CYBER CERCLE

24 OCTOBRE 2019
LYON
RENCONTRES CYBERSÉCURITÉ
AUVERGNE RHONE-ALPES

#RCYBERARA
#TDFCYBER2019

La Région Auvergne-Rhône-Alpes

RHÔNE LE DÉPARTEMENT

TOUR DE FRANCE DE LA CYBERSÉCURITÉ

#TDFCYBER

@CyberCercle
@CyberTerritoire

ESPACES DÉMOS
TABLES RONDES
FORMATION
NETWORKING
RECRUTEMENT
ATELIERS

DOSSIER PARTICIPANT

RCyberAra LYON 24 OCTOBRE 2019

Edito

Christophe GUILLOTEAU
Président du Département du Rhône

La sécurité numérique est un enjeu majeur pour la protection de notre territoire national, face à la menace de cyberattaques qui se multiplient de manière considérable.

Ces attaques impactent l'Etat, les collectivités, les entreprises et les particuliers.

Les menaces sont bien réelles et transverses : ordinateurs bloqués et paralysie des sites Web, arrêt de la production d'entreprises et du fonctionnement des sites sensibles, incidence sur le chiffre d'affaires, vol de données bancaires ou données personnelles...
Pour les collectivités, ces attaques peuvent affecter la vie de tous les concitoyens, en paralysant par exemple le bon fonctionnement d'une cantine, d'une maison de retraite, ou d'un logement social...

Pour lutter contre ce fléau, la France et l'Europe s'organisent tout d'abord en se dotant d'un référentiel réglementaire.
Malgré ces nombreux dispositifs, près de 80 % des entreprises ont été victimes d'au moins une cyberattaque en 2018.
En France, le coût de ces cyberattaques est en hausse de 72% en 5 ans.

Devant ce constat et l'évolution quotidienne des attaques, l'inventivité croissante des pirates, il est donc primordial d'avoir un plan précis et d'identifier les éléments clés d'une cyber sécurité adaptée et spécifique.

Il faut sensibiliser les personnels, identifier les données sensibles, fixer des règles d'utilisation du système d'information, apprendre à repérer les anomalies de fonctionnement... et bien sûr aussi sécuriser son système d'information, avoir un plan de sauvegarde, éventuellement un plan de communication.

Cependant, toutes les collectivités ne sont pas équipées techniquement et financièrement pour répondre à ce défi qu'impose la sécurité numérique, sujet complexe et souvent mal appréhendé. C'est pourquoi nous devons, nous, acteurs des territoires, mutualiser nos ressources, nos outils, nos moyens. Et nos actions doivent être coordonnées et adaptées à nos territoires.

C'est aussi une priorité pour permettre à notre territoire et à l'action publique, ici au Département du Rhône, de se moderniser et de se développer : levier majeur de l'efficacité des services publics pour répondre au mieux aux attentes des usagers et de la protection de leurs données.

Les rencontres cyber sécurité sont essentielles pour créer des synergies avec l'ensemble des acteurs du monde économique public-privé, pour mieux cerner ce danger et apporter des solutions efficaces et concrètes.

DOSSIER PARTICIPANT

RCyberAra LYON 24 OCTOBRE 2019

Edito

Juliette JARRY
Vice-présidente de la Région Auvergne-Rhône-Alpes, en charge du numérique

Bienvenue aux Rencontres Cybersécurité Auvergne-Rhône-Alpes

Dans son rôle de fédérateur et en s'appuyant sur les acteurs de l'écosystème, la Région accompagne les entreprises dans leur transformation numérique.
Même si le nombre des cyber-attaques constatées en 2019 tend à se stabiliser, huit entreprises sur dix en France continuent d'être impactées, avec pour 59% d'entre elles des conséquences directes sur le chiffre d'affaire.
Face à la complexité croissante des avancées technologiques, des enjeux internationaux mais également de la pénurie de ressources humaines dans le domaine, nous devons nous doter d'une politique publique de cybersécurité efficace. Pour cela, il est primordial de prévoir les besoins à venir en matière d'emploi et de formation et de sensibiliser les utilisateurs pour une meilleure compréhension des enjeux qui entourent ces évolutions technologiques.
Pour répondre à ces objectifs, la Région s'est dotée d'un outil unique : le Campus Région du Numérique. Ce « navire amiral » dont l'ouverture sur notre site à Charbonnières-les-bains est prévue pour septembre 2020, constituera une plateforme d'échanges entre les écoles et les entreprises du territoire.
Il s'articulera autour de trois grands axes : la formation, l'accompagnement à la transformation des entreprises et l'innovation à travers une usine de recherche et d'innovation sur l'industrie du futur.

La sécurité numérique est une responsabilité individuelle et un enjeu collectif !

DOSSIER PARTICIPANT

RCyberAra LYON 24 OCTOBRE 2019

Edito

Crédit photo Alain Zimeray

Bénédicte PILLET
Présidente du CyberCercle

Le Tour de France de la Cybersécurité 2019 s'arrête à Lyon pour cette première édition des Rencontres de la Cybersécurité Auvergne-Rhône-Alpes.

Je remercie très sincèrement le Président du Départemental du Rhône, Christophe Guilloteau, d'avoir spontanément proposé d'accueillir cette étape du TDFCyber, et la Région Auvergne-Rhône-Alpes de s'y être associée également.

Nous vivons aujourd'hui une véritable transformation numérique, que ce soit au niveau national, international et bien évidemment territorial. Le travail à accomplir pour que nos territoires en pleine transformation numérique soient des territoires de « confiance numérique », favorisant le développement économique, la sécurité et des usages sécurisés au service de ses habitants, reste conséquent.

Le territoire dans lequel nous sommes pour cette 5ème étape du Tour de France de la Cybersécurité 2019 semble s'être résolument engagé dans cette voie. Le numérique et, de plus en plus, la sécurité numérique occupent en effet une place importante dans les politiques publiques des collectivités ici, en Auvergne-Rhône-Alpes, notamment la Région et le Département du Rhône, soutenues par un écosystème parmi les plus développés.
La sécurité numérique, si tout le monde (ou presque), est convaincu de sa nécessité, reste cependant parfois un axe insuffisamment pris en compte par les collectivités, PME-PMI, organismes de recherche et de formation, faute de temps, de moyens ou de solutions simples à mettre en œuvre. Pourtant, ces acteurs, maillons essentiels des écosystèmes, et ils sont nombreux dans la Région, sont au cœur du sujet.

Le CyberCercle a fait de la sécurité et la confiance numériques des territoires un axe majeur de son action. Raison pour laquelle il a, avec le soutien de CCI France, lancé l'année dernière le Tour de France de la Cybersécurité.
Aller au contact des acteurs locaux, quels qu'ils soient, 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, être force de propositions… sont les moteurs de notre action et de notre motivation.

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

Cette première édition des Rencontres de la Cybersécurité Auvergne-Rhône-Alpes, fort de ses nombreux partenaires, et je tiens à les en remercier, veut s'inscrire pleinement dans cette dynamique constructive.

Programme

RENCONTRES CYBERSÉCURITÉ AUVERGNE RHONE-ALPES

8h45 **Ouverture des travaux**

➤ Mot d'accueil
Bénédicte PILLIET, Présidente du CyberCercle
➤ Ouverture des travaux
Christophe GUILLOTEAU, Président du Département du Rhône
Juliette JARRY, Vice-présidente de la Région Auvergne-Rhône-Alpes, en charge du numérique
Général de corps d'armée Philippe LOIACONO, Gouverneur Militaire de Lyon, Officier général de zone de défense et de sécurité Sud-Est
Général de corps d'armée Philippe GUIMBERT, commandant de la région de Gendarmerie Auvergne-Rhône-Alpes - commandant la Gendarmerie pour la zone de défense et de sécurité Sud-Est

9h30 **Table ronde**
Innovation et cybersécurité :
quelles actions mener au profit de la transformation numérique des acteurs sur les territoires ?

Intervenants
- **ICA Chantal CAUDRON de COCQUEREAUMONT**, Responsable Innovation, Pôle SSI, Direction Générale de l'Armement
- **Alexandra KETCHEYAN**, Secrétaire générale, Délégation ministérielle à la sécurité et à la lutte contre les cybermenaces, ministère de l'Intérieur
- **Gabriel de BROSSES**, Directeur de la Cybersécurité, Groupe La Poste
- **Elisabeth DELALANDE**, Déléguée Régionale Auvergne-Rhône-Alpes, INPI
- **Jean-Baptiste MONIN**, Directeur IT Akademy, Campus Numérique

11h00 **Pause café**

11h30 **Interventions**
« Services numériques aux citoyens : où en sont les collectivités territoriales ? », présentation de l'étude du GROUPE LA POSTE
Nicolas PASTOR, Responsable des études et de l'ingénierie de projets pilotes, Direction du Développement territorial, Groupe LA POSTE

cybermalveillance.gouv.fr, un dispositif national au service de la cybersécurité sur les territoires : point de situation et perspectives
Adrienne CHARMET, chargée de mission, cybermalveillance.gouv.fr

La stratégie et les moyens de lutte contre la cybercriminalité de la Police nationale
Catherine CHAMBON, contrôleur général, sous-directrice de la lutte contre la cybercriminalité, DCPJ

Présentation de la Banque Européenne d'Investissement
Elodie de RECY, Directrice du Bureau du Groupe BEI en France, Banque Européenne d'Investissement

13h00 **Cocktail déjeunatoire**

14h30 **Ateliers**
Les ateliers durent deux heures et ont pour objectif, dans un cadre de confiance, de permettre aux différents acteurs, publics, privés, locaux, nationaux, spécialistes et non spécialistes de la sécurité numérique, d'échanger sur une thématique définie, de façon très pratique et opérationnelle. Des orateurs ouvrent l'atelier par des exposés d'une quinzaine de minutes chacun pour poser le cadre puis l'ensemble des participants est invité par l'animateur à s'exprimer, soit pour poser des questions, soit pour apporter une vision du sujet. L'objectif est d'une part de faire progresser l'ensemble des participants en favorisant le partage d'expérience, d'autre part de faire émerger des propositions d'actions susceptibles de faire avancer le sujet. A l'issue, des points forts de ces échanges sont dégagés et présentés en plénière en une quinzaine de minutes afin de permettre à l'ensemble des participants de bénéficier de ce travail.

➤ de la dématérialisation des services aux territoires de confiance, quels enjeux de sécurité numérique et quelles solutions pour les **collectivités territoriales** ?
Frédéric POINTU, RSSI, Métropole de Lyon
Eric POZZI, Référent régional à l'Intelligence Economique, Région de gendarmerie Auvergne-Rhône-Alpes
Nicolas PASTOR, Responsable des études et de l'ingénierie de projets pilotes, Direction du Développement territorial, Groupe LA POSTE

➤ de la sécurisation des infrastructures à l'industrie 4.0, comment insérer de la cybersécurité dans les **sites industriels** ?
Stéphane MEYNET, Président, CERTitude Numérique – senior advisor, CyberCercle
Alix MADET, Déléguée régionale à l'Information Stratégique et à la Sécurité Economique pour Auvergne-Rhône-Alpes, SISSE
Philippe GENOUX, Délégué général, Exera
Vincent RIONDET, Directeur Delivery – NEC (Network Engineering & Cybersecurity, Schneider Electric
Tarik ZEROUAL, Global Account Manager - Major industrial accounts, Stormshield
Vincent SERUCH, ICS Security Team Leader, Airbus Cybersecurity
Sébastien LAPIQUE, Responsable de l'Agence Auvergne Rhône Alpes, Digital Security

➤ à l'heure de la e-santé et d'une numérisation accrue des infrastructures médicales, quels enjeux de sécurité numérique et quelles perspectives pour le **secteur de la santé** ?
Cyrille ISAAC-SYBILLE, Député du Rhône, membre de la commission Numérique et Santé, Assemblée Nationale
Stéphane PASQUIER, Fonctionnaire de la Sécurité des Systèmes d'Information adjoint, ministères sociaux
Charles BLANC ROLIN, RSSI et DPO, Groupement Hospitalier de Territoire Cantal
Jean-Philippe GRANGETTE, Conseiller Défense et Sécurité Zone Sud/Est, Agence Régionale de Santé Auvergne-Rhône-Alpes

➤ **IA** et cybersécurité : enjeux et influences croisées ?
Jean-Michel LEFEVRE, Coordonnateur stratégique IA, Groupe La Poste
Mathieu MOREUX, Product Marketing Manager, Microsoft
Philippe NAULT, Responsable des équipes avant-vente régionales France, Fortinet
Sébastien GEST, Tech Evangelist, Vade Secure

➤ que peut-on attendre aujourd'hui de la **cyberassurance** ?
Maxime CARTAN, co-fondateur et Président, Citalid Cybersécurité
Cédric JOURDAN, souscripteur grands comptes et correspondant régional cyber assurance, Groupama Rhône-Alpes Auvergne
Eric LAMOURET, Président, syndicat des courtiers de réassurance et d'assurance, vice-président du cluster Assurance

➤ comment faire de la sécurité numérique un des piliers du développement **des transports et des véhicules intelligents** ?
Alexandra KETCHEYAN, Secrétaire générale, Délégation ministérielle à la sécurité et à la lutte contre les cybermenaces, ministère de l'Intérieur
Emmanuel de MAILLARD, Compliance Director and Data Privacy Officer, Renault Trucks
Michael KLINGER, Head of Security Consulting, et **Sylvie VOTTIER**, Expert Cybersecurity, ETAS & ESCRYPT
Philippe SCHIFANO, Directeur Technique et associé, et **Philippe CONCHONNET**, Consultant Senior en sécurité des systèmes d'information, Formind

➤ **comment sensibiliser en interne** ses collaborateurs aux bonnes pratiques de la sécurité numérique ?
Adrienne CHARMET, Chargée de mission, cybermalveillance.gouv.fr
François COUPEZ, avocat associé, Implid Legal - associé, groupe Implid , et **Noura MANSOURI**, Consultante manager, filière Sûreté et Sécurité, Implid

➤ **quels enjeux de formation pour la cybersécurité ?**
Thibault RENARD, Responsable Prospective et Anticipation du risque numérique, Pôle Data & Etudes, CCI France
Béryl BES, Déléguée générale, LDigital
Aline BARTHELEMY, membre du conseil d'administration, CefCys - Club des Femmes de la Cybersécurité
Axel ABATTU, Responsable du plateau NumericLab, Grenoble INP – Esisar

16h30 ■›› **Retex des ateliers par les animateurs en plénière**

17h30 ■›› **Verre de clôture** dans l'espace de rencontres-démonstrations

Les intervenants

Christophe GUILLOTEAU

Président du Département du Rhône

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.

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 au 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.

Juliette JARRY

Vice-présidente de la Région Auvergne-Rhône-Alpes, en charge du numérique

En 2006, tout juste diplômée d'un Mastère de sciences politiques (Institut d'Etudes Politiques de Lyon – EHEP de Paris), Juliette JARRY crée Adéa Présence, une entreprise spécialisée dans l'accompagnement à domicile de personnes âgées, enfants et adultes handicapés. Pour optimiser la gestion quotidienne, elle intègre très rapidement les outils numériques tant dans la relation avec ses salariés qu'avec ses clients.

Depuis janvier 2016, Juliette JARRY est Vice-présidente du Conseil régional Auvergne Rhône-Alpes déléguée aux infrastructures, à l'économie et aux usages numériques. Décidée à s'appuyer sur son expérience du monde entrepreneurial pour porter l'ambitieux projet numérique de la Région, elle propose une feuille de route stratégique autour de trois priorités : accélérer le déploiement des infrastructures (très haut débit et téléphonie), accompagner les entreprises dans leur transformation numérique - en s'appuyant sur le « campus numérique » pour développer les compétences via la formation initiale et continue - et développer les usages. Juliette JARRY a entrepris de fédérer les acteurs du territoire pour faire d'Auvergne-Rhône-Alpes la « Silicon Valley » européenne

GCA Philippe GUIMBERT

commandant de la région de Gendarmerie Auvergne-Rhône-Alpes - commandant la Gendarmerie pour la zone de défense et de sécurité Sud-Est

Depuis septembre 2018 : commandant de la région de Gendarmerie Auvergne-Rhône-Alpes, commandant la Gendarmerie pour la zone de défense et de sécurité Sud-Est

Précédemment...

