainsi qu'au Comité de Perfectionnement du Pôle Supérieur de la formation d'Expert Cybersécurité Industriel (Bac+5 reconnu par l'Etat) de ce même établissement.

RENCONTRES
CYBERSÉCURITÉ
AUVERGNE-RHÔNE-ALPES

MERCI À NOS PARTENAIRES & SOUTIENS

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

PARTICULIERS, ENTREPRISES, COLLECTIVITÉS TERRITORIALES :

VOUS ÊTES **VICTIME D'ACTES MALVEILLANTS** SUR INTERNET ?

PIRATAGE

ARNAQUE

CHANTAGE

VIRUS

RENDEZ-VOUS SUR
WWW.CYBERMALVEILLANCE.GOUV.FR
POUR ÊTRE ASSISTÉ
ET CONSEILLÉ

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

MISSIONS
DU DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

1. **ASSISTANCE AUX VICTIMES** D'ACTES DE CYBERMALVEILLANCE
2. **PRÉVENTION ET SENSIBILISATION** SUR LA SÉCURITÉ NUMÉRIQUE
3. **OBSERVATION ET ANTICIPATION** DU RISQUE NUMÉRIQUE

MEMBRES

PREMIER MINISTRE

MINISTÈRE DE L'ÉDUCATION NATIONALE, DE LA JEUNESSE ET DES SPORTS

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA RELANCE

MINISTÈRE DES ARMÉES

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE LA JUSTICE

SECRÉTARIAT D'ÉTAT CHARGÉ DE LA TRANSITION NUMÉRIQUE ET DES COMMUNICATIONS ÉLECTRONIQUES

PLUS D'INFORMATIONS SUR **WWW.CYBERMALVEILLANCE.GOUV.FR**

LES JEUNES IHEDN

ENGAGEMENT

De la jeunesse

Les Jeunes IHEDN est la **première association européenne** et générationnelle sur les questions d'engagement, de défense et de sécurité. Elle est **sous le double parrainage de la ministre des Armées** et du **chef d'état major des armées**.

L'association regroupe les **auditeurs jeunes** formés par l'Institut des hautes études de défense nationale et s'ouvre à **l'ensemble de la jeunesse**.

Plateforme d'**engagement** et **réservoir de réflexions**, l'association offre, en France et à l'international, différents moyens de s'investir au profit des grands enjeux d'avenir qui animent notre pays.

Citoyenneté, **défense**, **sécurité nationale**, **souveraineté** ou encore **relations internationales** sont autant de thématiques sur lesquelles la jeunesse peut **faire émerger des solutions concrètes et durables**. Cela passe par la sensibilisation du plus grand nombre et c'est là que tout réside : l'Engagement.

Propulser l'en

Passerelle entre les l'association offre transformer vos idé

Développer l

Chaque année, l'a conférences, atelie techniques en prise

Que vous souhaitiez pro développement, tout est

NOS ACTIONS

0 cadres, 14 comités d'études, 2000 membres, une équipe média dédiée : c'est l'envergure d'une association ynamique qui repose sur quatre objectifs :

ngagement !

mondes civil, diplomatique et militaire, de nombreuses opportunités de ées en engagement concret.

Promouvoir l'expertise innovante

Articles, revues spécialisées, rapports d'étude, veilles : chaque année, ce sont 80 publications qui sont rédigées par nos membres et mises en valeur.

