



CYBER
CERCLE

22 OCTOBRE 2020
en distanciel
RENCONTRES
CYBERSÉCURITÉ
AUVERGNE-RHÔNE-ALPES

#RCYBERARA
#TDFCYBER2020

La Région
Auvergne-Rhône-Alpes







TOUR DE FRANCE DE LA CYBERSÉCURITÉ 2020

#TDFCyber2020

ESPACES DÉMOS
TABLES RONDES
FORMATION
NETWORKING
RECRUTEMENT
ATELIERS



@CyberCercle
@CyberTerritoire



**DOSSIER
PARTICIPANT**

RCYBERARA

en distanciel

22 OCTOBRE 2020

Edito



Juliette JARRY

**Vice-présidente déléguée aux infrastructures, à l'économie et aux usages numériques
Région Auvergne-Rhône-Alpes**

Bienvenue à la 2^{ème} édition des rencontres Cybersécurité Auvergne-Rhône-Alpes !

La crise sanitaire que nous vivons montre à quel point le numérique est un enjeu stratégique et un facteur de résilience notamment dans le secteur économique, sanitaire et éducatif. Il a démontré toute son importance dans la gestion de la crise et face à sa diversification et à l'intensification de ses usages, il doit s'accompagner d'une vraie stratégie de transformation numérique de confiance.

C'est dans ce cadre-là que de nombreuses actions sont menées en matière de cybersécurité pour permettre de couvrir les différents besoins des TPE/PME de la région, de la sensibilisation du dirigeant et de ses équipes à la mise en œuvre d'un plan d'actions interne à l'entreprise.

Le Campus Région du Numérique, dont l'ambition s'articule autour de trois grands axes : la formation, l'accompagnement à la transformation des entreprises et l'innovation propose des formations en lien direct avec la thématique cybersécurité. Sa plateforme phytale présente un MOOC de l'ANSSI sur « se former à la cybersécurité » et un dossier « focus » qui sensibilise les petites entreprises sur l'importance de la Cybersécurité.

Le dispositif Ambition Région accompagne également les entreprises de la région Auvergne-Rhône-Alpes, à travers différents parcours, dans la mise en place d'une culture et d'un savoir-faire lié à la cybersécurité. De nombreux partenaires engagés de la Région s'inscrivent dans cette démarche de démocratisation de la cybersécurité auprès de leurs réseaux avec des ateliers, des séminaires, des formations en ligne et des événements autour de cette thématique.

N'hésitez pas à vous consulter l'agenda de ces manifestations sur le site du Campus Région du Numérique :
<https://campusnumerique.auvergnhonealpes.fr/>

RCYBERARA

RCYBERARA

en distanciel

22 OCTOBRE 2020



Crédit photo Alain Zimeray

Bénédicte PILLIET
Présidente du CyberCercle

Edito

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

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

Avec la crise sanitaire, le Tour de France de la Cybersécurité s'est bien évidemment réinventé en maintenant deux objectifs majeurs : permettre dans le contexte actuel d'avoir accès à une parole de confiance sur la sécurité numérique et favoriser les échanges constructifs pour avancer ensemble vers des territoires numériques de confiance, alors même que le recours au numérique est devenu essentiel dans la crise que nous traversons.

La transformation numérique qui impactait déjà l'ensemble des acteurs, publics et privés, quelle que soit leur taille, que ce soit au niveau national, international et bien évidemment territorial, s'est en effet accélérée sous l'effet de la crise actuelle, l'urgence favorisant souvent la mise de côté de la dimension sécurité au profit de l'efficacité et de la continuité d'activité.

Force est de constater, une fois de plus, que le travail à accomplir pour que nos territoires deviennent des territoires numériques de confiance, favorisant le développement économique, la sécurité et des usages sécurisés au service de ses habitants, ses entreprises, ses collectivités, est encore immense. Nous en sommes seulement au début mais nous devons avancer vite, et ensemble.

En effet, si tout le monde (ou presque), entend le message sur le risque cyber, la sécurité numérique reste cependant 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 territoire dans lequel nous sommes s'est résolument engagé dans la construction de territoires numériques de confiance, sous l'impulsion de la Région Auvergne-Rhône-Alpes, en particulier avec le Campus Région du Numérique. Nous sommes heureux au CyberCercle de contribuer à cette dynamique.

Je remercie très sincèrement la vice-présidente de la Région en charge du Numérique, Juliette JARRY, de son soutien à notre action ici, en Auvergne-Rhône-Alpes.

Je tiens également à remercier nos partenaires, qui pour certains nous suivent sur l'ensemble du TDFCyber depuis sa création comme le Groupe La Poste, Cybermalveillance.gouv.fr et CERTitude NUMERIQUE, des entreprises comme FORMIND et SIEMENS qui s'y investissent davantage cette année. Je remercie enfin nos soutiens, ministères, écoles, associations, qui s'associent à cet événement dans cet esprit fédérateur qui est le nôtre.

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

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

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

8h30 ■>> OUVERTURE DE LA JOURNÉE

- ▶ Mot de bienvenue par **Bénédicte PILLIET**, présidente, CyberCercle
- ▶ Ouverture par **Juliette JARRY**, vice-présidente déléguée au numérique, Région Auvergne-Rhône-Alpes

9h00 ■>> TABLE RONDE

Quelles actions et quelle stratégie de développement pour des territoires numériques de confiance ?

Juliette JARRY, vice-présidente déléguée au numérique, Région Auvergne-Rhône-Alpes

Communauté d'agglomération de l'ouest rhodanien

Bénédicte PILLIET, présidente, CyberCercle

Michel CADIC, délégué adjoint, Délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité, ministère de l'Intérieur (DPSIS)

Lieutenant-colonel Yoni FOREST, chef du bureau sécurité publique, sécurité des mobilités, Région de Gendarmerie Auvergne Rhône-Alpes

Stéphane MEYNET, président, CERTitude NUMERIQUE

10h15 ■>> KEYNOTES

- ▶ **la lutte contre la cybercriminalité : état de la menace et réponses de la Gendarmerie**

Capitaine Dorian DIDIER et **Capitaine Paul-Alexandre GILLOT**, Pôle Judiciaire de la Gendarmerie Nationale

- ▶ **la sécurité numérique à l'heure du COVID-19 : retour sur l'action de [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) et recommandations**

Franck GICQUEL, responsable des partenariats, cybermalveillance.gouv.fr

- ▶ **sensibilisation : jouer pour apprendre**

Grégory DEMULE, directeur commercial associé, et **Florian PINARD**, consultant cybersécurité, FORMIND

- ▶ **l'identité numérique**

Dr Michel DUBOIS, chef du bureau Expertise, direction de la cybersécurité, Groupe La Poste

13h00 ■>> FIN DE LA MATINÉE

14h30 ■>> ATELIERS

Les ateliers durent deux heures et ont pour objectif de permettre aux participants d'échanger, de façon très pratique et opérationnelle, dans un cadre de confiance - ils sont placés sous les règles de Chatham House. Des orateurs ouvrent l'atelier par des exposés d'une douzaine de minutes chacun pour poser le cadre puis l'ensemble des participants est invité à s'exprimer, soit pour poser des questions, soit pour apporter un témoignage, un retex ou une vision du sujet. A l'issue, des points forts de ces échanges sont présentés via un compte rendu sur le site en quelques points afin de permettre à l'ensemble des participants de bénéficier de ce travail.