1982-1985 : élève-officier à l'Ecole Spéciale Militaire de Saint-Cyr 1985-1986 : officier-élève à l'Ecole des Officiers de la Gendarmerie Nationale 1986-1989 : commandant de peloton à l'escadron 10/11 de gendarmerie mobile à Bordeaux-Bouliac 1989-1991 : escadron de sécurité de Berlin 1991-1994 : commandant la compagnie de gendarmerie départementale de Draguignan 1994-1998 : officier rédacteur à la section opérations puis chef de la section opérations extérieures (direction générale de la gendarmerie nationale/DGGN) 1998-1999 : stagiaire de la 6e promotion du collège interarmées de défense (école de guerre) 1999-2002 : officier rédacteur à la division Monde de l'état-major des Armées (relations internationales) 2002-2003 : auditeur au Collège de Défense de l'OTAN à Rome 2003-2006 : commandant du groupement de gendarmerie de la Sarthe au Mans 2006-2009 : attaché de sécurité intérieure près l'ambassade de France au Canada 2009-2010 : chef du bureau de la coopération internationale bilatérale à la DGGN/SDCI 2010-2013 : sous-directeur adjoint de la coopération de sécurité à la direction de la coopération internationale (ministère de l'Intérieur) Avril 2013 : sous-directeur de la coopération multilatérale et partenariale Août 2015 : conseiller pour la communication du DGGN et chef du SIRPA-Gendarmerie
Officier de la légion d'honneur Commandeur de l'ordre national du mérite Médaille de bronze de la défense nationale Médaille d'honneur de la police nationale Médaille Vigilance et Loyauté de la Sureté du Québec
Marié, 3 enfants
Cursus...
ESM Saint-Cyr : 1982-85 EOGN Melun : 1985-86 CID : 1998-1999 Auditeur du collège de Défense de l'OTAN : 2002/2003 Cycle des hautes études européennes de l'ENA : 2010 Cycle interministériel de management de l'État : 2013

GCA d'armée Philippe LOIACONO

Gouverneur Militaire de Lyon,
Officier général de zone de défense et de sécurité Sud-Est

Le général de corps d'armée Philippe Loiacono est né le 29 juillet 1962 à Castres. Saint-Cyrien de la promotion lieutenant-colonel Gaucher (1983-1986), il choisit l'arme des Troupes de Marine et poursuit sa formation à Draguignan.
Il sert au 3e Régiment d'artillerie de marine à Verdun puis au 5e Régiment Interarmes d'outre-mer à Djibouti comme officier de tir et officier de reconnaissance.
Il est affecté au 11e Régiment d'artillerie de marine à la Lande d'Ouée où il tient la fonction de commandant d'unité. Il participe à différentes opérations dans la corne de l'Afrique, en ex-Yougoslavie et au Rwanda.
Breveté d'études militaires supérieures, il est promu colonel en juillet 2004. L'année suivante, il prend le commandement du 4e Régiment du Service Militaire Adapté à la Réunion.
A l'issue de son temps de commandement, à l'été 2007, il rejoint l'Inspection de l'Armée de Terre pour y exercer les fonctions d'assistant militaire auprès du général inspecteur. Il participe notamment aux travaux du Livre Blanc sur la Défense et la Sécurité Nationale ainsi qu'à la montée en puissance de la Mission pour la Coordination de la Réforme (MCR) en charge de l'animation et de la coordination de la mise en oeuvre de la réforme portant réorganisation du ministère de la Défense.
Auditeur du centre des hautes études militaires et stagiaire à l'Institut des hautes études de défense nationale en septembre 2008, il devient adjoint au sous-chef « performance-synthèse » de l'état-major de l'armée de Terre en 2009 avec en particulier la responsabilité de conduire l'ensemble du chantier «participation pleine et entière» de la France dans l'OTAN pour la partie Terre.
A l'été 2010, il rejoint l'état-major des Armées pour y exercer les fonctions de chef de bureau relations internationales au sein de la division Cohérence Capacités de la chaîne Plans. Dans ce cadre, il porte les positions françaises au sein de l'agence européenne de défense, participe pleinement à la montée en puissance de la coopération franco-britannique et apporte sa contribution aux principaux travaux de l'Alliance atlantique.
Nommé général le 9 juillet 2012, il prend le commandement du Service Militaire Adapté.
Le 1er août 2015, il prend les fonctions de commandant du Centre Interarmées de Coordination du Soutien. Il est promu général de division le 1er août 2017.
Il est élevé au rang et appellation de général de corps d'armée le 1er juillet 2018, et nommé Gouverneur militaire de Lyon, officier général de zone de défense et de sécurité Sud-Est et commandant de zone Terre Sud-Est.
Le général de corps d'armée Philippe LOIACONO est commandeur de la Légion d'honneur, commandeur de l'ordre national du Mérite et titulaire de deux citations.
Il est marié et père de trois enfants.

Bénédicte PILLIET

Présidente fondatrice du CyberCercle

Crédit photo Alain Zimeray

Bénédicte Pilliet est depuis 2011 la Présidente fondatrice du CyberCercle, cercle de réflexion, d'expertise et d'échanges placé sous la dynamique des élus, parlementaires et locaux, qui traite des questions de confiance et de sécurité numériques, sous l'angle de la gouvernance, de la stratégie, des politiques publiques, de l'organisation et de la formation. Dans ce cadre, elle organise des événements fédérateurs réunissant l'ensemble des acteurs concernés, avec pour objectif de faire progresser les sujets de sécurité numérique en créant des cadres de confiance pour échanger expertises et expériences, favoriser le dialogue entre les organisations, entreprises, collectivités territoriales, engagées dans des process de transformation numérique et les acteurs publics et privés de la cybersécurité. Elle édite également une lettre d'information trimestrielle "Cybersécurité & Politiques Publiques".
Bénédicte Pilliet est 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 Capitole 1, et Directeur pédagogique du Certificat Sécurité Numérique de l'Université Paris-Dauphine. Elle est chargée de cours à l'Université Catholique de Lyon et à l'Institut Léonard de Vinci. Elle est également amenée à intervenir comme experte sur les sujets de sécurité numérique au sein de nombreuses organisations, colloques, congrès et salons.
Diplômée de Sciences Po Paris en 1990, Bénédicte Pilliet bénéficie d'une expertise dans la communication institutionnelle qu'elle a exercée dans plusieurs agences de communication au profit de collectivités, d'entreprises, de groupes industriels ou d'associations professionnelles dans différents secteurs. En 2001 elle s'oriente vers les Affaires Publiques sur les questions de Défense et de Sécurité Nationale, avant de se spécialiser sur la cybersécurité à partir de 2011.
Bénédicte Pilliet est, depuis 2007, Lieutenant-colonel de réserve (Citoyenne) de 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 auprès du Coordonnateur National.
Elle est Vice-présidente de l'association Les Amis de la RCC, membre d'honneur du CefCys (Club des Femmes de la Cybersécurité), membre fondateur du Cercle K2 et membre du CESIN (Club des Experts de la sécurité de l'information et du numérique).
Bénédicte Pilliet est titulaire de la Médaille de la Défense nationale, échelon or, agrafe cyber, et de la Médaille des Services Militaires Volontaires, échelon bronze.

Alexandra KETCHEYAN

Secrétaire Général
DMISC - ministère de l'Intérieur

Diplômée de l'Université Paris Nanterre (Master I en science politique et Master II en droit public) et de l'Université de Valenciennes (Master II en administration publique), Alexandra Ketcheyan est également auditrice-jeune de l'Institut national des hautes études de la sécurité et de la justice. Après quelques stages dans le secteur public, elle intègre, en 2014, le ministère de l'Intérieur, où elle a exercé des missions d'encadrement dans les services territoriaux, avant de rejoindre la Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces en 2018. En charge du secrétariat général de la Délégation, elle a participé à de nombreux travaux, dont la rédaction du rapport public annuel *État de la menace liée au numérique*.

Les intervenants

ICA Chantal CAUDRON DE COCQUEREAUMONT

Responsable Innovation, pôle SSI
Direction Générale de l'Armement, ministère des Armées

Après avoir été adjoint au responsable du Pôle SSI de la DGA, l'ICA Chantal Caudron de Cocquereaumont est depuis l'été 2019 responsable Innovation.

Elisabeth DELALANDE

Déléguée Régionale Auvergne-Rhône-Alpes
INPI

Ingénieur diplômée de l'UTC (Université de Technologie de Compiègne), puis diplômée du CEIPI (Centre d'Etudes Internationales de la Propriété Intellectuelle), Elisabeth DELALANDE est passionnée par l'innovation, l'entreprenariat et la propriété intellectuelle depuis plus de 20 ans. La protection et la valorisation du patrimoine des entreprises est au cœur de ses préoccupations. Elle dirige l'équipe de l'INPI (Institut National de la Propriété Industrielle) en région Auvergne-Rhône-Alpes. Ses missions : nouer des partenariats solides avec l'écosystème de l'innovation ; accompagner les entreprises pour que la propriété industrielle devienne un véritable atout de leur développement et soit un actif immatériel à forte valeur ajoutée.

Jean-Baptiste MONIN

Directeur IT Akademy, Campus Numérique

Jean-Baptiste Monin s'est passionné dès l'enfance pour l'informatique. Précurseur et de culture autodidacte, il s'est très tôt orienté sur la programmation et plus particulièrement la sécurité informatique. Après une carrière de consultant entamée il y a 20 ans, principalement exercée auprès d'acteurs publics et de grands comptes, il fonde à Lyon l'IT-Akademy : la première école de code et de cybersécurité.
Jean-Baptiste, en homme engagé, anime le club « Ethical Hacking » du CLUSIR et co-préside le « Pôle Jeunes » de la CPME Rhône. Il est également ancien élu de la Ville de Lyon et Juge au Tribunal de Commerce de Lyon.
Certifications professionnelles : ESD (Expert en Sécurité Digitale - ASTON), Zend PHP et Zend Framework Certified Engineer, GitHub Campus Advisor.

Nicolas PASTOR

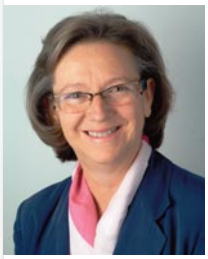
Responsable des études et de l'ingénierie de projets pilotes, Direction du développement territorial
GROUPE LA POSTE

Nicolas Pastor est responsable des études et de l'ingénierie de projets pilotes au sein de la direction du développement territorial du Groupe La Poste. Il y conduit des activités de développement stratégique en contribution à la modernisation de l'action publique.

Au sein d'administrations publiques locales, il a notamment accompagné des projets de transformation de la relation aux citoyens par le numérique. Il est diplômé de Sciences Po Bordeaux et de l'Université Paris-Dauphine.

Catherine CHAMBON

Contrôleur général
Sous-directeur de la lutte contre la cybercriminalité, DCPJ



Catherine CHAMBON a passé sa carrière au sein de la police judiciaire.

Adjoint au chef de la section économique et financière au sein de la SRPJ d'Orléans en 1989, elle devient chef de la brigade centrale de la répression des trafics de faux documents et de véhicules volés à la sous-direction des affaires criminelles de la DCPJ. Elle a ensuite occupé les fonctions de chef de la section économique et financière de la SRPJ d'Ajaccio puis d'adjoint et au chef de la 10ème division et de l'office de répression du faux monnayage au sein de la sous-direction des affaires économiques et financières de la DCPJ. De 2001 à 2006, elle occupe le poste de chef de l'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication). Puis, jusqu'en 2010, elle est adjoint au sous-directeur des ressources de l'évaluation et de la stratégie de la DCPJ. De 2010 à 2013, elle est sous-directeur des supports opérationnel au sein du service des technologies et des systèmes de l'information de la sécurité intérieure.

Elle occupe aujourd'hui la fonction de sous-directeur de la lutte contre la cybercriminalité.

Catherine CHAMBON est titulaire de l'ordre national du mérite, de la médaille d'honneur de la police nationale et de l'ordre de la légion d'honneur.

Elodie de RECY

Directrice du bureau du Groupe BEI en France
Banque Européenne d'Investissement

Diplômée de l'EM Lyon, Elodie de Récy a commencé sa carrière chez Arthur Andersen, elle a rejoint ensuite Cheuvreux de Virieu sur les activités de trading pour compte propre et de négociation pour compte de tiers. Puis elle entre à l'Inspection Générale de la Banque européenne d'investissement à Luxembourg, prend des responsabilités de coordination et stratégie sur l'activité Prêts en Europe avant de devenir Banquier Senior sur les opérations Corporates en Europe Occidentale puis Responsable adjointe de l'équipe Financements Corporate et Banques au sein du Département Europe Occidentale (France, Royaume-Uni, Belgique, Pays-Bas, Irlande et Luxembourg).

Alix MADET

Déléguée régionale à l'Information Stratégique et à la Sécurité Economique pour Auvergne-Rhône-Alpes
SISSE

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.
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.

Eric POZZI

Référent régional à l'Intelligence Economique
Région de Gendarmerie Auvergne-Rhône-Alpes

En gendarmerie depuis près de 31 ans, Eric POZZI occupe depuis 2008 la fonction de référent régional à la sécurité économique pour l'Auvergne-Rhône-Alpes :
- **2011 -2012 :** Création du schéma directeur IE régional et des outils associés dont 2 ont été retenus par les ateliers de performances de la Gendarmerie (2016 – Opération tranquillité Entreprises primé par le directeur général et 2017, les messages d'attention retenus au catalogue des ateliers comme bonne pratique. Ces mêmes messages ont également été retenus dans un avis de l'assemblée nationale édité en octobre 2017).
- **Depuis 9 ans :** Rédaction de plus de 750 rapports de pré-diagnostics de sécurité.
- **Septembre 2015 :** Cycle d'expertise IE auprès de l'INHESJ à l'Ecole Militaire PARIS.
- **Septembre 2014 à Mars 2015 :** Participation durant 6 mois à un groupe de travail national IE présidé par Mme Claude REVEL, déléguée interministérielle à l'intelligence économique avec, à l'issue, la remise d'un rapport au Premier Ministre
- **Janvier à Avril 2016 :** Participation durant 4 mois à un groupe de travail régional sur la création de la brigade numérique.
- **Depuis mi 2015 :** Eric POZZI a animé 136 conférences sur les thèmes des escroqueries aux faux ordres de virements internationaux et des cybermenaces pour un total de plus de 6 000 participants.

Frédéric POINTU

RSSI - Métropole de Lyon

Frédéric POINTU, diplômé d'une école d'ingénieur en informatique et d'un mastère spécialisé en management Qualité, Sécurité, Environnement (QSE), est Responsable Sécurité des Systèmes d'Information (RSSI) du Grand Lyon (Métropole de Lyon) depuis plusieurs années. À ce titre il est en charge de la gouvernance de la Sécurité des Systèmes Informatique (SSI) (définition et mise en œuvre de la politique sécurité informatique, définition et tenue à jour des processus et procédures SSI, communication sensibilisation formation interne sur la sécurité informatique), de la veille réglementaire SSI, des aspects techniques liés à la SSI (accompagnement sécurité des projets informatiques, sponsor des projets dédiés SSI), ainsi que de la gestion de crise informatique.

Avant ceci, il a travaillé en tant qu'architecte logiciel et développeur au sein du Grand Lyon et diverses sociétés de service. Il a auparavant travaillé plusieurs années dans le domaine du management QSE au sein de grands groupes de la région ainsi qu' en tant que conseil.

Les intervenants

Adrienne CHARMET

cybermalveillance.gouv.fr
Chargée de mission

Adrienne Charmet travaille depuis plus de 10 ans dans le numérique. Chargée de mission à l'ANSSI depuis 2017, elle rejoint le dispositif Cybermalveillance.gouv.fr en 2018 pour prendre en charge, entre autres, les relations institutionnelles et les projets menés avec les territoires.

Stéphane MEYNET

Président-Fondateur
CERTitude NUMERIQUE

Stéphane Meynet, ingénieur de l'École des Mines d'Alès, a démarré sa carrière dans l'industrie de la micro-électronique.
Après avoir été en charge pendant 10 ans de systèmes automatisés de contrôle de procédés industriels dans un contexte opérationnel, il a rejoint l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Dans un premier temps, il a conduit le projet sécurité des systèmes industriels en traitant les aspects de cybersécurité des infrastructures critiques de la nation. Puis, dans le cadre du déploiement de l'ANSSI au niveau territorial, il a été le délégué à la sécurité numérique pour la région Auvergne-Rhône-Alpes.