a connaissance

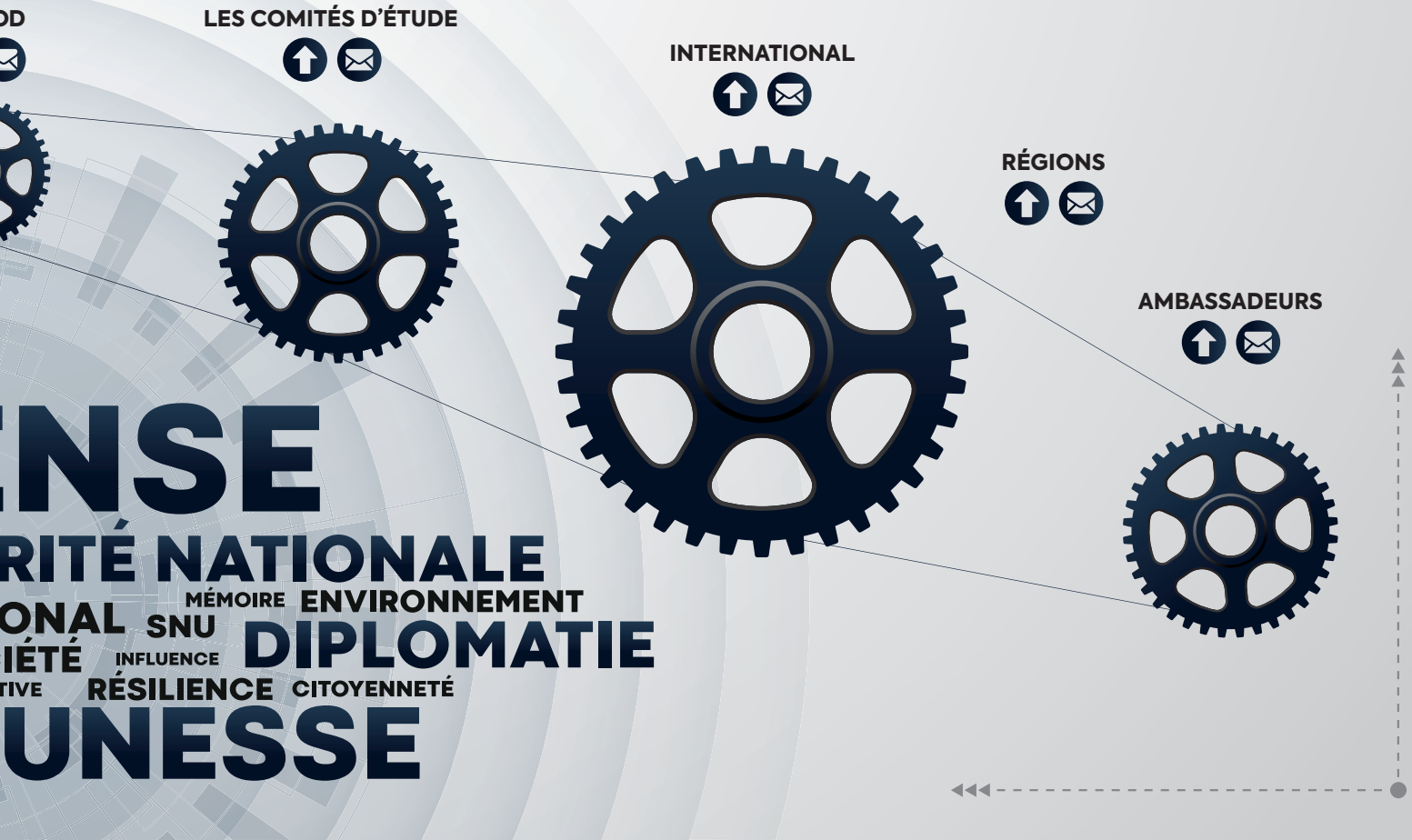
association organise une centaine de rs et visites sur des sujets généralistes ou e avec l'actualité.

Fédérer un réseau international

Étudiants, universitaires, chercheurs, jeunes professionnels, fonctionnaires, militaires ou salariés du secteur privé, le réseau des Jeunes IHEDN est riche de sa variété.

NOTRE ORGANISATION

ofiter des nombreux événements organisés par l'association, participer à ses actions ou soutenir son possible ! Il vous suffit de prendre contact ou d'aller sur le site jeunes-ihedn.org.



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

CONFIANCE, QUALITÉ, EXPERTISE : LE LABEL EXPERTCYBER

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Face à la professionnalisation et la complexité des cyberattaques, il est essentiel que les TPE, PME, collectivités et associations soient accompagnées dans leur sécurité numérique par des prestataires de confiance. Afin de leur offrir une meilleure lisibilité de la qualité des prestations et services, et un accompagnement adapté, **Cybermalveillance.gouv.fr lance un label reconnaissant l'expertise numérique de ces prestataires : le label ExpertCyber.**

1 QU'EST-CE QUE LE LABEL EXPERTCYBER ?

Le label ExpertCyber a été développé par Cybermalveillance.gouv.fr, en partenariat avec les principaux syndicats professionnels du secteur (Fédération EBEN, Cinov Numérique, Syntec Numérique), la Fédération Française de l'Assurance (FFA) et le soutien de l'AFNOR. Il vise à reconnaître l'expertise des professionnels en sécurité numérique assurant des **prestations d'installation, de maintenance et d'assistance en cas d'incident.**

Le label couvre les domaines suivants :
- **systèmes d'informations professionnels** (informatique, logiciels bureautiques, messageries, serveurs…) ;
- **téléphonie** (serveurs téléphoniques professionnels) ;
- **sites Internet** (administration et protection).