► De la smart city aux **territoires intelligents** : quels enjeux de sécurité numérique pour le **développement des collectivités** (dématérialisation, réglementation, e-citoyen, identité numérique, mobilité...) ?

Bénédicte PILLIET, présidente, CyberCercle

Colonel Mathieu DEMESY, conseiller pour les affaires métropolitaines du général commandant la région de gendarmerie Auvergne Rhône-Alpes et la gendarmerie pour la zone de défense et de sécurité sud-est, Gendarmerie Nationale

Philippe SCOFFONI, membre, PLOSS-RA

Stéphane MEYNET, président, CERTitude NUMERIQUE

► De la sécurisation des infrastructures à l'industrie 4.0, comment insérer de la cybersécurité dans les **sites industriels** ?

Philippe GENOUX, délégué général, Association des EXploitants d'Equipements de mesure, de Régulation et d'Automatismes (EXERA)

Valérie LANCELOT, chargée de mission industrie du futur, Campus Région du Numérique, Région Auvergne-Rhône-Alpes

Alix MADET, déléguée régionale Auvergne-Rhône-Alpes à l'information stratégique et à la sécurité économiques, SISSE

Daniel LAZZARONI, chef de branche Energies et Transports, Division Digitale Industrie, SIEMENS

► A l'heure de la e-santé et d'une numérisation accrue des infrastructures et des usages médicaux, quels retex numériques de la crise de la crise sanitaire, quel enjeux de sécurité numérique et quelles perspectives pour **les acteurs de la santé sur les territoires** ?

Cyrille ISAAC-SIBILLE, député du Rhône, rapporteur du rapport d'information parlementaire sur le dossier médical partagé et les données de santé

Philippe LOUDENOT, fonctionnaire de sécurité des systèmes d'information, ministères sociaux

Charles BLANC-ROLIN, RSSI et DPO, Groupement Hospitalier de Territoire 15, vice-président de l'APSSIS

► **Comment sensibiliser en interne ses collaborateurs aux bonnes pratiques de la sécurité numérique** ?

Atelier de cybermalveillance.gouv.fr animé par **Franck GICQUEL** avec un retex d'**Olivier RIBAUX**, Directeur de l'Ecole des Sciences Criminelles de Lausanne, Vice-doyen de la Faculté de droit, des sciences criminelles et d'administration publique

► **Quels enseignements tirer de la crise liée au covid 19** dans le champ du numérique pour les acteurs des territoires ? Echanges d'expérience, difficultés rencontrées, propositions de solutions (télétravail, gestion de crise, résilience, projets-coopérations à développer sur le territoire)

Dr Michel DUBOIS, chef du bureau Expertise, direction de la cybersécurité, Groupe La Poste

Laurane RAIMONDO, chercheure associée, Centre Lyonnais d'Etudes de Sécurité Internationale et de Défense, Université Lyon III

Eric POZZI, référent régional à l'IE, Région de Gendarmerie Auvergne-Rhône-Alpes

16h00

■>> **FIN DES ATELIERS et de la JOURNÉE**

Les intervenants

Juliette JARRY

**Vice-présidente déléguée aux infrastructures, à l'économie et aux usages numériques
Région Auvergne-Rhône-Alpes**



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. Vice-présidente du Conseil régional Auvergne Rhône-Alpes déléguée aux infrastructures, à l'économie et aux usages numériques, elle s'appuie sur son expérience du monde entrepreneurial pour porter l'ambitieux projet numérique de la Région. A travers la présentation d'une feuille de

route stratégique votée en février dernier en Assemblée plénière, Juliette Jarry a souhaité affirmer les priorités de la Région : accélérer le déploiement des infrastructures (très haut débit et téléphonie), créer un campus pour développer les compétences numériques par la formation initiale et continue, accompagner les entreprises dans leur transformation numérique, développer les usages. Juliette JARRY a entrepris de fédérer les acteurs du territoire pour valoriser son fort potentiel et faire d'Auvergne-Rhône-Alpes la « Silicon Valley » européenne.

Michel CADIC

**DPSIS adjoint
Ministère de l'Intérieur**



Michel Cadic est ingénieur en chef de l'armement. De spécialité ingénieur armement terrestre (Ensta Br), il bénéficie également d'une formation en économie (Doc) et en droit public (Lic). Il est ancien auditeur du CHEDE.

Ayant commencé sa carrière au ministère de la défense / Délégation Générale pour l'Armement en 1988 par les essais d'engins blindés, dont le char Leclerc, (DGA/Angers), il rejoignit la DGA /DRI en 1997 et fut en charge du soutien à l'exportation pour plusieurs pays du Moyen

Orient (DGA/DRI), puis d'activités transverses comme chef de cabinet (2002-2003). Il est ensuite nommé directeur de projet Portail de l'armement, intégrant la place de marchés dématérialisées pour l'ensemble des achats du ministère de la Défense. En 2005, il fut chargé de créer le service de l'attaché d'armement auprès de l'ambassade de France à Stockholm. De retour en France en 2008, il occupa plusieurs postes à caractère financier à la DGA (programme Rafale, démarche d'orientation de la DGA). De 2014 à 2018, il fut en charge d'activités de sécurité économique, de protection d'installations puis de prospective sécuritaire au profit de la sphère défense.

Yoni FOREST

**chef du bureau sécurité publique, sécurité des mobilités
Région de Gendarmerie Auvergne Rhône-Alpes**



Saint-Cyrien de formation, breveté de l'école de guerre, le lieutenant-colonel Yoni FOREST est chef du bureau sécurité publique, sécurité des mobilités de la région de gendarmerie Auvergne-Rhône-Alpes. Officier régional chargé de la sécurité économique, il coordonne l'action des différents intervenants gendarmerie qui y concourent, dans les dimensions prévention situationnelle, analyse, sécurité et cybersécurité des entreprises. Ayant commandé un escadron de gendarmerie mobile et une compagnie de

gendarmerie départementale, il a également servi auprès du Haut Fonctionnaire de Défense et de Sécurité du ministère de la transition écologique.

Bénédicte PILLIET

Présidente fondatrice du CyberCercle



Credit photo Alain

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. Avec deux objectifs majeurs : favoriser la diffusion d'une culture de sécurité numérique et agir au niveau des politiques publiques dans

ce champ, aux niveaux national et local.

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, intervient comme experte dans des formations d'entreprises et des colloques. Diplômée de Sciences Po Paris en 1990, Bénédicte Pilliet a acquis à travers son parcours professionnel une expertise reconnue dans la communication institutionnelle et les Affaires Publiques, sur les sujets de défense, de sécurité nationale et de sécurité numérique.

Elle a rejoint en 2007 la Réserve Citoyenne de l'armée de Terre, puis en 2012 la Réserve Citoyenne de Cyberdéfense où elle sera en charge du rayonnement jusqu'en 2018. Elle est titulaire de la Médaille de la Défense nationale, échelon or, agrafe cyber, et de la Médaille des Services Militaires Volontaires, échelon bronze. Bénédicte Pilliet est Vice-présidente de l'association Les Amis de la RCC, membre d'honneur du CEFYCS (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).

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.

Franck GICQUEL

**Responsable des partenariats
cybermalveillance.gouv.fr**



Franck Gicquel est Responsable des partenariats de Cybermalveillance.gouv.fr.

Il intègre l'équipe dès la phase de préfiguration du dispositif au sein de l'ANSSI en 2016.