Il est aujourd'hui le président de CERTitude NUMERIQUE, entreprise dédiée à la sécurité numérique, et plus particulièrement appliquée aux systèmes industriels, qu'il a fondé en janvier 2018.

Philippe GENOUX

Délégué général
EXERA

Philippe Genoux est depuis juin 2014 le délégué général de l'association Exera regroupant une trentaine de membres, groupes industriels exploitant des équipements de mesure, de régulations et automatismes, ou centres d'essais et d'expertise. Parallèlement, il exerce une activité de consultant indépendant depuis fin 2000, et a mené plusieurs missions de conseil, notamment en ingénierie financière, rapprochement d'entreprises ou stratégie et organisation (voir www.pronoia-consulting.com).

Précédemment, il a occupé de 2009 à 2012 le poste de chef de la mission "Partenariats Public Privés" (PPP) du ministère de la défense, mission qu'il a créée en mars 2009. À la tête d'une équipe d'une douzaine de personnes hautement qualifiées (juristes, analystes et chargés de projets, il a ainsi directement participé à l'ensemble des opérations d'externalisations et des PPP lancés par le ministère de la défense durant cette période. De 2004 à 2009, il occupait le poste de chef du bureau "Nouveaux modes d'acquisition" qu'il a créé en juillet 2004 au sein de la délégation générale pour l'armement (DGA), et, à ce titre, a mené la passation du premier contrat de partenariat du ministère de la défense, notifié en janvier 2008, portant sur la mise à disposition de la base-école de Dax d'une flotte d'une quarantaine d'hélicoptères (durée 22 ans, montant 430 M€ HT).

Philippe Genoux a débuté sa carrière professionnelle au ministère de la défense en 1983 après un stage professionnel d'un an aux États-Unis en tant qu'ingénieur de recherche. D'abord chargé de l'orientation et du financement de projets de recherche, il a ensuite animé de 1985 à 1990 une équipe d'ingénieurs au sein du Bassin d'essais des carènes pour mener à bien la conception de propulseurs innovants destinés aux sous-marins nucléaires lanceurs d'engin types « l'Indomptable » et « le Triomphant ».

Entré en 1991 à Innolion, société de capital risque alors filiale du Crédit Lyonnais, il a constitué et géré un portefeuille de participations, valorisé à 10 M€, dans des sociétés "starts-up" de technologie. Dans le cadre de ses activités, il a été administrateur de sociétés françaises et étrangères (Grande Bretagne, États-Unis, Pays-Bas), et a directement participé à deux introductions en bourse (Londres et Amsterdam) et à de nombreuses cessions industrielles. Parallèlement, de 1994 à 1997, il a été directeur général puis président directeur général de 1994 à 1997 d'une société de robotique médicale détenue par Innolion avant de céder cette société au groupe médical suédois Elekta. À ce titre, il a négocié de nombreux accords (transferts technologiques, accords de distribution, dépôts de brevet).

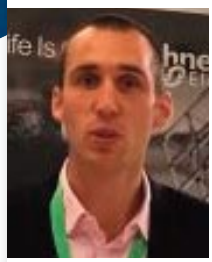
De 1997 à 2000, il a occupé le poste de Senior Vice-President au sein de la direction centrale des grandes entreprises du Crédit lyonnais. En charge du suivi relationnel de la banque avec ses clients français et étrangers dans les secteurs des équipementiers automobile et des fabricants d'électroménager, il a assuré la coordination des lignes métiers spécialisés de la banque et de son réseau d'agences nationales et étrangères, et, par ailleurs, le dimensionnement des enveloppes financières consolidés en fonction des évaluations de risque global.

Né en 1955, Philippe Genoux est diplômé de l'École Polytechnique (Promotion 1976) et de l'École Nationale Supérieure de Techniques Avancées (1981), et est Docteur de l'Université de Paris VI en Mathématiques Appliquées (1988). Il s'est vu décerné par l'Amicale du Génie Maritime et des Ingénieurs ENSTA le prix Roger Brard en 1993. Il a assuré de 2004 à 2012 de nombreuses formations sur les partenariats public-privé (ENA, IHEDN, CID, CFMD, etc.).

Ingénieur général de l'armement (2S), il est chevalier de la Légion d'Honneur et officier dans l'Ordre national du Mérite.

Vincent RIONDET

Directeur Delivery – NEC (Network Engineering & Cybersecurity)
Schneider Electric



De formation académique en automatique et contrôle industriel Vincent Riondet rejoint les équipes services du constructeur Schneider Electric dès sa sortie d'école en 2005. Il contribue dans un premier temps à l'expertise de Schneider dans les domaines de la disponibilité des installations et du contrôle avancé pour les procédés industriels. En 2010 l'attaque Stuxnet prend les industriels de court et ces derniers prennent conscience de la fragilité de leurs installations face aux cybermenace. Chez Schneider une équipe projet se constitue pour sécuriser une infrastructure industrielle de très grande ampleur et Vincent Riondet occupera un poste d'ingénieur réseau au sein de cette équipe. Par la suite il deviendra leader technique sur ce projet. En 2014 il participe à la création de l'équipe projets et services dédiée à la cybersécurité industrielle de Schneider Electric « NEC - Network Engineering & Cybersecurity » en devenant chef de projets au sein de cette dernière. Pendant 3 ans il managera des projets de sécurisations de petits sites industriels ainsi que des programmes portant sur plusieurs sites industriels en France et à l'étranger. Depuis 2018 il est responsable de l'équipe NEC ; une équipe intervenant en phase amont (audit, évaluation des risques, définition d'un PSSI industrielle, conception d'architecture, ...), en phase réalisation (déploiement de solutions), en phase exploitation (Maintien en Conditions de Sécurité, veille de vulnérabilités, ...) et proposant également des formations.

Vincent SERUCH

ICS Security Team Leader
AIRBUS CyberSecurity

Après plusieurs expériences significatives dans le domaine de la sécurité des systèmes d'information, Vincent rejoint Airbus CyberSecurity en 2018 en qualité d'Architecte afin de développer la sécurité des ICS.

Spécialiste en qualité de ICSS Lead Engineer et consultant, il met ses compétences au service de pré-étude d' installations dans divers pays on-shore et off-shore ainsi qu'au remplacement d'ICS incluant la sécurisation et mise en service de terminaux sur différents ports.

Vincent est diplômé de l'université de Versailles et d'un diplôme d'ingénieur en réseaux et cybersécurité du CNAM.

Tarik ZEROUAL

Global Account Manager - Major industrial accounts
Stormshield

Issu du monde de informatique opérationnel, Tarik ZEROUAL débute son parcours chez Psion Teklogix en 2004, au poste d'Ingénieur avant-vente. Entre 2008 et 2016, crée et dirige la filiale africaine de Be IP, société spécialisée dans la distribution de solutions de convergence et de sécurité des réseaux basée à Casablanca. De retour en France en 2016, Tarik devient consultant en Cybersécurité industrielle et participe à l'élaboration de programmes "industrie 4.0" au sein de grands groupes industriels français tel que PSA, ADP ou SAFRAN. Il intègre Stormshield en 2019 pour gérer les relations commerciales avec les grands groupes industriels français. Tarik ZEROUAL est titulaire d'un MBA de l'EM Lyon. Bickers à ses heures perdues, les Harley Davisdon et les belles courbes sont pour lui une autre manière de partager et vivre ses émotions.

Sébastien LAPIQUE

Responsable de l'Agence Auvergne Rhône Alpes
digital security

Sébastien Lapique, Responsable de l'Agence Auvergne Rhône Alpes chez digital.security : Ancien RSSI d'une société de services dans le domaine du nucléaire et ancien responsable d'activité dans d'autres sociétés de services. Il a œuvré tout au long de sa carrière dans le domaine de la sécurité des systèmes d'information. Il intervient également en qualité d'architecte sécurité dans les SI industriels afin d'accompagner nos clients pour l'identification des risques, la prise en compte des contraintes métier, et la déclinaison de plans projets s'intégrant dans une démarche d'Industrie 4.0.

Cyrille ISAAC-SYBILLE

Député du Rhône
Assemblée Nationale

Retrouver la présentation du député sur le site de l'Assemblée Nationale. ici

Les intervenants

Mathieu MOREUX

Product Marketing Manager Cybersécurité
Microsoft France

Mathieu Moreux est diplômé en Economie-Finance de l'Institut d'Etudes Politiques - Sciences Po Lille et en management international de projets (MIB) de l'Université Paris-Dauphine. Après plusieurs années d'expérience chez des pure-players de la cybersécurité, successivement en tant que Chef de projet Marketing et Stratégie puis Responsable des partenariats technologiques, il est depuis 2018 Product Marketing Manager Cybersécurité chez Microsoft France.

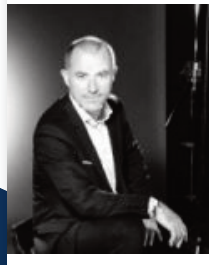
Sébastien GEST

Tech Evangelist
VADE SECURE

Fort d'une expérience acquise dans les Télécom et l'infrastructure informatique, Sébastien GEST occupe la fonction de Tech Evangelist chez Vade Secure. Il intervient dans des conférences internationales et auprès des entreprises et il a pour mission d'éduquer les utilisateurs des systèmes d'informations sur les risques liés à la cybercriminalité.

Philippe NAULT

Responsable des Equipes Avant-Vente Régionales France
Fortinet



Philippe NAULT possède plus de 20 ans d'expérience dans les réseaux, la sécurité et la mobilité. Après avoir assuré l'encadrement et le développement d'équipes techniques auprès de différents constructeurs tels que Newbridge, Symantec, Symbol, Motorola et Zebra Technologies, il a rejoint il y a quelques mois, Fortinet, leader de la cybersécurité en France, en tant que Responsable des Equipes Avant-Vente Régionales France (Paris et Régions)

Stéphane PASQUIER

FSSI adjoint - ministère sociaux

Stéphane Pasquier, ingénieur de recherche diplômé de Télécom Lille, est fonctionnaire de sécurité des systèmes d'information adjoint pour les ministères sociaux depuis octobre 2015. A ce titre, il est en charge du pilotage de la voie fonctionnelle de la SSI du ministère, de la définition et du contrôle des politiques de sécurité des SI, de la sensibilisation des personnels, du déploiement d'outils sécurisés de l'état et de l'animation des organismes et établissements sous tutelle. Il a été pendant 9 ans responsable de la sécurité des systèmes d'information pour le ministère de la culture et de la communication, après avoir exercé pendant 15 au sein de France Télécom en tant que RSSI poste de travail et expert réseau. Stéphane Pasquier donne également des cours dans le domaine SSI, intervient dans de nombreux colloques et est présent dans la vie associative des experts en Sécurité du Système d'Information : il est notamment membre du Clusif et du CESIN.

Jean-Michel LEFEVRE

Coordinateur stratégique Intelligence Artificielle
GROUPE LA POSTE

Issu de l'Ensimag en 2014 et après une activité de Recherche en Intelligence Artificielle au laboratoire de l'INPG, Jean-Michel LEFEVRE s'est alors tourné vers la Robotique et l'informatique Industrielle, soit dans des start-ups innovantes soit dans des grands groupes (Alstom, Groupe Open, Dassault Systèmes,). Il prend en 2009 la Direction de Probayes, société d'IA née en 2003 et intégrée au groupe La Poste en 2016. Probayes regroupe aujourd'hui à Grenoble et Paris 55 ingénieurs et docteurs en IA et travaille dans de nombreux secteurs industriels et de services. Jean-Michel LEFEVRE est depuis Septembre 2018 coordinateur stratégique Intelligence Artificielle du groupe La Poste et ainsi l'ambassadeur de Probayes au sein du groupe.

Cédric JOURDAN

Souscripteur grands comptes et correspondant régional cyber assurance
Groupama Rhône-Alpes Auvergne

Très engagé dans secteur des assurances, Cédric Jourdan a débuté sa carrière chez Allianz dans l'analyse des risques d'entreprises puis vers des fonctions d'inspecteur commercial dans le milieu du courtage. Chez Groupama Rhône-Alpes Auvergne depuis 2016, il est désormais en charge de l'élaboration des offres pour les grands risques relevant des marchés publics et participe à la conception des produits cyber en tant que correspondant régional.

Emmanuel de MAILLARD

Compliance Director Data Privacy Officer
Renault Trucks

ESC Amiens 1997 -2005 : EDS- A.T. Kearney : Conseil en Stratégie, Organisation et Systèmes d'Information 2006-2019 : Renault Trucks (Volvo Group) :

- Développement d'une entité de conseil interne
- Directeur Stratégie
- Directeur de la Conformité

Michaël KLINGER

Head of Cyber security
ETAS - ESCRYPT

Michaël Klinger a travaillé plusieurs années chez Thales dans le développement de logiciel radio où il a acquis toutes les bonnes pratiques en sécurité logiciel, mis en application l'eXtrem Programing et managé des équipes pour améliorer leur flexibilité et réactivité.

Après cette expérience dans le contexte des radios militaires, il a développé son expertise dans la division cyber de Thales en tant que program manager. Il a piloté pendant 10 ans l'innovation et le développement de nouveaux produits de cyber sécurité. Certains de ces produits ont été qualifiés par la Direction Générale de l'Armement Maîtrise de l'Information ou par l'ANSSI, en particulier dans le contexte de la directive européenne NIS (Security on Network Information System), transposée en France par la LPM (Loi de Programmation Militaire).

Il développe aujourd'hui les activités de cyber sécurité chez ESCRYPT France, dont le champ d'action s'étend aussi sur la Belgique, le Luxembourg, l'Espagne, le Portugal et l'Afrique du nord. Les domaines abordés concernent les industries Automobile, Industries 4.0, Opérateurs d'Importance vitale, Opérateurs de Services Essentiels, Smart City, Smart Transport, ... Smart écosystèmes ainsi que le support dans la mise en oeuvre des nouvelles règlementations internationales ISO 21434 et UNECE WP.29 pour l'accompagnement des OEMs et Tier x du secteur automobile.

Maxime CARTAN

Président cofondateur
Citalid Cybersécurité

Maxime Cartan est le Président de Citalid Cybersécurité, start-up qu'il a co-fondée avec Alexandre Dieulangard fin 2017. Doublement primée aux Assises de la Sécurité 2018, Citalid propose une plateforme innovante de management des risques cyber. Auparavant, Maxime Cartan travaillait au centre opérationnel de l'ANSSI (l'autorité nationale de cyberdéfense) en tant que spécialiste des cybermenaces. Ingénieur en sécurité informatique offensive de l'École Centrale Paris et diplômé de l'ESSEC, il avait auparavant eu une première expérience comme associé d'une start-up d'analyse géopolitique prédictive.

Eric LAMOURET

Président
Syndicat des courtiers de réassurance et d'assurance

Diplômé de l'ESC Bretagne, Éric LAMOURET évolue depuis 28 ans dans le secteur de l'assurance, spécialisé dans la maîtrise stratégique et opérationnelle de projets de croissance intensive à forts enjeux de structuration, développement, rationalisation et valorisation des groupes au sein desquels il a exercé successivement des fonctions de direction commerciale puis Directeur Associé au sein de 3 compagnies d'assurances leaders du marché. Devenu depuis 15 ans Directeur Général dans le monde du courtage, il était depuis 2010 Directeur Général Associé de l'entité directe du Groupe AXELLIANCE, 10ème groupe de courtage français, avant de prendre en charge mi-2014 le lancement in extenso d'un pôle spécialisé de la structure grossiste AXELLIANCE SOLUTION. Eric LAMOURET est par ailleurs Président du plus ancien syndicat de courtage en France, le SYCRA, Syndicat des Courtiers de Réassurance et d'Assurance, membre du MEDEF Lyon-Rhône, Vice-Président du premier et seul pôle d'excellence du genre au niveau national, le Cluster d'Assurance de la région Auvergne-Rhône-Alpes, première place régionale du courtage national après Paris-Île de France. Éric LAMOURET est également Vice-Président de l'Association Interprofessionnelle de l'Assurance Lyonnaise (AIAL), administrateur de l'Institut des Assurances de Lyon (IAL) et membre permanent du Comité Scientifique de l'Ecole Polytechnique d'Assurance. Acteur aguerri dans sa sphère professionnelle des risques cyber, il est dirigeant associé d'une structure spécialisée en cyber sécurité et cyber assurance qui accompagne les entreprises dans la protection de leur patrimoine numérique et informationnel. Ce parcours riche et varié, avec une complète et très active immersion dans le monde de l'assurance et du courtage lui octroie une parfaite maîtrise du secteur et de ses réseaux de distribution.