2 QUI SONT LES PRESTATAIRES LABELLISÉS ?

Sont éligibles à la labellisation, les entreprises de services informatiques de toute taille, justifiant d'une **expertise en sécurité numérique**, ayant démontré un niveau d'expertise technique et de transparence dans les domaines de l'assistance et de l'accompagnement de leurs clients.
Les candidats répondent à un questionnaire technique et produisent des documents attestant de leurs compétences afin de justifier l'ensemble des critères à satisfaire. Ils sont labellisés à l'issue d'un **audit réalisé par l'AFNOR**.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

3 QUI PEUT FAIRE APPEL À UN PRESTATAIRE LABELLISÉ EXPERTCYBER ?

Les prestataires labellisés ExpertCyber s'adressent à un **public professionnel** : toute entité justifiant d'une activité professionnelle, quels que soient son secteur et le nombre de salariés, une association, une collectivité…

4 POURQUOI FAIRE APPEL À UN PRESTATAIRE LABELLISÉ ?

Le label est un gage de qualité pour les professionnels souhaitant se faire accompagner par des prestataires de confiance. Ils peuvent en attendre :

- **Un niveau d'expertise et de compétence** en sécurité numérique ;
- **Un conseil de qualité** pour prévenir la survenue d'autres actes de cybermalveillance et sécuriser leurs installations informatiques ;
- **Une conformité administrative** (respect du cadre législatif et réglementaire, traitement des données personnelles conforme au RGPD, etc.) ;
- **Un sens de l'intérêt général** (veille et remontée d'incidents, conservation de la preuve numérique, etc.).

Les TPE, PME, collectivités et associations peuvent être mises en relation avec des professionnels labellisés ExpertCyber en se connectant au site Internet www.cybermalveillance.gouv.fr.

À PROPOS DE **CYBERMALVEILLANCE.GOUV.FR**

Cybermalveillance.gouv.fr est le dispositif national d'assistance aux victimes d'actes de cybermalveillance, de sensibilisation aux risques numériques et d'observation de la menace sur le territoire français.
Ses publics sont les particuliers, les entreprises (hors OIV et OSE) et les collectivités territoriales.
Le dispositif est piloté par une instance de coordination, le Groupement d'intérêt public (GIP) ACYMA, composé d'une cinquantaine de membres issus du secteur public, du privé et du domaine associatif, et qui contribuent chacun à sa mission d'intérêt général.
Cybermalveillance.gouv.fr référence sur sa plateforme des professionnels en sécurité numérique, répartis sur tout le territoire français, pour venir en aide aux victimes.

PLUS D'INFORMATIONS SUR
WWW.EXPERTCYBER.FR

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

LE RÉSEAU DES RÉFÉRENTS CYBERMENACES

Un réseau de professionnels partenaires, publics et privés, au service du tissu économique local.

UN CONSTAT

- Plus de 7 000 PME/TPE ont bénéficié d'une sensibilisation au risque cyber par la police judiciaire (source : SDLC).
- 1 entreprise française sur 5 ayant subi une attaque a versé une rançon. Les petites entreprises, plus vulnérables, sont les moins bien préparées (source: Rapport cyber HISCOX 2020).
- 84% des PME ont mis en place une formation de sensibilisation à la cybersécurité obligatoire (source: Rapport CISCO sur la cybersécurité 2020).
- 43% des violations des victimes de violations de données étaient des PME (source: Varonis blog cybersecurity statistics).

3 AXES OPÉRATIONNELS STRATÉGIQUES

AXE 1

Une équipe déployée sur tout le territoire national, associant des commissaires de police des services territoriaux de la police judiciaire, des policiers spécialisés en cybercriminalité, des réservistes opérationnels et citoyens de la Police nationale sur des missions d'experts en prévention ainsi que des partenaires privés.

AXE 2

Un dispositif visant à mener des actions de sensibilisation et de prévention auprès des entreprises sur les risques liés à la cybercriminalité.

AXE 3

Un accompagnement des victimes de cyberattaques en leur prodiguant les premiers gestes de sauvegarde des intérêts de l'entreprise et une orientation vers les services de police pour faciliter le dépôt de plainte et le recueil des preuves numériques.