Il officiait alors depuis plus de 10 ans dans l'écosystème de la sécurité et des systèmes d'informations. Il a notamment été Directeur Commercial chez DG Consultants, Groupe Comexposium, où il a contribué à développer leur événement phare, les Assises de la Sécurité à Monaco, et à fédérer la communauté des professionnels du secteur. Franck est également père de deux enfants.

Dr Michel DUBOIS

**Chef du Pôle Expertise, Direction de la cybersécurité
GROUPE LA POSTE**



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

Grégory DEMULE

**Directeur Associé
Formind**



Grégory DEMULE intervient depuis plus de 10 ans dans le secteur du conseil, d'abord dans le domaine des infrastructures et du digital où il occupe des fonctions de management commercial et de Business unit avant de plonger dans celui de la cybersécurité. Directeur Associé au sein de Formind, il rejoint ce pure player du conseil en cybersécurité et gestion des risques en 2015 en tant que directeur commercial et participe activement à son développement (160 personnes en 2020) à travers l'accompagnement de nombreux clients et le renforcement de l'offre du cabinet. En 2019, il conduit l'implantation à Lyon de Formind dont il assure également le développement au niveau régional et le pilotage des équipes opérationnelles.

Florian PINARD

**Consultant Senior en sécurité des SI et gestion des risques
Formind**



Après une partie de carrière au sein d'un acteur industriel où il participe fortement au développement de la filière cybersécurité, Florian PINARD rejoint Formind en 2020 en tant que consultant senior en sécurité des SI et gestion des risques. Son intérêt précoce pour la technologie et les données personnelles l'ont logiquement amené vers la protection des données et il allie depuis 8 ans son expertise SSI et sa culture industrielle dans des projets de mise en conformité, d'analyse de risque mais aussi de sensibilisation avec plusieurs interventions dans ce domaine. L'humain restant au cœur de ces problématiques, il accompagne également en mode coaching les professionnels de la SSI pour optimiser leurs influences dans le pilotage de la sécurité au sein de leurs organisations.

Mathieu DEMESY

**conseiller pour les affaires métropolitaines du général commandant la région de gendarmerie
Auvergne Rhône-Alpes et la gendarmerie pour la zone de défense et de sécurité sud-est
Gendarmerie Nationale**



Le colonel Mathieu DEMESY est conseiller pour les affaires métropolitaines du général commandant la région de gendarmerie Auvergne-Rhône-Alpes et la gendarmerie pour la zone de défense et de sécurité sud-est. À ce titre, il s'intéresse aux questions territoriales et participe au développement de la stratégie de sécurité de la gendarmerie sur les métropoles d'AURA, en particulier en matière de sécurité économique et de sécurité des mobilités. Breveté de l'école de guerre, sa carrière, à dominante opérationnelle, l'a conduit à la tête de 5 unités différentes, dans les domaines du maintien de l'ordre public, de la gestion de crise spécialisée, de la sécurité publique et de la police judiciaire, enrichie d'une expérience en administration centrale à dimension interservices.

Les intervenants

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-Président 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 décerner 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.

Valérie LANCELOT

Chargée de mission industrie du futur
Région Auvergne-Rhône-Alpes
Campus Région du numérique



Après 25 ans d'expérience à Mines Saint-Etienne, dans le développement de projets en France et à l'étranger alliant formation et transfert technologique, Valérie LANCELOT a rejoint l'équipe projet Campus Région du numérique en juin 2019, pour contribuer à l'installation du Campus à Charbonnières-les-Bains et au déploiement de l'offre de services de l'Usine. L'Usine est composée de 4 plateformes technologiques dédiées à la transformation digitale des process et processus industriels des TPE-PME/PMI régionales.

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, plaçant 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. Il s'intéresse particulièrement à l'analyse de la délinquance sérieuse par les traces et à ses développements numériques. Il a contribué, depuis son origine, au développement du dispositif opérationnel d'analyse des crimes répétitifs mis en œuvre par les polices romandes.

Daniel LAZZARONI

**Chef de Branches Energie et Transport
SIEMENS Digital Industrie France**



De formation INSA Lyon en Génie Electrique, après un début de carrière dans l'automatisme pour un groupe japonais, M. LAZZARONI débute chez Siemens en Application technique puis Ingénieur de vente, responsable commercial régional puis grand compte. Depuis 2007, il est Chef de Branches Energies et depuis 2013 a ajouté les activités du Transport et des Infrastructures.

Dans le domaine des Energies M. LAZZARONI a déployé divers solutions de contrôle commande en sûreté et sécurité pour tous types d'Energie de l'éolien, Hydraulique, Photovoltaïque, Stockage Hydrogène, Thermique et Nucléaire .

Charles BLANC-ROLIN

Administrateur systèmes et réseau



Charles BLANC-ROLIN est administrateur systèmes et réseaux de formation. Il a intégré la DSI du Centre Hospitalier de Saint-Flour en 2008. Au cours de ces douze années, il a pu participer à de nombreuses étapes de sa mutation numérique et continue d'y contribuer. Le système d'information de santé a très vite suscité chez lui un certain engouement. Passionné par nature, toujours en quête de renouveau, il s'est rapidement épanoui dans le rôle de référent des systèmes d'information de l'établissement, puis responsable sécurité des systèmes d'information pour le GHT Cantal. Il est également vice-président de l'APSSIS, chroniqueur pour DSIH magazine et fondateur du Forum SIH.

Philippe LOUDENOT

**FSSI
Ministères sociaux**



Après une carrière au sein du ministère de la défense à différents postes Philippe LOUDENOT devient responsable national de la sécurité des systèmes d'information du service de santé des armées. Puis FSSI adjoint dans le service du Haut fonctionnaire de défense et de sécurité pour les ministères chargés des affaires sociales, il rejoint les services du Premier ministre en 2011, où il participe à la création et met en place un service du haut fonctionnaire de défense et de sécurité. Il en est nommé fonctionnaire de sécurité des systèmes d'information et

conseille les autorités des services du Premier ministre, juridictions administratives indépendantes en matière de cybersécurité.

Il vient de rejoindre à nouveau le service du Haut fonctionnaire de défense et de sécurité des ministères chargés des affaires sociales comme FSSI.

Chargé de cours SSI au profit de différentes universités et écoles d'Ingénieurs, Philippe LOUDENOT est également présent dans la vie associative des experts en Sécurité du Système d'Information, il est membre du conseil d'administration de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information et du CESIN, membre du club EB IOS.

Cyrille ISAAC-SIBILLE

**Responsable des partenariats
cybermalveillance.gouv.fr**



Cyrille ISAAC-SIBILLE a été élu député du Rhône en 2017. Au sein de l'Assemblée Nationale, il est Secrétaire de la commission des Affaires sociales, Président du groupe d'études Prévention santé et rapporteur de la Branche Vieillesse du Projet de Loi sur le Financement de la Sécurité Sociale actuellement en examen à l'Assemblée. Il est membre du Haut conseil pour l'avenir de l'assurance maladie.

Médecin ORL à la clinique Charcot et au sein des Hôpitaux de Lyon, il a été adjoint au maire de Sainte-Foy-lès-Lyon

de 1995 à 2008, président-fondateur de l'Union départementales des CCAS du Rhône de 2002 à 2008.