Les intervenants

Sylvie VOTTIER

Expert Cybersecurity
ETAS - ESCRYPT

Sylvie Vottier bénéficie de 30 ans d'expériences en recherche duale et en innovation au CNRS en partenariat avec des industriels du secteur civil et militaire, startup, spin-off et SATT. Elle y est notamment coordinatrice régionale de la SSI sur la région centre-est pour les unités de recherche du CNRS, puis Fonctionnaire Sécurité Défense et Responsable du Management de la SSI sur sites sensibles et critiques : responsable de la mise en place de la PPST, création de Zones à Régime Restrictif ZRRs. En 2015 elle devient FSSI - Fonctionnaire Sécurité des Systèmes d'Information auprès du Haut Fonctionnaire Correspondant de Défense et de Sécurité à la direction diplomatique et de défense du Ministère des Affaires Etrangères, de l'ANSSI, du SGDSN et de l'interministériel : responsable de la gouvernance cyber de l'administration centrale et des emprises diplomatiques à l'étranger, avant de devenir en 2017 architecte de cohérence SSI pour l'ensemble des opérations d'armement de l'unité de Management Terrestre de la Direction Générale de l'Armement. Après avoir été consultante expert en stratégie et en gouvernance cyberdéfense et cybersécurité pour le groupe SII Ile de France et Centre Loire, elle est aujourd'hui consultante expert en cybersécurité au sein d'ESCRYPT ETAS.

Philippe SCHIFANO

Directeur technique et Associé
Formind

Directeur technique et Associé de Formind, Philippe SCHIFANO intervient depuis 20 ans au sein de grands groupes sur des sujets de cybersécurité et de gestion des risques. Au cours de ces dernières années, il a notamment accompagné plusieurs acteurs majeurs du Transport et de l'Industrie dans la prise en compte des enjeux de sécurité SI dans leurs programmes de transformation digitale ainsi que dans l'accompagnement sécurité de projets relatifs à l'IoT et au développement de systèmes de transport autonome.

Noura MANSOURI

Consultante manager, filière Sûreté et Sécurité
Implid

Nora Mansouri, consultante Manager au sein d'implid et plus spécifiquement de sa filière Sûreté et Sécurité. Elle accompagne, avec une dizaine de consultants, les entreprises dans la gestion de leurs projets de sécurité, dans la transformation de leurs organisations et dans la mobilisation des hommes. De la compréhension des besoins à la déclinaison des stratégies des clients, elle apporte et crée de la valeur dans des projets de changement à fort enjeu tout en intégrant différentes préoccupations : gouvernance de la fonction sécurité, conformité réglementaire, évolution des modèles de management et du pilotage des équipes, sensibilisation des acteurs opérationnels pour mieux répondre aux enjeux de la cybersécurité. L'ambition de la filière Sûreté et Sécurité d'implid est double : Rendre résiliente l'entreprise en protégeant son patrimoine numérique. A l'heure du tout numérique il est devenu vital pour les entreprises de maintenir leurs activités et images malgré les pires scénarios cyber redoutés. Augmenter le capital confiance de l'entreprise en l'aidant à intégrer la sécurité dans le développement de ses produits et services. La confiance numérique - autrement dit la sécurisation des services et la protection des données - est aujourd'hui une source de valeur ajoutée commerciale.

Philippe CONCHONNET

Consultant Senior en sécurité des systèmes d'information
Formind

Consultant Senior en sécurité des systèmes d'information, Philippe intervient auprès de grands groupes français depuis plus de 20 ans sur des problématiques aussi bien techniques qu'organisationnelles et a mené plusieurs missions de sensibilisation auprès de diverses populations. Après presque 10 années au sein d'un opérateur télécom et de nombreux travaux dans le domaine de la gestion des identités et des accès, Philippe est plus récemment intervenu sur les problématiques de devsecops ainsi que de sécurité applicative dans des contextes industriels.

Thibault RENARD

Responsable Prospective - Anticipation du risque numérique Pôle Data & Etudes
CCI France

Thibault RENARD est depuis juillet 2018 Responsable Prospective et Anticipation du risque numérique au Pôle Data & Etudes de CCI FRANCE, établissement national fédérateur et animateur des Chambres de Commerce et d'Industrie. Il y était auparavant Responsable Intelligence Economique après avoir été en poste à la Mission Economique de l'Ambassade de France en Autriche.

Il est également administrateur au syndicat Français de l'Intelligence Economique (Synfie).

Titulaire d'une Maîtrise de Science Physiques et d'un DESS Intelligence Économique et Développement de l'Entreprise, il intervient par ailleurs sur l'Intelligence Economique Européenne et Territoriale en Ecoles de Commerce et d'Ingénieur.

Béryl BES

Déléguée Générale
Fondation LDIGITAL

Béryl BES est Déléguée Générale de la Fondation LDigital depuis janvier 2019. Créé en 2016, le collectif LDigital regroupent déjà plus d'une centaine d'acteurs locaux dans la région Auvergne Rhône Alpes investis sur la problématique de la présence des femmes dans les métiers du numérique. Depuis janvier 2018, ce collectif se structure et devient la Fondation LDigital, abritée par la Fondation Pour l'Université de Lyon qui a pour objectif d'accompagner et sensibiliser les femmes sur les métiers et leurs débouchés dans la filière du numérique. Dans ce cadre la Fondation LDigital développe des actions concrètes auprès des jeunes filles, des femmes et des entreprises afin de connecter les besoins en numérique des entreprises et les talents féminins. Diplomée de Skema Business School en 1993, Beryl Bès a travaillé pendant 15 ans dans la banque et l'assurance. En 2009, elle démissionne et créée son propre cabinet de courtage en assurance et en crédit : BB-A Conseil. Elle accompagne des entrepreneures à passer de l'idée au projet et du projet à l'action en actionnant notamment les leviers numériques et financiers.

François COUPEZ

Avocat associé
Implid Legal Associé - Groupe Implid

Associé du cabinet implid Legal Avocat à la Cour, fondateur et associé-gérant d'ATIPIC Avocat devenu implid Legal (en fusionnant avec deux autres cabinets), juriste de formation, Me Coupez est titulaire d'un Master 2 « Audit et Expertise en informatique et techniques associés » pour l'aspect technique et d'un Master 2 « Droit du multimédia et de l'Informatique » pour l'aspect juridique. Il met sa double compétence en droit et technologies de l'information au service des entreprises internationales ou de taille plus réduite afin de les conseiller et de les assister face à leurs contraintes réglementaires. Ancien responsable du droit des nouvelles technologies du Groupe Société Générale, ou encore avocat associé-gérant et responsable de l'entité parisienne d'un cabinet d'avocat reconnu spécialisé dans le droit des nouvelles technologies, il est également titulaire du Certificat de spécialisation en Droit des nouvelles technologies délivré par le Conseil National des Barreaux, ainsi que du Certificat de Délégué à la Protection des Données (référentiel de la CNIL – certification AFNOR). Intervenant régulier dans des colloques, des tables rondes, ou des formations spécifiques, auteur d'articles de doctrine sur les problématiques juridiques émergentes et le droit de la sécurité des systèmes d'information, Me Coupez enseigne depuis de nombreuses années dans le Master 2 « Droit du multimédia et de l'Informatique » de l'Université Paris 2 Panthéon-Assa, à Paris Dauphine ou encore au CNAM. Il a également enseigné le droit de la sécurité des systèmes d'information au CFSSI. Il est membre de l'Association nationale des juristes de banque (ANJB), de l'association du droit des nouvelles technologies Cyberlex, et de l'Association Française des Correspondants à la protection des Données à caractère Personnel (AFCDP).

Aline BARTHELEMY

Membre du conseil d'administration
Club des Femmes de la Cybersécurité

Aline Barthelemy travaille dans le domaine de la cybersécurité depuis 15 ans. Elle a occupé différents postes dans la sécurité applicative, le gestion de risques IT ou la sécurisation d'assets critiques, avant de prendre le poste de RSSI Groupe chez Louis Dreyfus il y a 2 ans. De formation Ingénieure en Genie Industriel INSA, Aline a complété son cursus avec un execMBA, pour pouvoir mieux adresser la complexité des enjeux cyber et leur impact au plus haut niveau de l'entreprise.

RENCONTRES
CYBERSÉCURITÉ
AUVERGNE RHONE-ALPES

MERCI À NOS PARTENAIRES

Collectivité locale de proximité, le Conseil départemental exerce, à l'échelle de son territoire, les compétences qui lui sont confiées par la loi.
Depuis 2015, le Département du Rhône dispose d'une nouvelle configuration territoriale avec la séparation de la Métropole de Lyon. C'est une exception française.

RHÔNE
LE DÉPARTEMENT

Grâce à ses politiques sociales innovantes et à ses investissements, le Département constitue le premier acteur des solidarités humaines et territoriales. Sur le territoire, le Département est représenté par des Maisons du Rhône, dans chacun des 13 cantons. Elles offrent aux Rhodaniens un accueil de proximité.

SOLIDARITÉ, ACTION SOCIALE ET SANTÉ

Véritable « chef de file » des solidarités, le Département accompagne les Rhodaniens à toutes les étapes de la vie et est présent pour les familles et tous ceux confrontés à des difficultés sociales, économiques ou humaines.
Il intervient dans le champ de l'enfance (protection maternelle et infantile, adoption, protection de l'enfance, soutien aux familles en difficulté), du handicap (hébergement, insertion sociale et aides financières aux personnes handicapées), des personnes âgées et de la dépendance (création et gestion des maisons de retraite, aides), de la gestion des allocations individuelles de solidarité (RSA, APA, PCH), de l'insertion et de l'emploi.

COLLÈGES

Le Rhône s'engage à construire, rénover, entretenir et équiper les 33 collèges publics de son territoire, subventionner les 18 privés, assurer le fonctionnement des demi-pensions des collèges, gérer les agents techniques des collèges, assurer le transport des collégiens vers les sites sportifs, et la location d'installations sportives dans le cadre des cours d'EPS. Au-delà de ces obligations, le Rhône mène une politique volontariste d'actions vers le développement des usages numériques éducatifs (une classe mobile par collège, collèges connectés…) et le devoir de mémoire.

CULTURE, TOURISME, SPORT

Le Département dispose d'une **médiathèque avec 2 sites (Chaponost et Limas)** afin d'alimenter les 156 bibliothèques municipales des communes de notre territoire.
Unique musée du Département, le **Musée et Site archéologique de Saint-Romain-en-Gal – Vienne** dispose d'une image moderne qui allie son ancrage archéologique à sa résonnance au monde contemporain grâce à une programmation d'expositions, d'événements et de rendez-vous culturels invitant scientifiques, archéologues, artistes plasticiens, musiciens et publics à revisiter cet héritage exceptionnel.
Les **Archives départementales et métropolitaines du Département du Rhône et de la métropole de Lyon** constituent la mémoire des habitants du territoire.
Le Département accompagne et développe la pratique du sport, en soutenant les associations et des manifestations sportives de haut niveau et le développement des sections sportives des collèges.
Le Rhône affirme également son soutien à différentes filières touristiques : l'oeno-tourisme/gastronomie, les randonnées, le tourisme fluvial, culturel et patrimonial.

DÉVELOPPEMENT DES TERRITOIRES ET INFRASTRUCTURES

L'aménagement et le développement équilibré des territoires fait partie des principales préoccupations dans l'exercice des missions départementales, ce que le Rhône concrétise à travers le Partenariat territorial, qui fait de lui le partenaire privilégié des communes et communautés de communes.
Le Département du Rhône est un territoire agricole. Il est le partenaire historique des agriculteurs : les conventions de partenariats avec la Chambre d'agriculture et les aides exceptionnelles en témoignent.

LE TRÈS HAUT DÉBIT : UN PROJET DE TERRITOIRE

Le Département du Rhône s'investit dans l'aménagement en très haut débit de son territoire. Atout essentiel de développement territorial, l'aménagement numérique en très haut débit est un facteur de modernité, de vitalité et d'attractivité du territoire rhodanien. En 2022, 100% des foyers et locaux professionnels du Rhône pourront ainsi se raccorder à la fibre.
Le Département intervient aussi dans le domaine de l'environnement (eau, déchets, protection des espaces naturels…).
Il est chargé de la construction et de l'entretien des 2872 km de routes départementales.

Le Département et la Métropole de Lyon participent à la gestion du Service Départemental et Métropolitain d'Incendie et de Secours. Bien que le SDMIS soit une entité autonome, le Conseil départemental lui apporte un soutien financier. Les dépenses comprennent notamment l'organisation de la lutte contre l'incendie et celle des secours en cas de catastrophe.

La Région
Auvergne-Rhône-Alpes

BOOSTEZ VOTRE ENTREPRISE GRÂCE AU NUMÉRIQUE

ET PRÉPAREZ
VOTRE PROJET SUR LE SITE
MA SOLUTION NUMÉRIQUE

MA SOLUTION NUMÉRIQUE

ma-solution-numerique.fr

Accédez à des outils personnalisés, des aides et des formations adaptées à vos besoins.

En ce moment, retrouvez notre focus **Cybersécurité** :
ma-solution-numerique.fr/cybersecurite-ma-petite-entreprise-est-aussi-concernee

CAMPUS RÉGION DU NUMÉRIQUE

17 formations innovantes

Près de 40 formations labellisées hors-les-murs

3 acteurs du numérique

Votre passeport pour les métiers de demain !

Depuis septembre 2017, le Campus Région du numérique accueille près de 900 apprenants sur 3500 m² au cœur du quartier de la Confluence à Lyon 2e.

Former, transformer, innover : le Campus Région est un écosystème unique qui réunit tous les acteurs du numérique pour répondre aux besoins de transformation des entreprises et des industries sur tout le territoire d'Auvergne-Rhône-Alpes.

Toutes les infos sur
www.campus-region.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES USAGES PRO-PERSO Mémo

ADOPTER LES **BONNES PRATIQUES**

10 CONSEILS POUR SÉCURISER VOS USAGES PRO ET PERSO

1. Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez
2. Ne mélangez pas votre messagerie professionnelle et personnelle
3. Ayez une utilisation raisonnable d'Internet au travail
4. Maîtrisez vos propos sur les réseaux sociaux
5. N'utilisez pas de service de stockage en ligne personnel à des fins professionnelles
6. Faites les mises à jour de sécurité de vos équipements
7. Utilisez une solution de sécurité contre les virus et autres attaques
8. N'installez des applications que depuis les sites ou magasins officiels
9. Méfiez-vous des supports USB
10. Évitez les réseaux Wi-Fi publics ou inconnus

POUR EN SAVOIR PLUS OU VOUS FAIRE ASSISTER, RENDEZ-VOUS SUR:
www.cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES MOTS DE PASSE Mémo

ADOPTER LES **BONNES PRATIQUES**

10 CONSEILS POUR GÉRER VOS MOTS DE PASSE

1. Utilisez un mot de passe différent pour chaque service
2. Utilisez un mot de passe suffisamment long et complexe
3. Utilisez un mot de passe impossible à deviner
4. Utilisez un gestionnaire de mots de passe
5. Changez votre mot de passe au moindre soupçon
6. Ne communiquez jamais votre mot de passe à un tiers
7. N'utilisez pas vos mots de passe sur un ordinateur partagé
8. Activez la double authentification lorsque c'est possible
9. Changez les mots de passe par défaut des différents services auxquels vous accédez
10. Choisissez un mot de passe particulièrement robuste pour votre messagerie

POUR EN SAVOIR PLUS OU VOUS FAIRE ASSISTER, RENDEZ-VOUS SUR:
www.cybermalveillance.gouv.fr

La stratégie de Microsoft est d'assurer la sécurité de nos clients pour permettre leur transformation numérique grâce à une plateforme complète, des renseignements uniques sur les menaces et de larges partenariats.