LA MISE EN ŒUVRE DU RÉSEAU

Par qui ?

Le réseau est constitué :

- Du référent cybermenaces, commissaire de police de la DZPJ/DTPJ.
- De réservistes de la Police nationale issus du monde de l'entreprise: chef d'entreprise, cadre salarié, responsable de la sécurité des systèmes d'information.
- De partenaires privés (notamment commissaires aux comptes).

Avec l'appui de nombreux acteurs et de leurs réseaux : préfet de la zone de défense et de sécurité, CNCC, ANSSI, CNIL, FBF, etc.

Pour qui ?

Le réseau s'adresse principalement :

- à l'ensemble des directions de la Police nationale présentes sur le territoire national;
- aux TPE/PME.

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

VOUS SOUHAITEZ BÉNÉFICIER D'UNE SENSIBILISATION À LA CRIMINALITÉ FINANCIÈRE ET À LA CYBERCRIMINALITÉ ?

Les réservistes du RCM dispensent des conseils de prévention face à la criminalité utilisant les moyens numériques. Ces sensibilisations s'adressent aux salariés de l'entreprise, aux responsables informatiques et à leurs dirigeants. Les réservistes donnent des conseils de bonne hygiène numérique et de premiers secours en cas de cyberattaque. La connaissance des modes opératoires des criminels permet de prendre conscience des différentes failles humaines et technologiques employées. Ces conseils assurent une meilleure préservation des intérêts de l'entreprise face à la menace cybercriminelle.

VOUS ÊTES VICTIME D'UNE CYBERATTAQUE ?

Vous pouvez contacter le réseau des référents cybermenaces le plus proche. Ce service vous orientera vers les entreprises labellisées spécialisées en remédiation des systèmes informatiques. Les réservistes et policiers vous accompagneront également vers un service spécialisé de la Police nationale pour déposer plainte, en vue de demander réparation du préjudice subi. Les investigateurs en cybercriminalité de la police judiciaire veilleront à recueillir les preuves numériques afin de retrouver les auteurs de la cyberattaque.

LE RÉSEAU DES RÉFÉRENTS CYBERMENACES

Le réseau des référents cybermenaces renseigne, sensibilise et accompagne les PTE/PME du territoire :

CONTACTS

Bordeaux	cybermenaces-bordeaux@interieur.gouv.fr
Lille	cybermenaces-lille@interieur.gouv.fr
Lyon	cybermenaces-lyon@interieur.gouv.fr
Marseille	cybermenaces-marseille@interieur.gouv.fr
Montpellier	cybermenaces-montpellier@interieur.gouv.fr
Rennes	cybermenaces-rennes@interieur.gouv.fr
Strasbourg	cybermenaces-strasbourg@interieur.gouv.fr
Toulouse	cybermenaces-toulouse@interieur.gouv.fr

POLICE NATIONALE

Avantde Cliquer .com

L'humain au cœur de la cybersécurité

Vous êtes décideur…

Divisez /10
le risque de cyberattaques.

Développez la vigilance de vos utilisateurs et gagnez en sérénité

STOP

Pour en finir avec le phishing !

80% DES CYBERATTAQUES ONT POUR ORIGINE UN **E-MAIL FRAUDULEUX**

3 outils complémentaires

en live

UN AUDIT DE VULNERABILITÉ

L'APPRENTISSAGE PAR L'ACTION

UN BOUTON ALERTE CYBER

conçus / hébergés / développés en FRANCE

Les outils
Avant de Cliquer

UN AUDIT DE VULNERABILITÉ

En situation réelle, **IL MESURE** la vigilance de vos collaborateurs face à une **ATTAQUE** par **PHISHING !**

UN BOUTON ALERTE CYBER

Installé sur la **BARRE D'OUTILS** de la messagerie des utilisateurs, **IL SIGNALE** en direct les mails douteux au RSI.

L'APPRENTISSAGE PAR L'ACTION

Un algorithme intelligent

Il coordonne les résultats de l'audit avec le niveau des mails d'apprentissage et la plateforme de e-learning. Cet algorithme intègre 4 niveaux de difficulté croissante : de l'attaque de masse au mail personnalisé.

Notre solution EN VIDEO

SENSIBILISATION SUR POSTE DE TRAVAIL

Envoi d'e-mails de faux phishing

- Les mises en situation sont constituées de mails d'apprentissage adaptés au niveau de vigilance.