Les intervenants

Laurane RAIMONDO

**Chercheuse associée (cyberdéfense, espace exo-atmosphérique & données personnelles)
Centre Lyonnais d'Etudes de Sécurité Internationale et de Défense**



En 2014 d'abord, puis en 2016, pendant ses études, Laurane RAIMONDO travaille pour la data unit du Conseil de l'Europe. En 2018, ses travaux mêlent la protection des données, le cyber et la question de la militarisation et l'arsenalisation de l'espace extra-atmosphérique. Ses recherches sur ce dernier sujet sont primées par le prix du Gouverneur militaire de Lyon. Exerçant dans le même temps comme data protection officer auprès d'un organisme traitant des données sensibles de personnes vulnérables, elle développe l'enseignement cyber dans le

Master Relations Internationales à la Faculté de Droit à l'Université Jean Moulin Lyon 3 et celui des données personnelles dans le parcours Expertise et Risques Internationaux. Auteure de l'ouvrage La protection des données personnelles en 100 questions-réponses à paraître chez Ellipses début 2021, elle écrit pour la série Stories of Conflict d'Arte, le magazine Sécurité & Défense et entend poursuivre l'écriture à destination du grand public ainsi que l'enseignement. Deux axes visant à rendre le cyber accessible à tous pour développer la confiance dans l'espace numérique.

Olivier RIBAUX

**Professeur et Directeur - Vice-doyen de la Faculté de droit, des sciences criminelles et d'administration publique
ESC | Ecole des Sciences Criminelles
Université de Lausanne**



Olivier RIBAUX est Directeur de l'École des Sciences Criminelles de l'Université de Lausanne et Vice-Doyen de la faculté de Droit, des Sciences Criminelles et d'Administration Publique. Diplômé en mathématiques, il a commencé sa carrière dans des sociétés de services en informatique (développement de logiciels). Son engagement au service informatique de la police cantonale genevoise a ensuite coïncidé avec l'apparition de l'analyse criminelle dans les pratiques policières et comme domaine académique. Ces évolutions l'ont amené

à réaliser une thèse de doctorat, puis à occuper simultanément, durant huit ans, un poste d'analyste criminel dans les polices romandes et de Professeur à l'Université de Lausanne.

Maréchal des Logis Chef 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**.



RENCONTRES
CYBERSÉCURITÉ
AUVERGNE-RHÔNE-ALPES

**MERCI
À NOS
PARTENAIRES
& SOUTIENS**



La Région

Auvergne-Rhône-Alpes

TPE/PME

SUIVEZ UN PARCOURS 360°
POUR PRÉPARER VOTRE
PROJET NUMÉRIQUE !

RENDEZ-VOUS SUR

campusnumerique.auvergnerhonealpes.fr

CAMPUS
RÉGION 
DU NUMÉRIQUE

Un portail web unique pour accéder à toute l'offre numérique délivrée par le Campus Région du numérique sur l'ensemble des territoires d'Auvergne-Rhône-Alpes : Formation, Transformation des entreprises, Innovation industrielle.

#Fichesoutils
#Vidéos
#Témoignages
#Diagnostics
#Accompagnements
#Financements



AVEC LE CAMPUS RÉGION DU NUMÉRIQUE :

accédez à toute l'offre de services numériques en Auvergne-Rhône-Alpes, en matière de formation, de transformation des organisations et d'innovation industrielle.

→ INSPIREZ-VOUS

D'entrepreneurs qui ont boosté leur activité grâce au numérique.

→ PRÉPAREZ-VOUS

Avec des études, des fiches-outils, des formations en ligne et en présentiel.

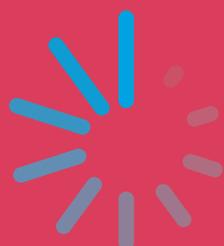
→ PASSEZ A L'ACTION

Grâce à des accompagnements et des financements et avec l'appui d'experts et de prestataires près de chez vous.



RETROUVEZ NOS DOSSIERS CYBERSÉCURITÉ SUR LE PORTAIL CAMPUS

Lutte contre les cyberattaques, sauvegarde des données, protection en situation de télétravail, RGPD... accédez à des conseils, outils et bonnes pratiques pour vous aider à sécuriser votre entreprise !



campusnumerique.auvergnerhonealpes.fr >> [Les services pour transformer mon organisation](#) >> [Sécurité](#)

PARTICULIERS, ENTREPRISES,
COLLECTIVITÉS TERRITORIALES:
VOUS ÊTES VICTIME D'ACTES
MALVEILLANTS SUR INTERNET?

PIRATAGE



ARNAQUE



CHANTAGE



VIRUS



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



MISSIONS

DU DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

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

MEMBRES

PREMIER MINISTRE
 MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA RELANCE
 MINISTÈRE DE L'INTÉRIEUR
 MINISTÈRE DE LA JUSTICE
 SECRÉTAIRE D'ÉTAT CHARGÉ DE LA TRANSITION NUMÉRIQUE
 ET DES COMMUNICATIONS ÉLECTRONIQUES



NOTRE MÉTIER



Formind est un cabinet de conseil en sécurité de l'information et gestion des risques.

Notre mission est simple et belle : protéger nos clients. Nous sommes des passionnés, animés par des valeurs de bienveillance, d'engagement, d'excellence, de partage et d'écoute.

NOS CHIFFRES CLÉS

2010

Création de
Formind Consulting

200

Clients de différents
secteurs d'activité

(Grands comptes,
startup et ETI)

150

Collaborateurs
(cible à 2025 :
500 collaborateurs)

NOS INTERLOCUTEURS



Security
Stream



CIO
& CTO



Continuity



DPO



Business
Owner



Regulator



Risk &
Compliance



NOS BUREAUX

Paris, Rennes, Nantes, Lyon, Toulouse et Casablanca



HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY





Prévenir

Gestion des risques
Sécurité des projets
Sensibilisation
& formation



Être conforme

Accompagnement
(RGPD, NIS, LPM,
ACPR/EBA...)

Audit
SMSI



Réagir

Continuité
Gestion de crise
Cyber-résilience

NOS OFFRES



Protéger

Sécurité Cloud

Gestion
des identités
et des accès

Sécurité OT



Détecter & Tester

Sécurité
opérationnelle

Audit technique
(pentest / redteam)

Audit sûreté



Intégrer

Expertise & pilotage
Intégration & recette

Maintien en
Condition Opérationnelle
/ Sécurité

Xavier Fauquet
Directeur Général

Hervé Morizot
Directeur Général

Grégory Demule
Directeur Commercial

Siège Social
43 rue Camille Desmoulins
92130 Issy-les-Moulineaux
contact@formind.fr

SIEMENS

*Ingenuity for life**

Société : Siemens SAS
 Adresse : 40, avenue des Fruitières -
 93210 Saint-Denis (France)
 Tel : +33 1 85 57 00 00
 Site Web :
<https://new.siemens.com/fr/fr/entreprise/thematiques/la-cybersecurite-chez-siemens.html>

Spécialisations :

Grâce à son approche holistique, Siemens est le partenaire de référence et de confiance pour répondre aux enjeux de la digitalisation et de la cybersécurité des systèmes industriels. En effet, Siemens est le premier équipementier – et le seul à ce jour – à avoir obtenu en France la qualification de l'ANSSI pour une gamme complète d'automate programmable (Simatic S7-1500) et la certification d'un commutateur industriel (Scalance XM400).