Au-delà d'une protection périmétrique devenue obsolète, il faut présupposer qu'il y aura compromission et être en mesure de détecter les attaques et y remédier avant que celles-ci n'impactent sévèrement vos données et vos systèmes. C'est la raison pour laquelle, l'approche traditionnelle de protection du Système d'Information doit être complétée et s'appuyer, comme nous le préconisons, sur trois piliers : la Protection, de tous les points terminaux jusqu'aux centres de données ; la Détection, en utilisant des signaux ciblés, l'analyse comportementale et l'apprentissage statistique ; la Réponse, pour passer rapidement de la découverte à l'action.

La complexité est l'ennemi absolu de la sécurité : Microsoft intègre nativement dans l'ensemble de ses services des fonctionnalités de sécurité avancées qui protègent de bout en bout les identités, la messagerie, les appareils, les infrastructures et les données, le tout sans compromettre l'expérience utilisateur pour éviter toute stratégie de contournement de vos politiques de sécurité. Ce positionnement unique vous permet de faciliter la gestion, l'administration et la supervision de la sécurité de votre SI tout en renforçant votre posture de sécurité. Ainsi, en février 2019, Microsoft a annoncé le lancement d'Azure Sentinel, une solution de SIEM/SOAR nativement conçue dans et pour le cloud. Cette solution vient compléter les capacités de détection et réponse automatisée de la plateforme de sécurité intégrée de Microsoft.

Ainsi, la protection de nos plateformes prend en compte la protection et la gestion des identités avec comme point central le référentiel Azure Active Directory ; la protection de l'information qui s'appuie sur Azure Information Protection pour classifier et protéger les données les plus sensibles et assurer le partage sécurisé à l'intérieur et à l'extérieur de l'entreprise ainsi que sur notre solution de CASB Microsoft Cloud App Security pour encadrer le shadow IT ; et enfin la protection contre les menaces avancées grâce à la puissance du Cloud et de l'intelligence Artificielle aussi bien sur les environnements collaboratifs Office 365, les appareils et serveurs que les identités. Enfin, nos solutions d'accès conditionnel vous assurent une tranquillité d'esprit en bloquant l'accès à l'information confidentielle en dernier ressort, lorsqu'une identité ou un appareil sont compromis.

Nourris par nos 250 services cloud, le Microsoft Intelligent Security Graph consolide et analyse des signaux en provenance de plus d'un milliard de systèmes Windows, de 450 milliards d'authentifications mensuelles sur nos services Cloud, aux plus de 18 milliards de page Web qui sont parcourues en permanence par Bing et aux 200 milliards de mails que nous filtrons contre le Spam chaque mois. Cette intelligence est présente dans toutes nos solutions de sécurité grâce à des algorithmes de Machine Learning et d'analyse des anomalies ou des comportements basés sur la puissance du cloud Microsoft et permet d'appliquer des mesures préventives ou des mesures d'atténuation en quasi temps réel pour contrer les cyber menaces.

Tous les services Microsoft sont fondés sur des principes forts en matière de vie privée, de sécurité, de conformité et de transparence. Microsoft est le chef de file de l'industrie en matière de vie privée et de sécurité et c'est à ce titre que nous avons fondé l'Intelligent Security Association en 2017 qui réunit les pionniers de l'industrie de la cybersécurité.

Enfin, parce que la sécurité des objets connectés est l'un des grands défis à venir, Microsoft innove avec Azure Sphere, une solution 3-en-1 qui sécurise l'IoT du matériel jusqu'au cloud en passant par un système d'exploitation sécurisé dédié.

Retrouvez plus d'informations relatives à la sécurité & à la conformité sur https://aka.ms/MicrosoftSecurity2019

AIRBUS CYBERSECURITY : UN FOURNISSEUR SPECIALISÉ DANS LA PROTECTION DES INFRASTRUCTURES CRITIQUES, DES GOUVERNEMENTS, DES ARMÉES ET DES OPÉRATEURS D'IMPORTANCE VITALE

- Nous sommes la filiale **cybersécurité du groupe Airbus.**
- Nous sommes à 100% **une filiale de la division Defence and Space**.
- Nous développons et fournissons des produits fiables et des services de haute qualité pour **protéger, détecter et répondre** 24h/24 à des cyberattaques de plus en plus sophistiquées.
- Nous sommes le seul fournisseur de cybersécurité avec une **présence souveraine en France, en Allemagne et au Royaume-Uni.**

NOTRE MISSION

Identifier **Protéger** **Détecter** **Répondre**

4 SOC (SECURITY OPERATIONS CENTRE)

22 PROJETS DE RECHERCHE INNOVANTS

850 PROFESSIONNELS CYBER EN EUROPE ET AU PROCHE-ORIENT

30% CROISSANCE DU CHIFFRE D'AFFAIRES EN 2018

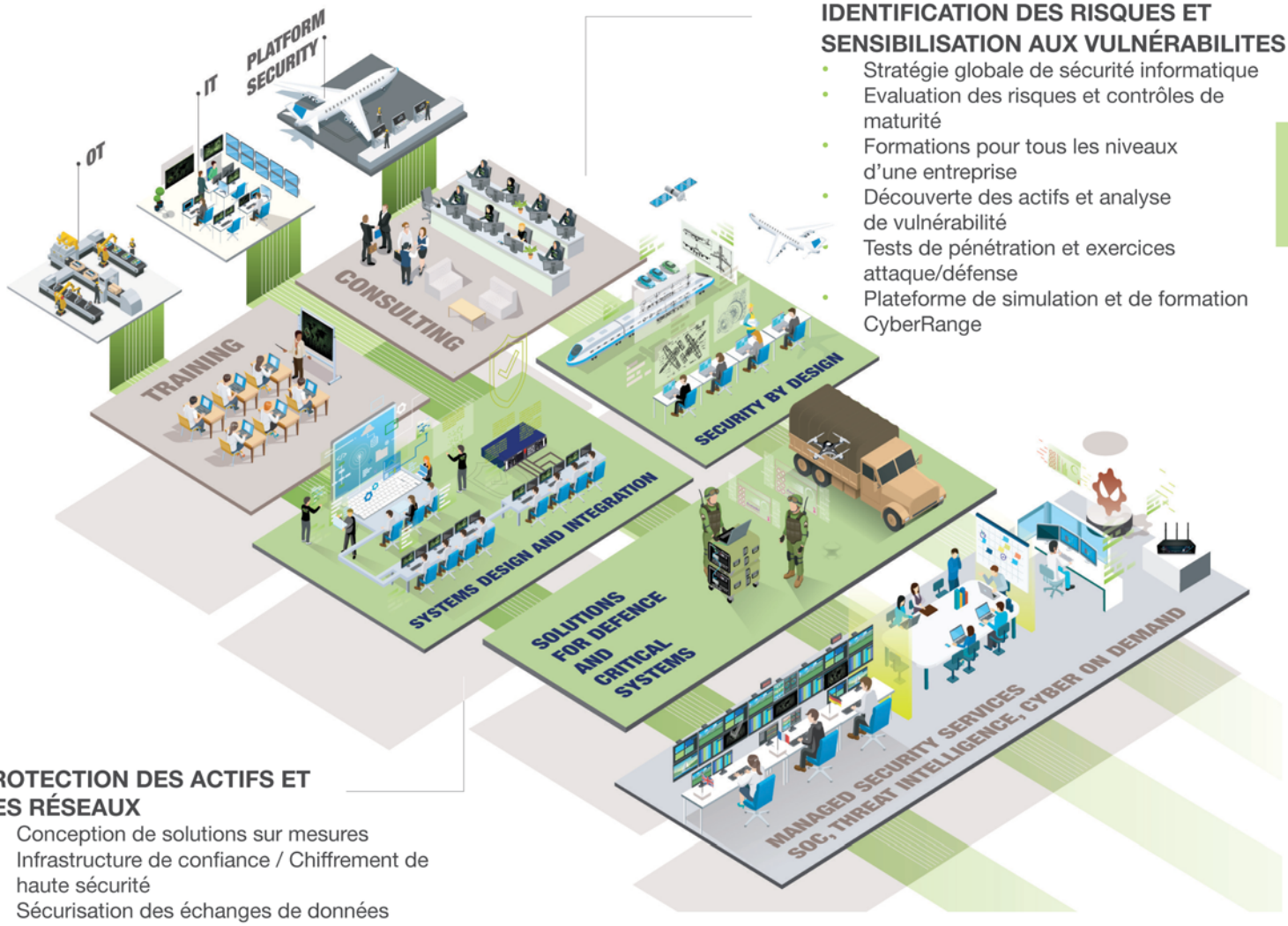
POURQUOI LES INVESTISSEMENTS DANS LA CYBERSÉCURITÉ SONT-ILS ESSENTIELS ?

« Pour tous nos clients, faire confiance à leurs systèmes informatiques IT et OT est vital pour leur transformation numérique et l'atteinte de leurs objectifs. La résilience devient à la fois un avantage concurrentiel et un produit en soi sur un marché où la moitié des organisations travaillent déjà avec plusieurs prestataires extérieurs en cybersécurité.

Grâce à notre ADN industriel combiné à des décennies d'expérience avec les systèmes de défense, chez Airbus CyberSecurity, nous avons une profonde compréhension des défis auxquels sont confrontés nos clients tels que la gestion des infrastructures complexes et des données sensibles. Nous les aidons à évaluer, créer, exploiter et maintenir des solutions de protection adaptées à leur environnement et leurs priorités. »

Markus Braendle, directeur d'Airbus CyberSecurity

NOTRE PORTEFEUILLE POUR CONSTRUIRE LA CYBERRESILIENCE DE DEMAIN



IDENTIFICATION DES RISQUES ET SENSIBILISATION AUX VULNÉRABILITES

- Stratégie globale de sécurité informatique
- Evaluation des risques et contrôles de maturité
- Formations pour tous les niveaux d'une entreprise
- Découverte des actifs et analyse de vulnérabilité
- Tests de pénétration et exercices attaque/défense
- Plateforme de simulation et de formation CyberRange

PROTECTION DES ACTIFS ET DES RÉSEAUX

- Conception de solutions sur mesures
- Infrastructure de confiance / Chiffrement de haute sécurité
- Sécurisation des échanges de données
- Sécurité réseau (pare-feux, VPN), sécurité des données et endpoint security

STORMSHIELD

DETECTION DES MENACES ET RÉPONSE AUX INCIDENTS

- Security Operations Centre (SOC) pour l'IT et l'OT
- Equipe spéciale d'intervention d'urgence (Computer Security Incident Response Team : CSIRT)
- Cyber Threat Intelligence
- Détection des intrusions avec la plateforme Orion Malware

En quelques mots

Un leader européen de la cybersécurité protégeant les institutions européennes

Un intégrateur de bout en bout de la cybersécurité industrielle IT et OT

Un partenaire de confiance pour Airbus, les gouvernements, les armées et les opérateurs d'importance vitale (OIV)

Une expérience unique dans la sécurité des plateformes et des systèmes embarqués

VISA DE SÉCURITÉ PASSI — ANSSI — CYBER ESSENTIALS PLUS — CERTIFIED ISO 9001:2015 COMPANY — Information Security Management ISO 27001 Certified

AIRBUS

FRANCE
Metapole 1, boulevard Jean Moulin / CS 40001 / 78996 Elancourt Cedex/ France

ALLEMAGNE
Willy-Messerschmitt-Str. 1 / 82024 Taufkirchen / Allemagne

ROYAUME-UNI
Quadrant House / Celtic Springs / Coedkernew / South Wales NP10 8FZ / Royaume-Uni

EMIRATS ARABES UNIS
Etihad Towers T3 / Corniche Road, 19th floor / P.O.Box: 72186 / Abu Dhabi / Emirats Arabes Unis

contact.cybersecurity@airbus.com
www.airbus-cyber-security.com


STORMSHIELD
Leader européen de la cybersécurité
Partenaire de confiance
pour
accompagner votre
transformation
numérique
IT
OT
www.stormshield.com

L'ESSENTIEL

DIAGNOSTIC NUMÉRIQUE DES TERRITOIRES

SERVICES NUMÉRIQUES

OÙ EN SONT LES COLLECTIVITÉS LOCALES ?

Le numérique est omniprésent dans la sphère privée. Il bouleverse les modes de travail, d'échange, de consommation. Il modifie aussi les attentes des citoyens à l'égard des services proposés dans la sphère publique. Ainsi, 70 % des Français jugent prioritaire le développement de l'e-administration et 88 % se disent prêts à utiliser ses services en ligne[1]. En parallèle, les collectivités locales doivent se conformer à des obligations légales et réglementaires pour simplifier les démarches des usagers. Ce nouveau cadre crée l'opportunité de répondre aux aspirations des citoyens en faveur du développement des services numériques des administrations : un enjeu de taille pour elles. La Poste, entreprise publique et tiers de confiance, qui conduit sa propre transition numérique, a procédé à un diagnostic approfondi des services numériques proposés aux citoyens par les collectivités locales. Son ambition ? Partager avec les communes et les intercommunalités l'état des lieux de cette transformation et les accompagner dans une nouvelle relation à l'usager, numérique et humaine, c'est-à-dire omnicanale.

1. Baromètre Digital Gouv' 2017 d'Ipsos pour Sopra-Steria. 2. Pour l'essentiel, ces obligations s'appliquent aux administrations publiques – et donc aux collectivités locales – en vertu du Code des relations entre le public et l'administration (CRPA). 3. Le décret n°2018-689 du 1er août 2018 détermine le calendrier d'équipement des collectivités en module.

L'ESSENTIEL EN 3 POINTS

Les défis à relever par les collectivités :

- **s'approprier** un environnement numérique en transformation ;
- **gérer** ses impacts sur l'organisation des services ;
- **transformer** le service rendu au citoyen.

Simplification des démarches

LES NOUVELLES OBLIGATIONS[2]

- Considérer la saisine électronique (SVE) comme ayant la même valeur que la saisine papier.
- Transmettre des accusés d'enregistrement et de réception de la demande, et prendre en compte le délai de réponse imparti, faute de quoi le silence pourrait valoir accord implicite (SVA).
- Simplifier le parcours de l'usager et garantir la transparence des voies de saisine utiles pour les citoyens.
- Fournir un module de paiement en ligne pour permettre et faciliter la souscription de services payants par Internet[3].

LE GROUPE LA POSTE

NUMÉRIQUE

LA RELATION AUX CITOYENS SE TRANSFORME

La mutation numérique des collectivités locales est bel et bien engagée. Toutefois, les défis qu'elles ont encore à relever sont nombreux. Le diagnostic numérique des territoires réalisé par La Poste met en lumière ces enjeux, auxquels s'ajoute celui de l'inclusion numérique des citoyens.

Méthodologie et échantillon

L'étude réalisée par Le Groupe La Poste* repose sur des données collectées de mai à octobre 2018.

9 340 communes ont été auditées en métropole et en outre-mer, soit 26 % des communes. Sur le total des communes étudiées, 438 intercommunalités sont représentées, soit 35 % des EPCI.

Population totale des communes étudiées 19 millions, soit 29 % de la population française.

30,5 % Pour chaque strate de communes, un échantillon représentatif a été audité, soit un taux de représentativité moyen de chaque échantillon de 30,5 %.

Le diagnostic numérique des communes et des EPCI en chiffres

42 % des communes ne sont toujours pas équipées d'un site Internet.

Une commune de moins de **2 000 habitants** sur deux ne dispose toujours pas d'un site Internet.

À titre de comparaison, **plus de 9 EPCI sur 10** donnent accès à un site Internet.

Le site Internet est la première brique pour proposer des services en ligne. Ainsi, pour près d'une commune de 2 000 habitants sur deux, la saisine par voie électronique n'est toujours pas mise en œuvre. De leur côté, les intercommunalités sont très largement équipées de ce premier niveau de services.

Plus de 3 communes sur 10 sont en situation de risque juridique en raison de l'hébergement de leur site Internet.

Les données et les documents des collectivités publiques répondent au régime des Archives publiques. Elles sont donc soumises à un cadre juridique contraignant qui impose une maîtrise de leur conservation, de leur intégrité et de leur traçabilité.
Avez-vous pensé au RGPD[5]? Pour s'y conformer, l'une des pistes est d'adopter la méthode du *privacy by design*. Cela consiste à mettre en place, dès leur conception, des systèmes de traitement des données adaptés aux exigences de protection des données personnelles des utilisateurs.