Une sensibilisation immédiate

- L'apprentissage par l'expérience développe une sensibilisation immédiate en cas de clic.

Montée en compétences personnalisée

- Programme créé sur mesure pour chaque utilisateur, il augmente la cybersécurité globale de l'organisation.

Ecrans de veille éducatifs

- Les écrans de veille personnalisés prônent les bonnes pratiques avec les contacts de vos services informatiques.

Plateforme de e-learning

- Des modules de formation en vidéo sont accessibles en ligne sur les risques cyber et les réflexes à acquérir.

Test de la clé USB

- Un système de suivi de la clé active la prise de conscience de la dangerosité des supports externes.

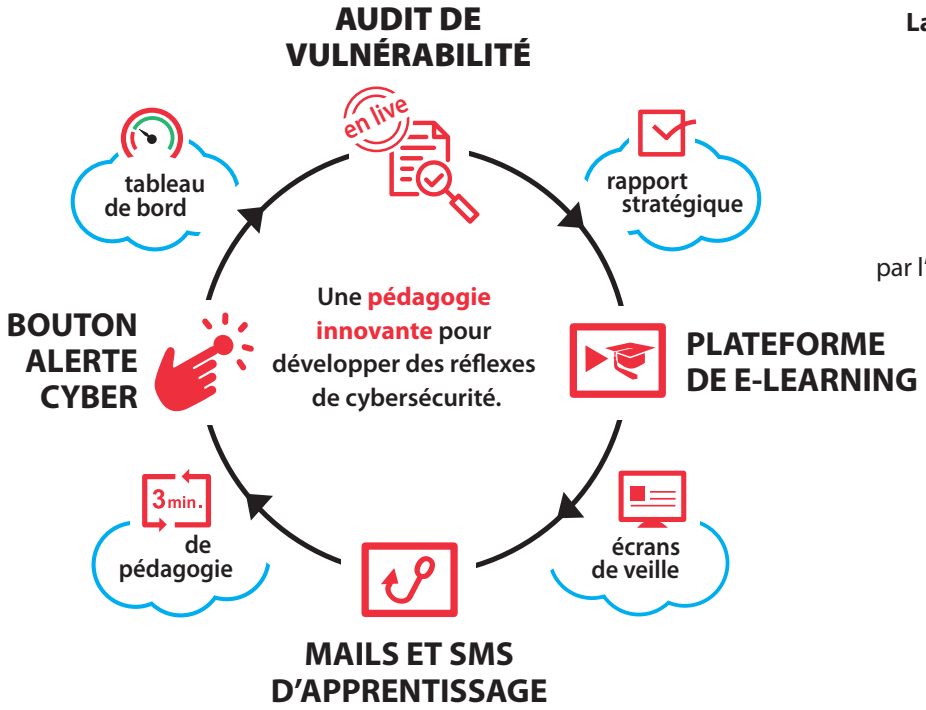
SOLAINN ACHATS INNOVANTS · bpifrance UNIVERSITE · C.A.I.H. Centrale d'Achat de l'Informatique Hospitalière · Éditeur référencé UGAP-SCC · UGAP · The 2021 French CYBER-SECURITY STARTUPS radar · WAVESTONE

Les formules
Avant de Cliquer

AUDIT DE VULNERABILITE : évaluer le niveau de maturité face au phishing

- Chaque utilisateur reçoit pendant une semaine des mails tests de difficulté croissante selon une méthodologie définie avec vous.
- Votre rapport de vulnérabilité, présenté en visioconférence, permet de définir votre stratégie de prévention cyber.
- L'audit de vulnérabilité est un outil indépendant d'évaluation ou intégré en phase initiale de la solution globale.

LA SOLUTION COMPLETE : des réflexes acquis



La sensibilisation à la cybersécurité réinventée pour diviser par 10 le risque de cyberattaques

Le programme de sensibilisation au phishing basé sur l'apprentissage par l'action est animé sur la durée de 1 an sans intervention de votre part.

Solution SaaS

La sensibilisation sur poste de travail est créée sur mesure pour chaque utilisateur.

2 MOIS EN TASK FORCE : parer à l'urgence

- Les clics malencontreux ouvrent une interface de conseils pour accroître les compétences des utilisateurs afin de ne pas recommencer !
- En initiant des réflexes de défense, cette solution constitue aussi une partie du programme complet de sensibilisation.
- Cet apprentissage sur poste de travail déclenche rapidement une prise de conscience concrète face aux attaques par phishing.