Par ailleurs, Siemens accompagne la sécurisation des installations au travers d'un large portfolio de services : cartographie, conseil (IEC 62443, analyse de risques, référentiels ANSSI...), durcissement des configurations, cloisonnement des réseaux, automates industriels sécurisés, switch industriels sécurisés, accompagnement à l'homologation et maintien en condition de sécurité.

Contact :
 Fabien Miquet
 PSSO Siemens Digital Industries France
fabien.miquet@siemens.com



« La certification TÜV SÜD IEC62443-4-1 de nos sites de développement associée à la certification ANSSI permet à Siemens d'atteindre le niveau le plus exigeant préconisé par l'ICCF Framework issu du groupe de travail de la commission européenne JRC dans le cadre de ses propositions pour une certification européenne des produits pour les systèmes industriels. Nous nous félicitons de cette nouvelle avancée ».

Vincent Jauneau, directeur Digital Industries chez Siemens France. © photo Vincent Jauneau

Depuis plus de 170 ans en France, le nom de Siemens est synonyme de performance technique, d'innovation, de qualité et de fiabilité. Siemens opère dans les domaines de l'électrification, de l'automatisation et de la digitalisation et compte parmi les principaux fournisseurs de technologies à haute efficacité énergétique, qui contribuent à préserver les ressources naturelles. L'entreprise est pionnière en matière d'équipements d'automatisme, de systèmes d'entraînement et de solutions logicielles destinées à l'industrie. Avec plus de 7 000 collaborateurs, 8 sites industriels et 11 centres de R&D dont 8 à responsabilité mondiale, Siemens France s'engage activement dans les filières stratégiques pour l'industrie française. Depuis 2017, Siemens est le seul équipementier dont les processus de développement sont certifiés sur la base de la Norme internationale IEC 62443-4-1 par le TÜV Sud, et également le seul à offrir des automates programmables industriels qualifiés par l'ANSSI.

Excellence par ailleurs renouvelée :

- avec le maintien en qualification obtenue en 2019 pour la gamme des automates S7-1500
- avec la labellisation SecNumEdu de sa formation Cybersécurité des systèmes industriels (SITRAIN DI-CYBER)
- avec notre SCADA WinCC Open Architecture (WinCC OA) doublement certifié, autant côté processus de développement que côté produit

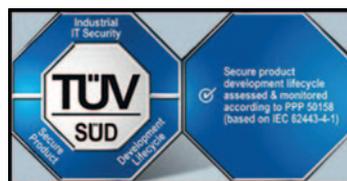
L'ensemble de ces distinctions montre combien le sujet cybersécurité est un enjeu stratégique pour le groupe. Associant la parole aux actes, Siemens est l'initiateur de la « Charter of Trust » pour promouvoir le sujet cybersécurité au plus haut niveau au sein des entreprises.

Suivez-nous sur Twitter
[@Siemens_France](https://twitter.com/Siemens_France)

Offre

Gamme complète d'automates industriels sécurisés, switch industriels sécurisés, surveillance de la sécurité des systèmes industriels

Certifications



Gamme complète d'automates industriels S7 1500 qualifiée



Switch industriels SCALANCE XM400, certifiés

Services

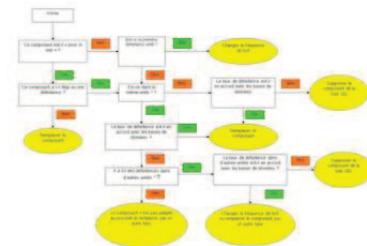
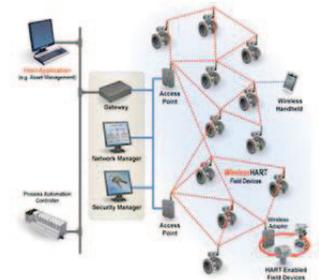
Un ensemble de services pour un accompagnement personnalisé :

- Diagnostic (cartographie, analyse de risques, évaluation de la maturité...)
- Conseil (gouvernance, formation...)
- Déploiement (cloisonnement réseau, durcissement des configurations...)
- Contrôle, validation, conformité (préparation à l'homologation, audit de conformité...)
- Maintien en condition de sécurité (mise à jour, gestion des vulnérabilités...)

* L'ingéniosité au service de la vie



Association des EXploitants
d'Équipements de mesure,
de Régulation et d'Automatismes



- Une trentaine de membres, de la PME à la multinationale
- Une douzaine de commissions techniques (+ de 60 réunions par an, 80 experts actifs au sein des commissions)
- 4 à 5 évaluations d'équipements lancées dans des laboratoires chaque année à la demande des membres
- Bibliothèque en ligne de rapports d'évaluation et de guides de bonnes pratiques (+ de 200 documents)
- 1 Hot-Line pour les échanges d'informations techniques rapides entre nos membres
- 1 à 2 journées techniques par an, ouvertes aux non-membres

CERCLE DES FEMMES DE LA CYBERSÉCURITÉ



**200 femmes
impliquées dans
les métiers et
les enjeux de
la cybersécurité**

Paris • Toulouse • Rennes • Lille • Marseille • Lyon



www.cefcys.com



contact@cefcys.com



www.linkedin.com/company/cefcys



[@CEFCYS_Officiel](https://twitter.com/CEFCYS_Officiel)



[facebook.com CEFCYS](https://facebook.com/CEFCYS)

LE CEFYCYS EN ACTION

Les actions du CEFYCYS visent à animer une communauté de femmes travaillant ou aspirant à contribuer au domaine de la Cybersécurité :

- Valoriser et professionnaliser les compétences des femmes via des groupes de travail, des programmes de mentorat, des publications de newsletters et de rapports...
- Organiser et/ou participer à des événements, des conférences en France et à l'international.
- Sensibiliser les entreprises, les partenaires éducatifs, les recruteurs à l'importance de la parité homme/femme et faire ainsi progresser la présence et l'impact des femmes.
- En action citoyenne, le CEFYCYS contribue à sensibiliser le grand public à la cybersécurité, en particulier les jeunes, pour la protection et l'éducation à l'usage sécurisé du numérique.

Parmi nos actions 2019...

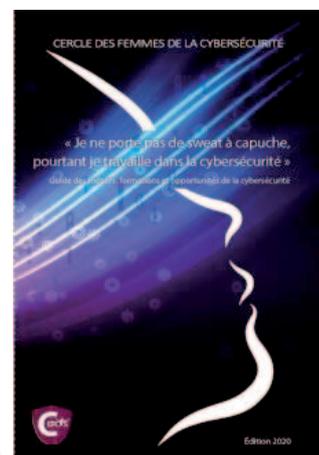
- Publication du livre « Je ne porte pas de sweat à capuche, pourtant je travaille dans la cybersécurité » : un guide inédit à destination des lycéens, parents, éducateurs, femmes souhaitant faire évoluer leur projet professionnel...
- Partenariat avec la Wild Code School pour la formation « analyste cybersécurité » : le CEFYCYS a collaboré à la définition du contenu de la formation. La première promotion de 15 élèves est 100% féminine..
- Fondation européenne Women4Cyber : CEFYCYS aspire à représenter la fondation européenne Women4Cyber en France, et militera dans ce sens derrière sa présidente.