Près d'un site Internet de commune sur deux n'est pas adapté à un support mobile (smartphone ou tablette).

L'accessibilité mobile des sites Internet des communes doit être renforcée. On estime que 42 % des Français se connectent le plus souvent à Internet via leur smartphone, contre 38 % via leur ordinateur[4].

Seulement 5 % des communes sont équipées d'un module de paiement en ligne.

Les collectivités devront pourtant proposer un service de paiement en ligne au plus tard le 1er juillet 2022.

13 MILLIONS
DE FRANÇAIS
n'utilisent pas ou peu Internet et se sentent en difficulté avec ses usages. Ainsi, la formation des citoyens est une priorité.

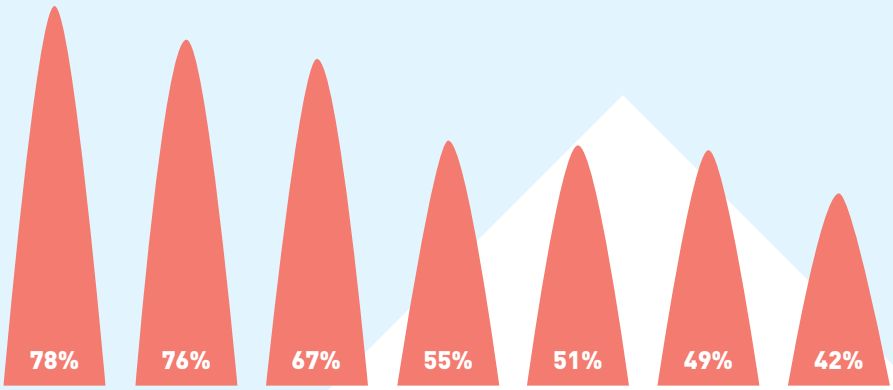
Un univers de services sécurisés et accessibles en omnicanal

La Poste accompagne les collectivités
afin qu'elles se dotent d'une plate-forme de services permettant aux citoyens de réaliser leurs démarches via n'importe quel canal (Internet, guichet, livraison à domicile). L'interface digitale est accessible par le biais d'un identifiant unique (agréé France Connect) et peut être associée à un coffre-fort électronique garantissant la sécurité, la conservation et la traçabilité des données.

Télé-services et principales thématiques

Seules 29 % des communes sont équipées de télé-services. Parmi les communes auditées et équipées d'un site internet, 59 % donnent accès à des démarches d'état civil, 6 % à un télé-service de signalement, 97 % ne donnent pas accès à un compte citoyen. Sur les 3 % de communes disposant d'un compte citoyen, 18 % permettent une identification via France Connect.

Principales thématiques des sites internet des communes *



*Audit numérique des collectivités locales, 2018, Groupe La Poste.

Une plate-forme de services mutualisable au niveau intercommunal

La mutualisation de la plate-forme omnicanale
de services au niveau intercommunal permet de faire bénéficier toutes les communes, y compris les plus petites, d'un même niveau de services aux citoyens. Grâce à la mutualisation, les coûts d'utilisation de la plate-forme sont en outre répartis entre les communes adhérentes.

Glossaire

L'identité numérique
pour se connecter à son compte citoyen et à tous les services en ligne, locaux et nationaux (CAF, Pôle emploi, impôts, Ameli, etc.). L'identité numérique est intégrée à France Connect, l'agrégateur d'identifiants mis en place par l'État pour faciliter et sécuriser les démarches en ligne.

Le compte citoyen
pour accéder aux services en ligne de ma commune dans la même interface, sans avoir à fournir des informations déjà détenues par l'administration.

Un coffre-fort électronique
pour stocker et gérer ses documents personnels et réaliser ses démarches administratives en toute sécurité.

L'omnicanal,
c'est mettre à disposition des citoyens tous les canaux d'accès disponibles (physique, numérique, humain) pour solliciter l'administration ou accéder aux services publics.

POUR TÉLÉCHARGER L'ÉTUDE COMPLÈTE, RENDEZ-VOUS SUR
GROUPELAPOSTE.COM

[4] Baromètre 2017 Arcep, Agence du numérique, CGE. [5] RGPD (règlement général sur la protection des données), entré en vigueur le 25 mai 2018. [6] Chiffres issus des travaux menés dans le cadre de l'élaboration du rapport de la Stratégie nationale pour un numérique inclusif (SNNI), auxquels La Poste a participé. [7] Étude CSA pour Les Petits Frères des pauvres, juin 2018. [8] Latribune.fr du 31 octobre, « Pour améliorer l'inclusion numérique, repenser les médiations sociales » (interview de Jacques-François Marchandise).

REGARDS CROISÉS

Les communes et les intercommunalités doivent opérer leur transformation numérique tout en accompagnant agents et citoyens, dans l'appropriation des usages et les potentialités des outils numériques. Rencontres avec des acteurs engagés.

ÉMILIE AGNOUX /
Directrice de l'innovation, du dialogue social et de l'animation managériale du Grand Paris Sud Est Avenir (GPSEA).

« ACCOMPAGNER LES AGENTS ET LES CITOYENS »

« Certains agents sont déjà très à l'aise avec les outils numériques, d'autres en sont beaucoup plus éloignés. D'autres encore, qui les mobilisent quotidiennement dans leur vie personnelle, restent arrimés à des usages datés dans le cadre professionnel. On peut donc commencer par s'appuyer sur les *early adopters* pour convaincre et accompagner leurs collègues. C'est tout le sens du réseau d'ambassadeurs du numérique que nous avons mis en place à GPSEA, pour sensibiliser et accompagner les agents dans l'appropriation des outils numériques. Cet accompagnement doit être quasi individualisé en fonction des besoins et des usages de chacun. Il en est de même pour les citoyens. Parce que l'obsolescence programmée des compétences sera accélérée, l'accompagnement au numérique est un élément fondamental du développement de la numérisation des services publics. »

PHILIPPE BUISSON /
Maire de Libourne (33).

« LA TRANSFORMATION NUMÉRIQUE EST EN ROUTE »

« La ville de Libourne est depuis de nombreuses années inscrite dans un processus de modernisation de son administration (e-administration, SIG, progiciels finances, RH, état civil, élections, site Internet, réseaux sociaux…). Elle compte poursuivre sur cette voie et a entrepris en 2018 l'écriture d'une feuille de route de sa transformation numérique. Première réalisation concrète à venir : la mise en ligne sur les "stores" d'une application mobile citoyenne dont l'objectif est, au-delà des fonctionnalités classiques, d'aller plus loin en matière d'e-administration et de gestion de la relation au citoyen (GRC). Une collectivité qui n'opèrerait pas sa transformation numérique risquerait, à terme, de ne plus être en mesure de remplir ses obligations de services publics et ne plus répondre aux attentes des habitants qui sont de plus en plus connectés. »

LAURENT BAUDRY /
DGS de Mulsanne (72).

« LE NUMÉRIQUE AU CŒUR DE LA MUTUALISATION »

« Dans leur très grande majorité, les communes, faute de moyens humains et financiers, ne peuvent déployer seules des outils numériques de gestion de la relation aux citoyens. L'intercommunalité, qui est désormais ancrée dans nos territoires et dans les habitudes des usagers, peut favoriser cette démarche et piloter des plate-formes de services. Il faut privilégier les passerelles entre les services publics communaux et communautaires pour simplifier les démarches de nos habitants. Il ne faut pas se limiter aux services des collectivités territoriales, mais intégrer aussi à ces plate-formes des interconnexions avec les autres services publics, ceux de la CAF notamment. Ainsi impulsée par l'intercommunalité, l'innovation numérique permettra de répondre aux attentes des élus communaux, qui souhaitent maintenir et améliorer le lien entre les services publics et les citoyens sur leur territoire. »

CONTACT

En savoir plus : téléchargez l'étude complète sur **groupelaposte.com**
Sollicitez un audit personnalisé de votre situation en écrivant à : **audit.numerique@laposte.fr**

Crédits photos : La Poste, , DR, iStock. Conception et réalisation : ici Barbès 146, rue du Faubourg-Poissonnière, 75010 Paris. Novembre 2018

Groupama
RHÔNE-ALPES AUVERGNE

CYBER Assurances

avec **Cyber UP**

GROUPAMA EST LE SEUL ASSUREUR À PROPOSER, EN INCLUSION DANS SES CONTRATS PROFESSIONNELS, DES GARANTIES DE GESTION DE CRISE, DE RESPONSABILITÉ CIVILE ET DE DOMMAGES AUX BIENS EN CAS D'ACTE DE MALVEILLANCE.

ELYSIUM
SECURITY

LA SÉCURITÉ INFORMATIQUE + UNE AFFAIRE D'EXPERTS

EXPERTISE
INNOVATION
EXPÉRIENCE
INDÉPENDANCE

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES APPAREILS MOBILES Mémo

ADOPTER LES **BONNES PRATIQUES**

10 CONSEILS POUR SÉCURISER VOTRE APPAREIL MOBILE

1. Mettez en place les codes d'accès
2. Chiffrez les données de l'appareil
3. Appliquez les mises à jour de sécurité
4. Faites des sauvegardes
5. Utilisez une solution de sécurité contre les virus et autres attaques
6. N'installez des applications que depuis les sites ou magasins officiels
7. Contrôlez les autorisations de vos applications
8. Ne laissez pas votre appareil sans surveillance
9. Évitez les réseaux Wi-Fi publics ou inconnus
10. Ne stockez pas d'informations confidentielles sans protection

POUR EN SAVOIR PLUS OU VOUS FAIRE ASSISTER, RENDEZ-VOUS SUR:
www.cybermalveillance.gouv.fr

L'HAMEÇONNAGE

CYBERCRIMINEL

VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (*phishing* en anglais) !

BUT

Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

TECHNIQUE

Leurre envoyé *via* un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce…

VICTIME

COMMENT RÉAGIR ?

- Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique
- Au moindre doute, contactez directement l'organisme concerné pour confirmer
- Faites opposition immédiatement (en cas d'arnaque bancaire)
- Changez vos mots de passe divulgués/compromis
- Déposez plainte
- Signalez-le sur les sites spécialisés (voir liens utiles)

Pour en savoir plus ou vous faire assister, rendez-vous sur cybermalveillance.gouv.fr

LIENS UTILES

- Signal-spam.fr
- Phishing-initiative.fr
- Info Escroqueries
  0 805 805 817 (gratuit)

Schneider Electric

Life Is On Schneider Electric

Conseil, Expertise et Solutions en cybersécurité industrielle

vous aider à optimiser votre rentabilité tout en protégeant vos systèmes des cyber attaques

Data centers

Industrie

Bâtiments

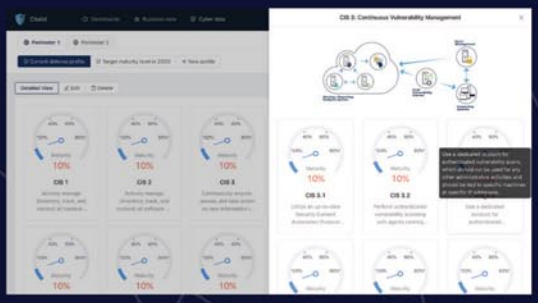
Infrastructures

Citalid

Cyber risk intelligence platform

Advanced cyber risk management turning
cyber intelligence into business value

Quantified profiles, enriched related context and recommended courses of action are strikingly offered through powerful analytics, advanced dashboards and displayed charts

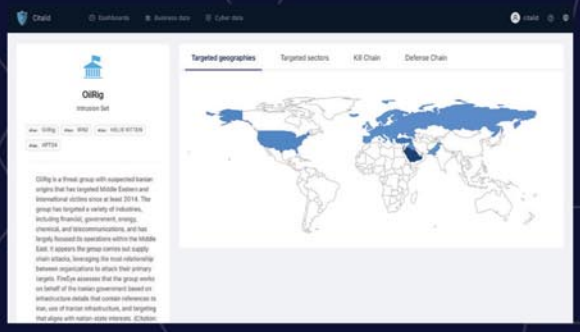


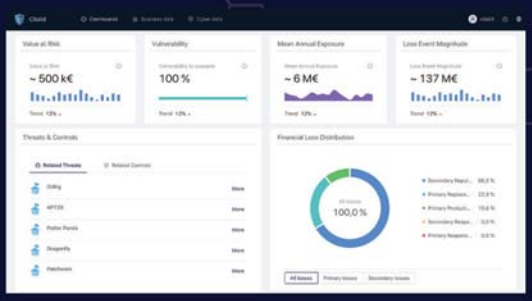
Cyber risk cartography

- CIS 20 defensive level assessment
- Pre-built library of operational risk scenarios applied
- Risk exposure and degree of vulnerability per scenario
- Aggregated view of most impacting threats aiming at your perimeter
- Simulation of recommended defense profile to reach
- Top-down view and simulation of suggested defensive measures

Threats knowledge hub

- Updated threats' characteristics and description
- Cyber kill chains breakdown
- Cyber defense chain computations
- Checklist appropriate countermeasures (threats & scenario)
- Shortlist of targeted locations areas, sectors of interest
- Review and historic database of past successful attacks





Risk exposure quantification

- Quantified value at risk and loss event magnitude
- Query and simulate "what if" defensive simulations to your organization
- Advanced risk aggregation, automatic course of action and investment recommendations
- Holistic and comparative oversight across activities and assets

Citalid background & expertise

Maxime Cartan
CEO

Alexandre Dieulangard
COO

Citalid's founders are renowned experts in risk assessment and threat intelligence. Before founding Citalid, they worked at the ANSSI (French National Agency for Cyber Security), reporting to the highest government authorities to inquire and undermine advanced threats. Built on this top notch and distinctive experience, Citalid's founders have pledged to upgrade the standards of risk management security and go one step further by redefining risk management and making it actionable once and for all.

Acknowledged & endorsed by strategic partners

Cyber awards

Assises de Monaco
Prix innovation & public

FIC 2019
Finaliste Prix Start'up

Research partners

Center for Internet Security
CIS20

Open Group
FAIR Certified

Ecole Polytechnique
PSC 2018

Investors

Citalid has raised €1,2 million seed round
June 2019

Strategic partners speak highly of us

« Citalid's sectoral and geographical approach makes it possible for the first time to connect Cyber Threat Intelligence to risk analysis. The synergy of the Citalid tool with ordinary methodologies and the flexibility of simulations help to guide and supervise defensive measures, and arbitrate budgets in line with the Business Units' financial exposure to cyber risks. »

Gilles Berthelot , CISO SNCF Group

La grande consultation des entrepreneurs

Perception et prise en compte du risque cyber
par les dirigeants d'entreprises
octobre 2019

Sondage “opinionway

pour

CCI FRANCE

LA TRIBUNE LCI

en partenariat avec

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

ESOMAR member

La méthodologie

	Étude réalisée auprès d'un échantillon de **613 dirigeants d'entreprise.** La représentativité de l'échantillon a été assurée par un redressement selon le secteur d'activité et la taille, après stratification par région d'implantation.
	L'échantillon a été interrogé **par téléphone.**
	Les interviews ont été réalisées **du mercredi 11 au mercredi 18 septembre 2019.**
	OpinionWay a réalisé cette enquête en appliquant les procédures et règles de la norme ISO 20252