ASSOCIATION | SANTE | SERVICE PUBLIC | PME | INDUSTRIE | SECURITE | OPHP

Vous êtes décideur…

Avant de Cliquer permet aux DSI, RSSI, DPO et dirigeants de **réduire le risque** de cyberattaques de manière drastique. Au delà du développement d'une culture globale à la cybersécurité, la solution intègre un **accompagnement personnalisé pour les DSI, RSI et dirigeants**.

RGPD

Les organisations respectent leurs obligations de mise en place de mesures organisationnelles **de protection des données personnelles du RGPD.**
Les services informatiques se dégagent de la tâche chronophage que constitue **la sensibilisation au phishing** pour développer leur stratégie globale de cybersécurité.

Une entreprise française créée pour allier un apprentissage proactif avec l'évolution des menaces cyber.

Avant de Cliquer en 2021 c'est :

« 23 collaborateurs installés en Normandie.
La jeune entreprise créée en 2017 sensibilise **plus de 250 000 utilisateurs** et se développe aujourd'hui **à l'international. »**

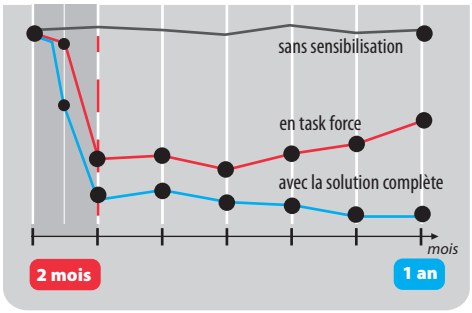
13 langues sous-titrées Français/anglais
Allemand, Anglais, Bulgare, Espagnol, Hongrois, Italien, Mandarin, Polonais, Portugais, Roumain, Russe, Turque, Ukrainien.

Niveau de risque

rouge : plus de 12% (rique extrême)
orange : de 9 à 12% (rique très élevé)
jaune : de 5 à 9% (rique élevé)
vert clair : de 2 à 5% (rique modéré)
vert foncé : moins de 2% (rique minoré)

Décideurs et RSI disposent de tableaux de suivi en temps réel.

Evolution des clics



Avantde Cliquer .com

L'humain au cœur de la cybersécurité

www.avantdecliquer.com

Coordination technique et commerciale
Carl : 06 31 37 41 50

Relations publiques
astrid@avantdecliquer.com
Astrid : 06 29 62 47 87

Lauréat de l'intelligence économique
Trophées de l'agroalimentaire 2019

Référencé CAIH
Centrale d'Achat de l'Informatique Hospitalière

Bpi France
Solution pertinente pour sensibiliser les utilisateurs à la cybersécurité

Référencé UGAP
L'achat public responsable

Finaliste du prix de l'innovation
Salon des Maires et les Collectivités Locales 2019

conçus / hébergés / développés en FRANCE

Conception Limage : 09/2021

PRÉSENTATION DU CYBERCERCLE

Missions / Vocation

Le CyberCercle est un cercle de réflexion créé en 2011 alors que la sécurité numérique – la cybersécurité - n'en était encore qu'à ses débuts pour de trop nombreuses organisations, et l'apanage d'un nombre encore limité d'experts techniques.

Convaincu que la sécurité et la confiance numériques ne pourront progresser qu'à la condition d'œuvrer collectivement, le CyberCercle s'est fixé 5 objectifs :

- Être un cadre privilégié d'échanges sur les questions de confiance et sécurité numériques,
- Être une plateforme de collaboration Public-Privé, Nationnal-Local, réunissant l'ensemble des parties prenantes,
- Décrypter le cadre réglementaire et les politiques publiques de sécurité et confiance numériques,
- Être une force de propositions pour accompagner la réflexion et le travail des parlementaires et des élus locaux sur ces questions,
- Favoriser le développement d'une culture de sécurité numérique, au delà de la sphère des experts techniques.

> **Agir efficacement ensemble pour construire une culture de sécurité numérique partagée.**

La sécurité et la confiance numériques ne constituent pas une finalité en soi mais un ensemble de disciplines et d'expertises à réunir aux services des métiers.
Dans cette perspective, le CyberCercle traite de sujets sectoriels avec une forte expertise dans les domaines de la santé, du maritime, des territoires, des collectivités, de la Défense et de sujets thématiques tels que la réglementation, l'innovation et la recherche, la formation, l'industrie 4.0...