4

mots clés
Sensibiliser
Éduquer
Prévenir
Protéger



WOMEN
4CYBER
EUROPEAN CYBER SECURITY ORGANISATION



ENGAGEMENT

De la jeunesse

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

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

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

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



Propulser l'en

Passerelle entre les
l'association offre
transformer vos idé



Développer l

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

Que vous souhaitiez pro
développement, tout est



DIRECTION



LA PRO



DÉFE

RÉFLEXIONS SÉCU
SERVICE INTERNATI

INNOVATION CULTURE

UNION EUROPÉENNE

STRATÉGIE

SOC

PROSPECT

JE

»»» NOS ACTIONS

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

Engagement !

mondes civil, diplomatique et militaire, de nombreuses opportunités de s'engager en engagement concret.



Promouvoir l'expertise innovante

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

Partager la connaissance

l'association organise une centaine de conférences et visites sur des sujets généralistes ou liés à l'actualité.

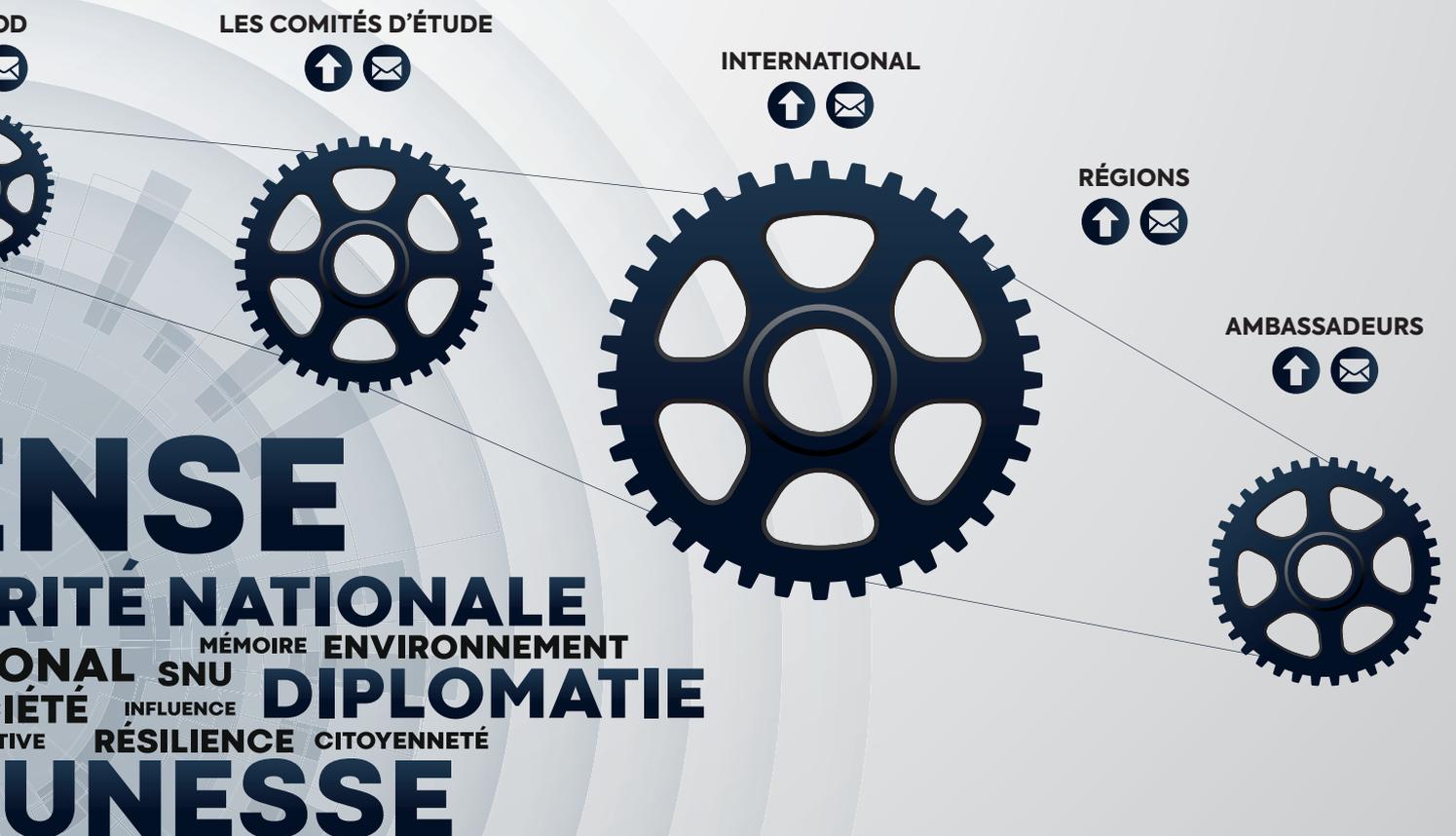


Fédérer un réseau international

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

»»» NOTRE ORGANISATION

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



CLUB DES EXPERTS

COOPÉRATION

DE LA SÉCURITÉ

CONFIANCE

DE L'INFORMATION

CONVIVIALITÉ,

ET DU NUMÉRIQUE



GROUPES DE TRAVAIL

Networking, vision transverse et retours d'expérience autour des sujets du moment

CONGRÈS

Prendre du recul sur les challenges de l'année, entre pairs

COLLÈGES

Focus sur de grandes thématiques, en groupes restreints

MENTORAT

Coaching, one-to-one et transmission des savoirs

LABS

Élaborer des réponses à des problématiques ciblées

PAROLES D'EXPERTS

Opportunité d'écouter des experts pour une vue technique d'ensemble



500+ MEMBRES

Directeur Cybersécurité, DSSI, RSSI, CISO, FSSI, RSI, Responsable de SOC/CERT, DSI
TOUS SECTEURS D'ACTIVITÉS GRANDES ENTREPRISES, ADMINISTRATIONS ET ENTREPRISES DE TAILLE INTERMÉDIAIRE

UNE VISION DU MÉTIER POUR MIEUX COMPRENDRE LES ENJEUX ET LES FAÇONS DE FAIRE, ET ÉLABORER DES MESSAGES CLÉS

↳ Un Club au service de ses membres, managers de la cybersécurité à travers une adhésion individuelle

↳ Une coopération pour construire une réponse plus efficace aux attaques

UNE DÉMARCHÉ INDÉPENDANTE

PAR RAPPORT À DES ENJEUX COMMERCIAUX ET INDUSTRIELS, UNE LIBERTÉ DANS LES CONVICTIONS ET LES PRISES DE PAROLE

↳ Une confidentialité des échanges, en mode Chatam House

↳ Une co-construction des bonnes pratiques

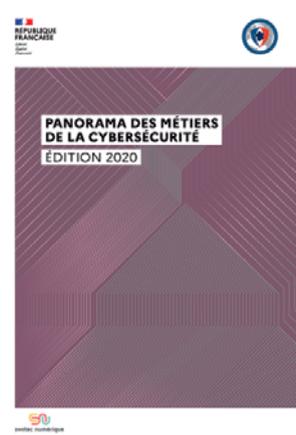
↳ Des évaluations et benchmarks

UNE LOGIQUE DE PARTAGE DES EXPÉRIENCES ET DES EXPERTISES ENTRE PROFESSIONNELS

↳ Une analyse commune des risques pour l'élaboration de stratégies de défense

↳ Une professionnalisation autour de modèles d'organisation et de compétences

DÉCOUVREZ LES CONTRIBUTIONS RÉCENTES DU CESIN :



NOS SPONSORS





UNIL | Université de Lausanne

Ecole des sciences criminelles



L'Ecole des sciences criminelles (ESC) est rattachée à la Faculté de droit, des sciences criminelles et d'administration publique de l'Université de Lausanne. Née de l'enseignement en photographie judiciaire donnée au début du XXe siècle par le Professeur Rodolphe Archibald Reiss, elle fut la première à délivrer une formation académique en police scientifique et demeure l'une des seules institutions en Europe à offrir une formation complète en science forensique.