Les risques de cybersécurité inquiètent peu les dirigeants

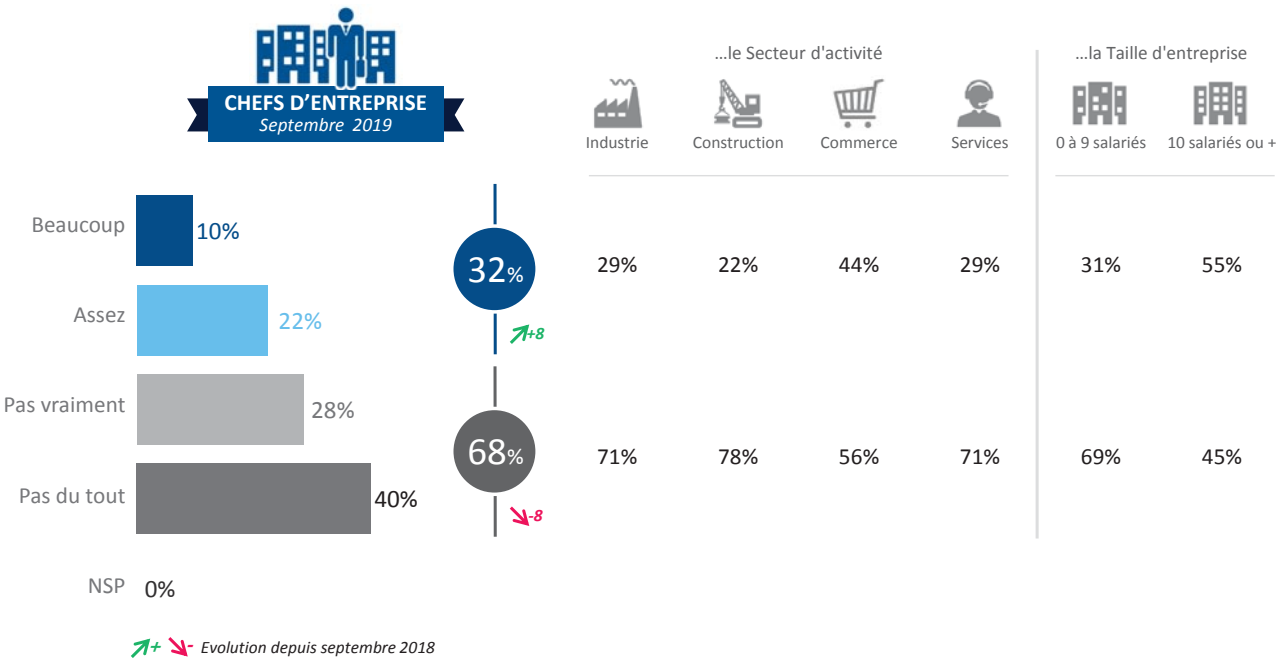
- **Globalement, les risques de cybersécurité préoccupent toujours peu les dirigeants d'entreprises malgré une hausse de 8 points par rapport à septembre 2018 (32% sont *assez* ou *beaucoup* préoccupés**, contre 68% qui ne sont *pas vraiment* ou *pas du tout* préoccupés). Seulement 10% des dirigeants déclarent que ces risques les préoccupent *beaucoup*, tandis que la plupart indiquent qu'ils ne les inquiètent *pas du tout* (40%). **Dans le détail, le risque d'un infection par un virus est celui que le plus de dirigeants craignent (31%)**, suivi par le vol de données sur un serveur (23%). Alors que les arnaques basées sur des système d'imitation de voix se développent, l'usurpation d'identité ou la fraude est également un risque craint par 23% des dirigeants. **47% des dirigeants ne craignent aucun des risques cités.**
  - Les dirigeants d'entreprises comptant 10 salariés ou plus sont davantage attentifs aux risques liés à la cybersécurité : 55% d'entre eux déclarent que ceux-ci les préoccupent (contre 31% des chefs d'entreprises comptant moins de 10 salariés). Le secteur du commerce est le plus sensible à ces enjeux, 44% des dirigeants d'entreprise concernés déclarent être préoccupés soit nettement plus que ceux de l'industrie ou des services (respectivement 29%) et deux fois plus que dans le secteur de la construction (22%),

- **Ne considérant pas vraiment leur entreprise comme une cible potentielle de cyberattaques, 67% des dirigeants déclarent n'avoir déployé aucune action de cybersécurité sur les 12 derniers mois.** Les seules actions menées par une partie des dirigeants sont le déploiement de nouveaux systèmes de pares-feux ou logiciels de sécurité (16%) ou le renforcement des systèmes de sécurité (14%). **S'ils considèrent peu les risques de cybersécurité auxquels leur entreprise peut faire face, les dirigeants demeurent lucides sur leur méconnaissance en la matière.** Les dirigeants donnent ainsi une note moyenne de 4,7 sur 10 à la maturité de leur entreprise en termes de cybersécurité, 62% d'entre eux donnant une note de 5 ou moins,
  - L'inaction des dirigeants en termes de cybersécurité vaut avant tout pour les entreprises comptant moins de 10 salariés (69% n'ont pris aucune mesure au cours des 12 derniers mois), 64% des dirigeants ayant au moins 10 salariés ou plus ayant pris des mesures sur cette période (contre 36% n'ayant rien entrepris).

Les préoccupations concernant les risques liés à la cyber sécurité

Q : Diriez-vous que les risques liés à la cyber sécurité (vol de données, e-réputation, perte d'information, etc.) de votre entreprise vous préoccupent… ?

– BASE : 613 CHEFS D'ENTREPRISE

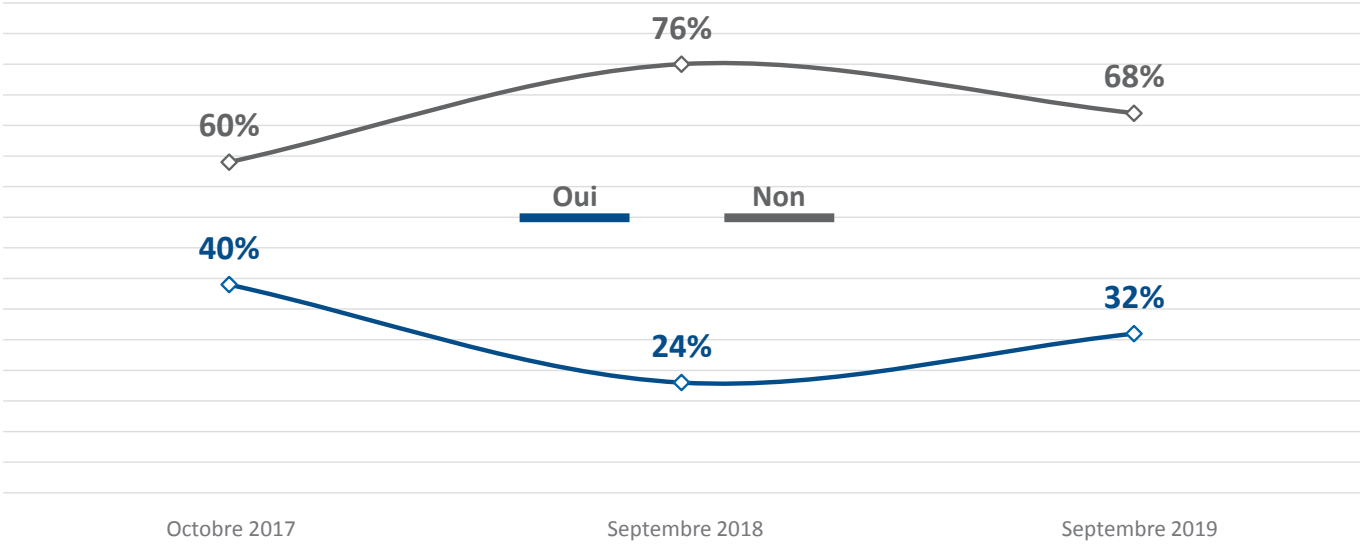


Les préoccupations concernant les risques liés à la cybersécurité

Q : Diriez-vous que les risques liés à la cyber sécurité (vol de données, e-réputation, perte d'information, etc.) de votre entreprise vous préoccupent… ?

– BASE : 613 CHEFS D'ENTREPRISE

CHEFS D'ENTREPRISE
Septembre 2019



Les risques de cyber sécurité les plus craints

Q : Parmi les risques de cyber sécurité suivants, quels sont ceux que vous craignez le plus ? *(Plusieurs réponses possibles)*

– BASE : 613 CHEFS D'ENTREPRISE

CHEFS D'ENTREPRISE
Septembre 2019

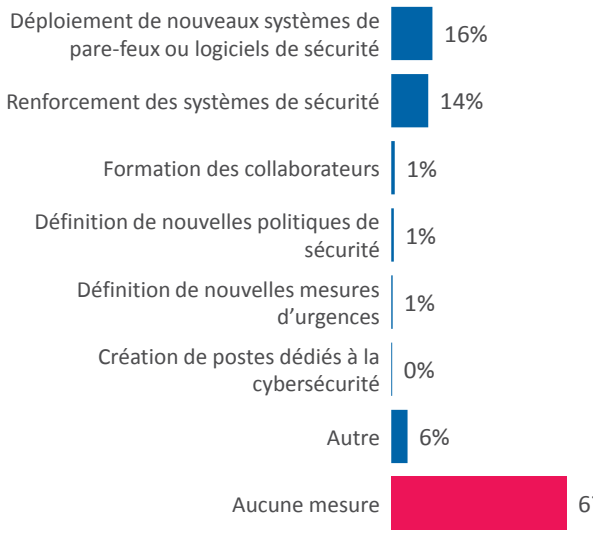
		…le Secteur d'activité				…la Taille d'entreprise	
		Industrie	Construction	Commerce	Services	0 à 9 salariés	10 salariés ou +
Un virus qui infecte vos ordinateurs	31%	35%	40%	43%	24%	31%	45%
Le vol de données présentes sur vos serveurs	23%	19%	19%	27%	23%	22%	50%
Une usurpation d'identité ou une fraude	23%	22%	21%	33%	19%	22%	30%
Le phishing (technique consistant à récupérer des informations confidentielles en se faisant passer pour une grande entreprise ou un organisme familier)	6%	8%	2%	6%	6%	6%	11%
Un logiciel de rançon (logiciel qui verrouille les données des utilisateurs qui ne peuvent être récupérées qu'en payant une rançon)	6%	12%	3%	7%	5%	5%	15%
Une atteinte à la e-réputation de votre entreprise	5%	7%	5%	5%	4%	4%	14%
Une perte d'information suite à la négligence des collaborateurs	4%	8%	4%	2%	5%	4%	20%
Une mauvaise gestion des données personnelles (clients, usagers, collaborateurs)	2%	9%	-	2%	2%	2%	8%
Aucun de ces risques	47%	45%	42%	34%	54%	49%	15%

Les actions déployées en matière de cybersécurité

Q : Dans les 12 derniers mois, quelles sont les actions que vous avez déployées en matière de cybersécurité au sein de votre entreprise ?

– BASE : 613 CHEFS D'ENTREPRISE

CHEFS D'ENTREPRISE
Septembre 2019



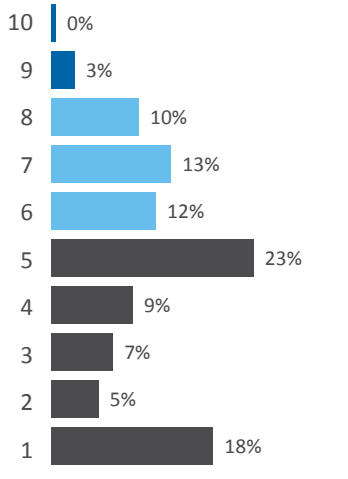
	...le Secteur d'activité				...la Taille d'entreprise	
	Industrie	Construction	Commerce	Services	0 à 9 salariés	10 salariés ou +
Déploiement de nouveaux systèmes de pare-feux ou logiciels de sécurité	24%	21%	14%	15%	15%	24%
Renforcement des systèmes de sécurité	15%	7%	22%	12%	13%	35%
Formation des collaborateurs	3%	1%	1%	2%	1%	15%
Définition de nouvelles politiques de sécurité	2%	2%	-	1%	-	11%
Définition de nouvelles mesures d'urgences	5%	-	-	-	-	6%
Création de postes dédiés à la cybersécurité	1%	-	-	1%	-	8%
Autre	1%	3%	5%	8%	6%	9%
Aucune mesure	67%	73%	62%	68%	69%	36%

Le niveau de maturité de son entreprise en matière de cybersécurité

Q : Sur une échelle de 1 à 10, où situeriez-vous le niveau de maturité de votre entreprise en matière de cybersécurité ?*1 signifiant que vous n'avez aucune connaissance, 10 une parfaite connaissance, les notes intermédiaires servant à nuancer votre réponse.*

– BASE : 613 CHEFS D'ENTREPRISE

CHEFS D'ENTREPRISE
Septembre 2019



		...le Secteur d'activité				...la Taille d'entreprise	
		Industrie	Construction	Commerce	Services	0 à 9 salariés	10 salariés ou +
10	0%						
9	3%	3%	2%	2%	4%	4%	3%
8	10%						
7	13%	44%	33%	44%	30%	33%	71%
6	12%						
5	23%						
4	9%						
3	7%	53%	65%	54%	66%	63%	26%
2	5%						
1	18%						
Moyenne	4,7/10	5,0	5,1	5,3	4,3	4,6	6,4

Vade Secure
Predictive Email Defense

Attaque de PHISHING : Même pas peur !

Vade Secure O365

Protection renforcée de la messagerie Office 365

Prévention Phishing

Détection en temps réel des URLs et sites malveillants pour les SOC

www.isitphishing.ai

digital.security | econocom

La révolution digitale s'accélère. Les usages permis par les nouvelles technologies, ouvertes et ultra connectées, amplifient les enjeux liés à la cybersécurité et en élargissent le spectre.

Nous sommes confrontés à un immense challenge : tirer profit de cette révolution tout en maîtrisant les risques induits par la transformation des processus, des services et des produits.

Pour aider à relever ce défi, **digital.security** s'est doté d'expertises rares et additionnelles ainsi que d'une capacité d'innovation et d'expérimentation au service des entreprises et administrations pour, tant sur les systèmes informatiques de gestion que sur les systèmes informatiques industriels :

- Garantir un niveau de sécurité constant et optimum des données numériques sensibles
- Contrer rapidement les menaces émergentes
- Intégrer les bonnes pratiques de la sécurité au quotidien
- Maîtriser et réduire les risques des projets numériques

Nos Expertises

SÉCURITÉ DES **SYSTÈMES D'INFORMATION**

Des compétences et un savoir-faire pour :

- Faire converger les impératifs des métiers et le besoin de sécurité
- Faciliter l'adhésion aux politiques de sécurité par les collaborateurs et les responsabiliser
- Appréhender le renforcement des lois, règlements et directives en matière de cybersécurité
- Réussir l'intégration de la sécurité dans les projets de transformation digitale

SÉCURITÉ DE L'**INTERNET DES OBJETS** (IOT)

Une passion et un investissement permanent pour apporter de la valeur ajoutée aux entreprises qui utilisent les solutions connectées :

- Intégrer l'IoT en toute sécurité dans le système d'information
- Adapter les politiques de sécurité existantes à l'IoT
- Limiter les risques liés aux usages des objets connectés
- Piloter en continu le niveau de sécurité des objets connectés

Et aux entreprises qui les créent :

- Tester et évaluer la sécurité des produits grâce à notre laboratoire dédié
- Bénéficier de conseils et préconisations pour valoriser les créations
- Accélérer leur insertion sur le marché en communiquant sur la sécurité des produits

Nos prestations

AUDIT

- Audit : architecture, conformité, code, processus, PASSI…
- Tests d'intrusion
- Exercices en mode « Red Team »
- Scans de vulnérabilités
- Gestion des programmes de « Bug Bounty »
- Inventaire des points de présence Internet
- Appréciation du niveau de maturité
- Evaluation des politiques et de la gouvernance
- Préparation aux certifications

FORMATIONS

- Sensibilisation à la sécurité des collaborateurs et des dirigeants
- Développement Web sécurisé
- « Ethical Hacking »
- Intégration de la sécurité dans les projets
- Sécurité des réseaux sans fil IoT
- Sécurité matériel de l'IoT
- Analyse de risques et conformité IoT

CERT

- Réponse sur incidents et enquêtes
- Interventions inforensiques
- Veille en vulnérabilités
- Etudes et veilles sur mesure
- Surveillance des menaces
- Contrôle permanent de la sécurité
- Détection des menaces radio-fréquences
- Evaluation de sécurité IoT
- Veille sur la sécurité de l'IoT
- Labellisation de la sécurité IoT

INTÉGRATION ET PROJET

- Authentification renforcée, solutions SSO
- Gestion des identités et des habilitations (IAM)
- Gestion de clés et signatures électroniques
- Contrôle d'accès au SI, gestion des privilèges
- Lutte contre la fuite de données (DLP)
- Collecte et analyse centralisée des fichiers journaux
- Solutions de contrôle de conformité

CONSEIL

- Stratégie, schéma directeur
- Evaluation et plan de traitement des risques
- Etudes prospectives et de cadrage
- Définition et mise en place de systèmes de management
- Intégration de la sécurité dans les projets
- Tests et recette des solutions de sécurité
- Organisation et mise en place des SOC et des solutions SIEM

SÉCURITÉ OPÉRATIONNELLE

- Mise à disposition d'expertise sécurité dans le cadre des projets
- Opération de centres de services sécurité (SOC, CERT, NOC...)
- Animation des dispositifs de contrôle et de reporting sécurité
- Organisation et mise en place des SOC et des solutions SIEM
- Maîtrise et gestion de la sécurité des actifs
- Détection des menaces
- Application et maintien des règles définies

Le LAB

digital.security a créé le CERT, premier CERT™ spécialisé sur l'écosystème des objets connectés.
Notre laboratoire R&D est un sanctuaire technologique dans lequel nous menons nos investigations numériques et tous types d'analyses logiques et physiques sur les objets connectés et les infrastructures associées. Ce laboratoire nous permet de délivrer un label sécurité qui garantit auprès des utilisateurs et donneurs d'ordre un niveau de sécurité conforme aux exigences fixées.