Enfin, pour compléter cette vision « 360° » et traiter l'ensemble des dimensions stratégiques de la sécurité et de la confiance numériques, le CyberCercle a engagé des actions à l'échelon territorial avec, en 2019, un renforcement de sa présence et de son action au sein des territoires, engagées depuis 2015.

PRÉSENTATION DU CYBERCERCLE

Valeurs

Si la sécurité numérique représente un marché en tant que tel, ce qui montre son utilité économique et sa meilleure prise en compte par les organisations, il ne faut pas perdre de vue que la sécurité et la confiance numériques sont, avant toute chose, des enjeux de développement, de sécurité et de souveraineté, que ce soit au niveau national, européen et territorial.

Ce sont ces dimensions fondamentales, au service de tous, qui animent l'action du CyberCercle dont la philosophie s'appuie sur des valeurs d'engagement, de confiance, de sens du collectif et d'éthique.

Positionnement

Le CyberCercle a un positionnement unique.

Il est à la fois un « think tank » par la production de contenus, réflexions et propositions issus de travaux collectifs, par la diffusion d'analyses de personnalités, et par son travail d'animation de communautés ; et un créateur-organisateur d'événements fédérateurs pour :

- diffuser les éléments d'acculturation à la sécurité numérique sur l'ensemble du territoire,
- favoriser la compréhension et l'adhésion au travail parlementaire,
- devenir un acteur du conseil et de la formation pour accompagner les infrastructures dans leur réflexion en matière de politique interne de sécurité numérique,
- constituer un cadre d'influence vis-à-vis des pouvoirs publics.

Activités

Les activités du Cybercercle s'articulent autour :

➤ d'événements récurrents
- des matinales mensuelles à Paris, présidées par des parlementaires, depuis mai 2012
- des matinales bimestrielles en région, présidées par des élus, depuis septembre 2019
- des journées de rencontres, à Paris avec les RPCyber depuis 2013 ou en région, étapes du Tour de France de la Cybersécurité, depuis 2018
- des séminaires thématiques ou sectoriels comme les RPCyberMaritime depuis 2015

Ces événements sont plus ou moins ouverts.

➤ de publications:
- chaque vendredi, une Parole d'Expert sur notre site
- chaque semestre, un ouvrage dans la Collection CyberCercle - Regards croisés. Sont déjà parus "la Cybersécurité Maritime", "Sécurité numérique & collectivités", disponibles en ligne et en format papier.

➤ des groupes de travail thématiques en fonction de l'actualité nationale, européenne ou locale.

Le CyberCercle est ainsi un cadre de confiance œuvrant sur des sujets d'intérêt collectif, ainsi qu'une entité fédératrice de nombreuses associations et organisations publiques et privées.

Le CyberCercle a souvent été précurseur, parfois suivi ou imité, ce qui est sans nul doute le signe qu'il œuvre dans la bonne direction, dans ce domaine où les certitudes sont peu nombreuses et souvent trompeuses, domaine qui demande en permanence d'être à l'écoute, de s'adapter, de réagir, mais toujours au service des acteurs, décideurs, métiers, et de l'intérêt général.

Quelques chiffres

Le CyberCercle c'est :

- 100 matinales à Paris depuis mai 2012
- 12 matinales en régions depuis septembre 2019
- 12 étapes du TDFCyber depuis 2018
- 7 colloques parlementaires avec les RPCyber depuis 2013
- 5 colloques parlementaires sur le Maritime avec les RPCyberMaritime depuis 2015
- une douzaine par an d'interventions dans des colloques ou salons extérieurs
- + de 850 intervenants de haut niveau
- + de 11 000 participants [1]
- un compte Twitter réunissant plus de 9200 followers
- un réseau de plus de 10 000 contacts

[1] Participants uniques, venus pour beaucoup à plusieurs événements

MERCI À NOS PARTENAIRES & SOUTIENS

Partenaires

Soutiens

CYBER CERCLE

TOUR DE FRANCE DE LA CYBERSÉCURITÉ

#TDFCYBER

CYBER CERCLE

18 rue Tronchet - 69006 Lyon • contact@cybercercle.com • cybercercle.com • @CyberCercle

Réalisation : S.I.M. Publicité : 01 40 92 05 55