La science forensique est à la croisée des sciences, du droit et des sciences humaines, des technologies et de leur application au droit. La criminalistique, la police scientifique et la criminologie, la politique criminelle et le droit pénal se penchent sur un phénomène de la société, le crime et ses dérivés, ainsi que sur les moyens de lutte, de prévention ou de répression dont elle dispose pour y faire face.

La mobilité et la technologie ont servi à l'internationalisation du crime. Ils alimentent les dérives criminelles au travers du terrorisme, des trafics de tout ordre (stupéfiants, armes, êtres humains, etc.) et des modes de reconversion du profit mal acquis par des filières financières organisées (blanchiment, corruption, etc.). Les conséquences politiques, économiques et judiciaires nécessitent des réponses que l'ESC aborde au travers de ses recherches, de ses développements méthodologiques et de la formation. Par des projets pilotes et des collaborations avec les organes judiciaires au plan local et international, l'ESC occupe une place particulièrement reconnue.

LA FORMATION DE BASE À L'ECOLE DES SCIENCES CRIMINELLES

L'ESC propose un Bachelor ès Sciences en science forensique. L'objectif de la première année est de poser les bases théoriques en chimie, sciences de base et sciences criminelles. La maîtrise de chacune des matières est essentielle à la poursuite des études. En seconde partie, le programme se spécialise et se concentre en offrant une proportion de travaux en laboratoires très importante.

L'ESC propose également plusieurs Masters.

Le Master ès Sciences en science forensique (120 crédits ECTS) a pour objectif de développer, d'approfondir et de compléter les connaissances acquises dans le cadre du Bachelor en science forensique. Ce Master possède trois orientations distinctes :

- orientation identification physique
- orientation criminalistique chimique
- orientation investigation et identification numériques

Le Master ès Sciences en traçologie et analyse de la criminalité (120 crédits ECTS) vise des compétences croisées en criminologie et en science forensique nécessaires à l'exploitation des traces dans l'analyse, la prévention et la gestion de phénomènes criminels variés. Il offre la possibilité d'étudier un semestre à l'Université de Montréal. Le Master en Droit en criminologie et sécurité (120 crédits ECTS) offre une formation pluridisciplinaire qui touche aussi bien à la sociologie qu'au droit, à la science forensique qu'à la psychologie.

L'ESC participe également aux Master interdisciplinaires suivants :

- Master en professions judiciaires
- Master en droit, criminalité et sécurité des technologies de l'information

RECHERCHE À L'ESC

Les recherches à l'École des sciences criminelles se sont développées autour d'axes scientifiques forts et au travers de travaux transdisciplinaires qui intègrent le phénomène criminel (le crime et ses auteur·e·s) comme dénominateur commun. Les domaines traités sont la trace, sa découverte et son interprétation, la documentation de scènes d'investigation et d'indices, le renseignement et l'analyse criminelle, la crimi-

nologie, les statistiques criminelles et la politique criminelle avec certains groupes qui focalisent leur intérêt sur la connaissance d'un type de phénomène (incendies, trafic de stupéfiants). L'ESC propose deux programmes de formation doctorale, un Doctorat en Sciences forensiques (PhD) et un Doctorat en Criminologie (PhD).

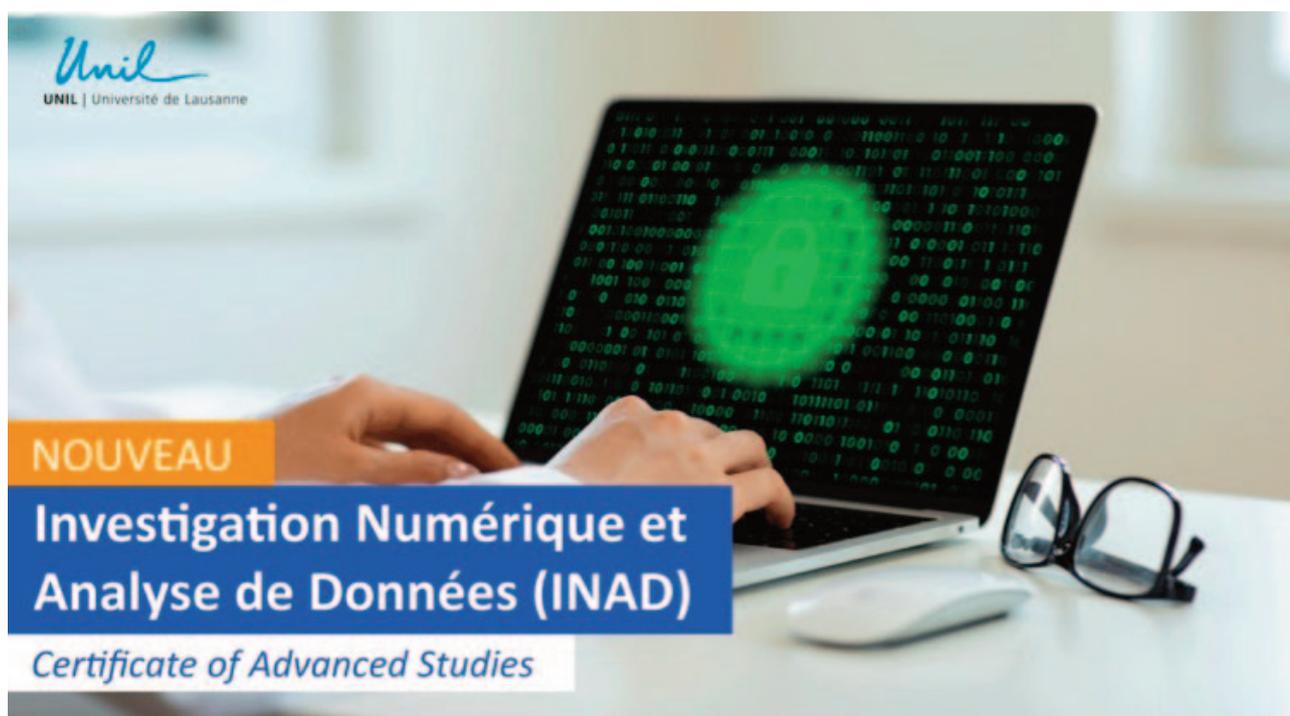
SERVICES D'EXPERTISES

L'ESC propose également des services d'expertises dans les domaines suivants :

- Stupéfiants
- Incendies et explosions
- Documents - écritures - signatures
- Identification de personnes
- Analyse d'images et photogrammétrie
- Microtraces
- Interprétation
- Investigations numériques

FORMATION CONTINUE

L'ESC offre de nombreuses formations continues et vient de mettre sur pied le CAS en Investigation numérique et analyse de données.

