CYBER CERCLE

# 27 OCTOBRE 2022 LYON

# RENCONTRES CYBERSÉCURITÉ AUVERGNE-RHÔNE-ALPES

#RCYBERARA
#TDFCYBER

La Région
Auvergne-Rhône-Alpes

DOSSIER PARTICIPANT

# RCyberAra

## Hôtel de Région - Lyon

## 27 OCTOBRE 2022

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 et renforcé depuis nos actions tout au long de l'année dans certaines régions.

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

Et la région Auvergne-Rhône-Alpes est le territoire sur lequel nous avons le plus développé nos actions.

Avec la crise de la COVID 19, le recours au numérique, devenu essentiel, a encore accéléré la transformation numérique des organisations, publiques et privées. Revers de la médaille : la surface de vulnérabilité face aux risques numériques a augmenté, les cyberattaques se multiplient de façon exponentielle et touchent aujourd'hui tous les acteurs, quels que soient leur taille ou leur secteur d'activité.

Permettre dans ce contexte d'avoir accès à une parole de confiance sur la sécurité numérique et favoriser les échanges constructifs pour avancer ensemble vers des territoires de confiance numérique sont les objectifs de cette quatrième édition des Rencontres de la Cybersécurité Auvergne-Rhône-Alpes.

Je remercie Renaud PFEFFER, Vice-président délégué à la sécurité de la Région Auvergne-Rhône-Alpes, de son soutien pour la réalisation de cet évènement dans l'Hôtel de Région.

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

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

Le territoire dans lequel nous sommes est un territoire dynamique, fort d'un écosystème économique riche et diversifié, doté de politiques publiques structurantes dont le Campus Région du Numérique est une réalisation phare.

Nous sommes heureux au CyberCercle de contribuer à cette construction d'un territoire de confiance numérique avec cette journée de Rencontres mais aussi, tout au long de l'année, avec nos matinales bimestrielles et notre Cycle Défense & Cyber.

Je remercie nos partenaires qui nous permettent le niveau organisationnel de qualité de ces Rencontres : la Région Auvergne-Rhône-Alpes, le Département du Rhône, le Groupe La Poste, Cybermalveillance.gouv.fr, proofpoint, le CEA, CERTitude NUMERIQUE, Elysium Security, Dicé, Avant de Cliquer, CSB School, ENEDIS, le cabinet S.B. & B.D, la Banque des Territoires et Stormshield.

Je remercie également nos soutiens, collectivités, ministères, écoles, associations, qui s'associent à cet événement dans cet esprit fédérateur qui est le nôtre.

Rappelons-nous que la sécurité numérique demande un effort individuel mais surtout collectif, une dynamique de gouvernance allant bien au-delà de la sphère des experts pour toucher l'ensemble de la Nation.

« *Construire ensemble des territoires de confiance et de sécurité numériques.* »
« *Agir efficacement ensemble pour construire une culture de sécurité numérique partagée au service des acteurs présents sur les territoires.* »

Cette quatrième édition des Rencontres de la Cybersécurité Auvergne-Rhône-Alpes s'inscrit pleinement dans cette double dynamique, de plus en plus fondamentale pour faire face collectivement aux enjeux actuels, qu'ils soient économiques, sécuritaires ou sociétaux.

**8h00** ■›› OUVERTURE DU CAFE D'ACCUEIL DANS L'ESPACE DE RENCONTRES-DEMONSTRATIONS

**8h30** ■›› OUVERTURE DES TRAVAUX
**Renaud PFEFFER**, vice-président délégué à la sécurité, Région Auvergne-Rhône-Alpes
**Bénédicte PILLIET**, présidente, CyberCercle

**9h00** ■›› KEYNOTES en plénière
9h00-9h30
Plan de transformation numérique et sécurité numérique d'une collectivité : le RETEX du Département du Rhône
**Daniel COISSARD**, directeur des Usages Numériques, Département du Rhône