Analyse et recherche sur les protocoles de radiofréquences et détection des équipements rayonnants

Attaques « physiques » et mise à l'épreuve des objets connectés

Inforensique pour identifier et sécuriser les preuves numériques

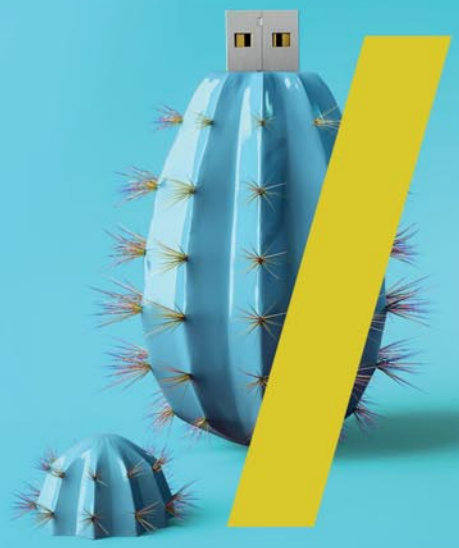
Contacts
Web : https://www.digital.security
Tél : +33 (0)1 70 83 85 85
Email : info@digital.security
FRANCE - BELGIQUE - LUXEMBOURG

Digital Security - Econocom
@iotcert

À propos
digital.security a été créé en 2015 par un groupe d'experts de la sécurité informatique et est un satellite du groupe Econocom.

implid

La sécurité, un vecteur de confiance



Chaque entreprise est différente en matière de sensibilisation aux enjeux, à l'exposition aux risques, à sa maturité en matière de protection. Chez implid, nous vous accompagnons dans la compréhension et la réduction globale de vos risques numériques.

Le **diagnostic** de votre **maturité sécurité** et **réglementaire** (SSI, RGPD, SAPIN) et la construction de feuille de route

La **sensibilisation** de vos utilisateurs aux **risques cyber** par la mise en situation, les exercices, le jeu

La **surveillance** de votre **e-réputation** ou de celle de votre écosystème sur le web, les forums, les blogs, les réseaux sociaux, le darknet

L'**accompagnement** par nos équipes mixtes de consultants et d'avocats sur votre mise en conformité (réglementaire, sectoriel)

Le **pilotage** de vos projets de cybersécurité et la **conduite du changement** auprès des utilisateurs (authentification forte, protection des données, sécurisation des échanges)

Envie d'en savoir plus ? ***Contactez jerome.masseau@implid.com***

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES MISES À JOUR Mémo

ADOPTER LES **BONNES PRATIQUES**

10 CONSEILS POUR GÉRER VOS MISES À JOUR

1. Pensez à mettre à jour sans tarder l'ensemble de vos appareils et logiciels
2. Téléchargez les mises à jour uniquement depuis les sites officiels
3. Identifiez l'ensemble des appareils et logiciels utilisés
4. Activez l'option de téléchargement et d'installation automatique des mises à jour
5. Pro — Définissez les règles de réalisation des mises à jour
6. Planifiez les mises à jour lors de périodes d'inactivité
7. Méfiez-vous des fausses mises à jour sur Internet
8. Pro — Informez-vous sur la publication régulière des mises à jour de l'éditeur
9. Pro — Testez les mises à jour lorsque cela est possible et faites des sauvegardes
10. Pro — Protégez autrement les appareils qui ne peuvent pas être mis à jour

POUR EN SAVOIR PLUS OU VOUS FAIRE ASSISTER, RENDEZ-VOUS SUR:
www.cybermalveillance.gouv.fr

LES RANÇONGICIELS

CYBERCRIMINEL

EXTORSION D'ARGENT

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (*ransomware*, en anglais) !

BUT

Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

TECHNIQUE

Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.

VICTIME

COMMENT RÉAGIR ?

- Débranchez la machine d'Internet et du réseau local
- En entreprise, alertez le support informatique
- Ne payez pas la rançon
- Déposez plainte
- Identifiez et corrigez l'origine de l'infection
- Essayez de désinfecter le système et de déchiffrer les fichiers
- Réinstallez le système et restaurez les données
- Faites-vous assister par des professionnels

Pour en savoir plus ou vous faire assister, rendez-vous sur cybermalveillance.gouv.fr

LIEN UTILE

www.nomoreransom.org/fr/index.4html

Grenoble INP ESISAR

esynov

TPE / PME, EMPAREZ-VOUS DES ENJEUX DE CYBERSÉCURITÉ

Formations à la carte
Conférences - Bonnes pratiques
Diagnostic de vulnérabilités
Tests intrusifs et «offensifs »

Sensibilisation
Fondamentaux
Niveau expert

Hacking &
sécurité

Sécuriser ses
infrastructures
Cloud

Systèmes
industriels

NumericLab est un plateau technique au sein de la plateforme Esynov dédié à la cybersecurité

ÉCOLE NATIONALE SUPÉRIEURE EN SYSTÈMES AVANCÉS ET RÉSEAUX

Contact : numericlab@esynov.fr | Site internet : www.esynov.fr

formind
CONSULTING

Cabinet de conseil en sécurité de l'information et gestion des risques

NOTRE POSITIONNEMENT

- Analyser
- Définir
- Choisir
- Mettre en oeuvre
- Détecter
- Réagir
- Sensibiliser
- Contrôler

VISA DE SÉCURITÉ — ANSSI

choose mycompany 2019 FRANCE 50-99 employees

Happy index / At Work

NOTRE SAVOIR-FAIRE

SECURITY FOR CISO
PSSI & Documentation
ISO 2700X
Coaching

RÉSILIENCE & CRISE
BIA
SMCA
Test et Exercice

GESTION DES RISQUES
Analyses de risques
ISP & Agilité
Dashboard & KRI

SURETÉ
Sécurité des sites
CCTV
Contrôles d'accès

CLOUD & INNOVATION SECURITY
Architecture & Expertise
Big data & IoT
Nouveaux usages

FORMATION
Inter et intra entreprises
Fonctionnel et technique
« tailor made »

PROTECTION DE L'INFORMATION
Classification
Protection – DRM
Détection DLP

SENSIBILISATION
Stratégie
Déploiement et outillage
Innovation et interactivité

CYBER SECOP
Assistance RSSI
SOC - SIEM
Réponse à incident

AUDITS
Tests d'intrusion
Audit d'architecture et de configuration
Audit organisationnel

SSI INDUSTRIELS
Schéma directeur
Analyse de risques & Architecture
SOC OT

CONFORMITÉ
RGPD
PCI-DSS
LPM, NIS, RGS, ACPR, ...

IDENTITÉS
IAM & IAG
PIAM
Authentification forte

NOUS TROUVER

France - Paris, Rennes, Lyon & Toulouse
Maroc - Casablanca

www.formind.fr

DIGITAL

La fondation ldigital, sous égide de la fondation pour l'université de lyon,
accompagne et sensibilise les femmes aux métiers
et aux débouchés du numérique en auvergne-rhône-alpes.

fondationldigital@gmail.com

NOS *AXES* D'INTER*V*ENTION

EDUQUER

MENER DES ACTIONS DE SENSIBILISATION AUPRÈS DES JEUNES, EN MILIEU SCOLAIRE OU NON, DE LA MATERNELLE À L'UNIVERSITÉ.

ACCOMPAGNER

ATTIRER LES FEMMES ACTIVES ET EN RECONVERSION PROFESSIONNELLE DANS LES MÉTIERS DU NUMÉRIQUE ET DÉVELOPPER LEURS COMPÉTENCES.

LA FONDATION EST COMPOSÉE DE MEMBRES BÉNÉVOLES, FEMMES, HOMMES, ÉCOLES, ÉTABLISSEMENTS DE FORMATION, ENTREPRISES, FÉDÉRÉS ET ACTIFS, POUR FAIRE PROGRESSER LE POURCENTAGE DE FEMMES DANS LE NUMÉRIQUE, SECTEUR EN FORT DÉVELOPPEMENT AU NIVEAU MONDIAL.

*A*GISSONS ENSEMBLE !

LDIGITAL.ORG

FONDATION LDIGITAL

@4LDIGITAL

LDIGITAL


TROUVEZ LE JOB
QUI VOUS CORRESPOND
DANS LA CYBERSÉCURITÉ
cyberjobs.fr
#jobboard
#média
CYBERJOBS

INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

Mastère spécialisé Cybersecurité du Numérique . Formation de haut niveau sur un an pour devenir Expert technico-managérial en cybersécurité

EN BREF

- 7ème promotion en cours
- 90% d'intervenants professionnels
- Préparation CISSP
- Certifications Stormshield (network securitt administrator) et iso27001 (Lead implementer et lead auditor)
- Label SECNUMEDU de l'ANSSI
- Classé second en France par EDUNIVERSAL
- Accredité conférence des grandes écoles

VOS OBJECTIFS

- Vous souhaitez acquérir de solides connaissances et compétences en sécurité de l'information
- Vous aspirez à dynamiser votre carrière en vous positionnant sur un marché porteur
- Vous désirez vous investir dans les métiers de l'audit, analyses des risques, du conseil et ingénierie en sécurité informatique

NOS POINTS FORTS

- L'INSA DE LYON est une école reconnue pour son expertise en ingénierie. Régulièrement classée première des écoles françaises en 5 ans et dans le top 5 des meilleures écoles d'ingénieurs
- 6 mois de formation théorique par un corps professoral professionnel et une mission professionnelle de 6 mois dans des grands groupes et des PME
- Un réseau de partenaires entreprises diversifié : Utilisateurs, constructeurs, opérateurs, Sociétés de service

QUELS METIERS ?

- Chef de projet , Intégration de solutions de sécurité
- Audit technique et organisationnel d'infrastructures de sécurité
- Responsable de la sécurité des systèmes d'information
- Développeur code sécurisé
- Architecte/Administrateur d'infrastructures de sécurité
- Analyste SOC, Conseil

POURQUOI CHOISIR UN M.S ?

- Une formation Post-diplôme de haut niveau
- L'avantage d'une double compétence technique et managériale en sécurité de l(information
- L'accès a des postes diversifiés dans tous les secteurs d'activité
- Des enseignements concrets et opérationnels

EN SAVOIR PLUS ?

Site web : https://www.insa-lyon.fr/fr/mastere-cybersecurite-numerique

Contact : omar.gaouar@insa-lyon.fr

CYBERCERCLE FORMATION : UN CADRE DE CONFIANCE POUR FORMER À LA SÉCURITÉ NUMÉRIQUE

Dans le prolongement de l'action qu'il mène depuis 2011 pour rendre plus appréhendables la sécurité numérique, ses enjeux, son cadre institutionnel et réglementaire, et ainsi participer à la diffusion d'**une culture de sécurité numérique**, le CyberCercle a créé des **modules de formation** qui permettent d'approfondir ces champs dans un cadre privilégié.

CyberCercleFormation aborde les sujets de cybersécurité dans toutes leurs dimensions et en particulier **stratégiques, juridiques et réglementaires, de gouvernance et organisationnels.**

CyberCercleFormation s'adresse à trois types de publics :

- les **dirigeants de PME-PMI et les cadres dirigeants non spécialistes de la cybersécurité** – directions générales, directions marketing, digital, conformité, service juridique ou ressources humaines – qui souhaitent mieux maîtriser cette nouvelle dimension indispensable aujourd'hui dans leur champ de compétences ;
- les **RSSI** et **DSI** qui désirent mieux maîtriser les **enjeux juridiques et réglementaires** liés à leurs champ d'action et responsabilités ;
- les **élus et cadres territoriaux** qui sont aujourd'hui confrontés à la transformation numérique des territoires et des usages, et qui doivent mieux appréhender la sécurité numérique pour assurer un développement pérenne de leurs actions, notamment pour garantir **la confiance dans les services numériques qu'ils mettent en œuvre au service des citoyens.**

Les modules de formation ont volontairement des **formats courts**, d'une ou de deux journées, afin d'éviter de peser trop lourdement sur les agendas.

CyberCercleFormation propose quatre modules de formations :

- **La cybersécurité au cœur de la transformation numérique des entreprises** pour les Top managers de PME/ETI, professions libérales et activités de conseil
- **La cybersécurité au cœur de la transformation numérique des collectivités** pour les élus, directions des services généraux, directions métiers
- **La cybersécurité des systèmes industriels** pour les Top managers de PME/ETI, directions générales de service de collectivités, directions métiers, acheteurs et juristes
- **Réglementation, juridique et cybersécurité** pour les risques managers, directions de la conformité, Top managers, directions des services généraux

Les formateurs de CyberCercleFormation sont tous des **professionnels** spécialistes de la cybersécurité et dotés de qualités de pédagogue qui leur permettent de transmettre leurs savoirs de façon efficiente, en adéquation avec leur auditoire. Des **représentants des institutions publiques** viennent apporter un éclairage sur des sujets définis, permettant aux participants un accès à une expertise institutionnelle et un échange personnalisé avec les représentants de l'État en charge de ces questions.

En parallèle des **sessions inter-entreprises** qui seront mises en place à partir de janvier 2019 à Paris et en région, notamment en Auvergne-Rhône-Alpes, le CyberCercle peut **définir et mettre en œuvre des formations et séminaires au sein de votre organisation**, en les adaptant aux besoins et aux profils de vos collaborateurs.

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES SAUVEGARDES

Mémo

ADOPTER LES **BONNES PRATIQUES**

10 CONSEILS POUR ÉVITER DE PERDRE VOS DONNÉES

1. Effectuez des sauvegardes régulières de vos données
2. Identifiez les appareils et supports qui contiennent des données
3. Déterminez quelles données doivent être sauvegardées
4. Choisissez une solution de sauvegarde adaptée à vos besoins
5. Planifiez vos sauvegardes
6. Déconnectez votre support de sauvegarde après utilisation
7. Protégez vos sauvegardes (perte, vol, casse...)
8. Testez vos sauvegardes
9. Vérifiez le support de sauvegarde
10 Pro. Sauvegardez les logiciels indispensables à l'exploitation de vos données

POUR EN SAVOIR PLUS OU VOUS FAIRE ASSISTER, RENDEZ-VOUS SUR:
www.cybermalveillance.gouv.fr

LES FAUX SUPPORTS TECHNIQUES

CYBERCRIMINEL

ESCROQUERIE FINANCIÈRE

Votre ordinateur est bloqué et on vous demande de rappeler un support technique ? Vous êtes victime d'une arnaque au faux support !

BUT

Inciter la victime à payer un pseudo-dépannage informatique et/ou la faire souscrire à des abonnements payants.

TECHNIQUE

Faire croire à un problème technique grave impliquant un risque de perte de données ou d'usage de l'équipement (par écran bloqué, téléphone, SMS, courriel etc.).

VICTIME

COMMENT RÉAGIR ?

- Ne répondez pas
- Conservez toutes les preuves
- Redémarrez votre appareil
- Purgez le cache, supprimez les cookies et réinitialisez les paramètres de votre navigateur
- Désinstallez tout nouveau programme suspect
- Faites une analyse antivirus
- Changez tous vos mots de passe
- Faites opposition auprès de votre banque si vous avez payé
- Déposez plainte

Pour en savoir plus ou vous faire assister, rendez-vous sur cybermalveillance.gouv.fr

LIENS UTILES

- Internet-signalement.gouv.fr
- Info Escroqueries
  0 805 805 817 (gratuit)

MERCI À NOS PARTENAIRES

CYBER CERCLE

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