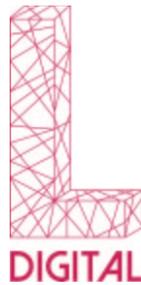


UNIL | Université de Lausanne

NOUVEAU

Investigation Numérique et Analyse de Données (INAD)

Certificate of Advanced Studies



Créé en 2016, le collectif LDigital fédère plus d'une centaine d'acteurs locaux dans la région Auvergne-Rhône-Alpes, investis sur la problématique de la présence des femmes dans le numérique. En janvier 2018, ce collectif est devenu la Fondation LDigital, abritée par la Fondation pour l'Université de Lyon.

L'objectif est de favoriser l'inclusion des femmes pour une économie numérique plus juste et plus performante. Grâce à l'implication de nombreux bénévoles et à ses partenaires, la Fondation LDigital développe des actions concrètes auprès des jeunes filles, des femmes et des entreprises. Ses missions sont de promouvoir le sujet, de connecter les besoins en numérique des entreprises et les talents féminins et de faire bouger les lignes.

Les actions de la Fondation LDigital se structurent autour de 4 grands thèmes :

- **FÉDÉRER** : Aider à coordonner des actions collectives en vue de mutualiser les énergies et outils et de déployer des actions plus impactantes en faveur de la place des femmes dans le numérique.
- **SENSIBILISER** : Coordonner des actions auprès des jeunes, en milieu scolaire ou non, de la maternelle à l'université. Ces actions de sensibilisation ont pour vocation d'initier les jeunes au code informatique et de les aider à découvrir le formidable éventail des métiers du numérique.
- **ACCOMPAGNER** : Faire profiter les femmes actives et en reconversion professionnelle des opportunités qu'offrent les métiers du numérique.
- **INCITER et VALORISER** la mixité dans les métiers du numérique en entreprises : Pour ce faire, la Fondation organise des matinées dédiées aux femmes pour leur présenter un éventail de métiers du digital à travers des témoignages de professionnelles. L'organisation de ces ateliers collaboratifs permet de créer des conditions favorables aux participantes pour se connaître, échanger et partager des questions communes et des solutions.



PLOSS-RA

Entreprises du Numérique Libre en Rhône-Alpes Auvergne
PLOSS-RA.FR

Ploss-RA est une association d'entreprises qui fédère, sur notre région Auvergne-Rhône-Alpes, plus d'une trentaine d'**Entreprises du Numérique Libre** (#ENL).

Ces entreprises proposent une très large gamme de services et solutions, **pour tous les secteurs et domaines de l'informatique et du numérique**, avec des logiciels libres et des logiciels Open Source. Les activités de nos entreprises sont essentiellement basées sur le service rendu à nos clients.

Logiciel Libre & Open Source ?

Une licence de logiciel libre vous donne :

- Liberté d'**utiliser** le logiciel ;
- Liberté d'**étudier**/examiner le logiciel ;
- Liberté de **modifier** le logiciel ;
- Liberté de **distribuer** le logiciel (modifié ou non).

Et il est important aussi de préciser :

- Libre ≠ Gratuit ;
- Libre ≠ Domaine public ;

Au sens littéral, Open Source ≈ Logiciel Libre – certaines libertés d'utiliser.

Pour chaque solution propriétaire, pour lesquelles vous vous acquittez de droits d'usages (licence), il existe **des alternatives Libres et Ouvertes**, du poste de travail (#Linux), sa bureautique (#LibreOffice), Internet (#Firefox), multimédia (#VLC) aux infrastructures « Internet » et serveurs, en passant par les ERP, les CRM, les logiciels spécifiques (gestion des délibérations, systèmes d'information géographiques, 2D, 3D etc.).

Les avantages sont très nombreux :

- **diversité** des offreurs et compétences pour le service (mise en place, formation, paramétrage, hébergement, maintien en condition opérationnelle, développements etc.) ;
- utilisations de **formats** de stockages de fichiers **ouverts** en phase avec le RGI version 2¹ ;
- **réversibilité**, ouverture et possibilité de contribuer, de financer des évolutions nécessaires (mutualisation de la demande pour les administrations et le secteur public ainsi que pour les entreprises).
- **sécurité** car, dans la mesure où le code source utilisé peut être librement étudié, cela constitue un gage évident et majeur pour assurer la sécurité des systèmes d'informations

Ploss-RA est membre fondateur du CNLL² qui a pour missions, au niveau national et européen, de structurer la filière du logiciel libre. Le CNLL fédère 11 clusters d'entreprises régionaux consacrés au logiciel libre, et représente plus de 300 entreprises dont le modèle économique repose sur l'open source : startups, éditeurs de logiciels, sociétés de service et cabinets de conseil - les ENL.



[Retrouvez l'annuaire des entreprises Ploss-RA.](#)

1 <http://referencemodernisation.gouv.fr/interoperabilite>

2 <https://cnll.fr/>



PRÉSENTATION DU CYBERCERCLE

Missions / Vocation

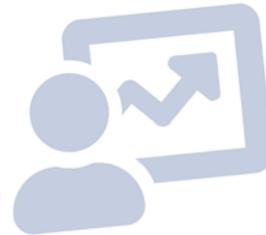
Le CyberCercle est un cercle de réflexion créé en 2012 alors que la sécurité numérique - la cybersécurité - n'en était encore qu'à ses débuts pour de trop nombreuses organisations, et l'apanage d'un nombre encore limité d'experts techniques.

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

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



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



La sécurité et la confiance numériques ne constituent pas une finalité en soi mais un ensemble de disciplines et d'expertises à réunir aux services des métiers.

Dans cette perspective, le CyberCercle traite de sujets sectoriels avec une forte expertise dans les domaines de la santé, du maritime, des territoires, des collectivités, de la Défense et de sujets thématiques tels que la réglementation, l'innovation et la recherche, la formation, l'industrie 4.0...

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



PRÉSENTATION DU CYBERCERCLE

Valeurs

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

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



Positionnement

Le CyberCercle a un positionnement unique.

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

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



Activités

Les activités du CyberCercle s'articulent autour de matinales, journées de rencontres, publications et modules de formation, déclinant un programme thématique établi chaque année.

En 2019, ce schéma directeur s'est construit autour de 3 thèmes principaux :

- Confiance numérique et politiques publiques aux niveaux national et européen : petits-déjeuners-débats-mensuels et RPCyber,
- Confiance numérique des territoires : Tour de France de la Cybersécurité (TDFCyber)
- Confiance numérique et maritime : des étapes du TDFCyber et les RPCyberMaritime.

Ces travaux se sont appuyés sur différentes publications et modules de formation.



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

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





Entre 2012 et 2018 le CyberCercle c'était :

- 72 petits-déjeuners-débats,
- + de 600 intervenants,
- + de 9000 participants

Quelques chiffres

En 2019, le CyberCercle a réalisé :

- 11 petits-déjeuners-débats,
- 6 étapes du Tour de France de la Cybersécurité,
- 2 matinales de rencontres (7^{ème} RPCyber - 5^{ème} RPCyberMaritime),
- Plusieurs interventions en Outre-Mer et à l'étranger.

Pour ce faire, il a mobilisé :

- 70 partenaires, sponsors et soutiens,
- un comité stratégique composé de 16 senior advisors,
- plus de 2300 participants ^[1] sur l'année,
- 250 intervenants de haut niveau,
- un réseau de plus de 10 000 contacts,
- un compte Twitter réunissant plus de 8300 followers



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

MERCI À NOS PARTENAIRES



CYBER
CERCLE



TOUR DE FRANCE DE LA CYBERSÉCURITÉ

#TDFCyber2020



CYBER
CERCLE