9h30-10h00
Normes, standards et réglementation en matière de cybersécurité : point de situation
**Maître François COUPEZ**, avocat-fondateur, Level Up Legal

**10h00** ■›› PAUSE CAFE – NETWORKING – ESPACE DE RENCONTRES

**10h30** ■›› WORKSHOPS – DEMONSTRATIONS
Workshops - démonstrations en parallèle
Deux sessions horaires :
de 10h30 à 11h15 – de 11h15 à 12h00

➤ **« Un programme de formation pour développer la cybersécurité face au phishing. »**
**Astrid FROIDURE**, responsable des Affaires Publiques, Avant de Cliquer

➤ 1ère session : **« Démonstration d'une attaque de ransomware bloquée par la plateforme NEMESIS »**
➤ 2ème session : **« Démonstration d'une attaque à visée d'espionnage industriel avec fuite de données »**
**Yoan ISSARTEL**, CTO, co-fondateur et **Adel ALLAM**, consultant cybersécurité, Elysium Security – Root-Me PRO

➤ **« Dans la peau d'un attaquant : vivez une cyberattaque de l'intérieur »**
**Sébastien VIOU**, directeur cybersécurité produit et Cyber-Evangéliste, Stormshield

➤ **« La cybersécurité des collectivités de moins de 3500 habitants : une étude et des outils »**
**Laurent VERDIER**, chargé de mission sensibilisation - risque cyber, Cybermalveillance.gouv.fr

➤ **« Data, intelligence artificielle et cybersécurité dans les territoires – note de conjoncture du Groupe La Poste et de la Banque des Territoires – Caisse des Dépôts »**
**Dr Michel DUBOIS**, directeur technique, Direction de la Cybersécurité, Groupe la Poste

➤ **« Ransomware : anticiper pour ne pas subir : l'humain au cœur du dispositif »**
**Loïc GUEZO**, directeur Stratégie Cybersécurité, Proofpoint

**12h00** ■›› INTERVENTIONS
**Général de division Bernard CLOUZOT**, commandant en second la région de Gendarmerie Auvergne-Rhône-Alpes et la Gendarmerie pour la zone de défense et de sécurité Sud-Est

**Christophe GUILLOTEAU**, président, Département du Rhône

**12h30** ■›› COCKTAIL - NETWORKING - ESPACE DE RENCONTRES

**14h30** ■›› **ATELIERS**

*Placés sous les règles de Chatham House, les ateliers durent une heure trente et ont pour objectif de permettre aux participants d'échanger librement dans un cadre de confiance. Des orateurs ouvrent l'atelier par des interventions courtes pour apporter un éclairage sur le sujet puis l'ensemble des participants est invité par l'animateur de l'atelier à s'exprimer, soit pour poser des questions, soit pour apporter un témoignage, un retex ou une vision du sujet.*

➤ **ATELIER 1**

**Plan de relance & investissement pour la cybersécurité sur les territoires**

**Florent POINDRON**, investisseur Confiance numérique, Banque des Territoires - Caisse des Dépôts

➤ **ATELIER 2**

**Cybersécurité & innovation : comment favoriser l'innovation en cybersécurité ?**

**Stéphane MEYNET**, président, CERTitude NUMERIQUE
**Jacques FOURNIER**, responsable du programme cybersécurité, CEA-Leti - directeur adjoint, Grenoble Alpes Cybersecurity Institute
**Sébastien DARTIGALONGUE**, co-fondateur, CEO, Elysium Security – Root-Me PRO

➤ **ATELIER 3**

**Cybersécurité en santé : comment renforcer la culture et la maturité des acteurs de la santé ?**

**Philippe LOUDENOT**, ancien FSSI, ministères sociaux - senior advisor, CyberCercle
**Loïc GUEZO**, directeur Stratégie Cybersécurité, Proofpoint

➤ **ATELIER 4**

**Cybersécurité et mobilités : comment favoriser le développement de transports sécurisés ?**

**Daniel LAZZARONI**, chef de branches Energies & Transports, Siemens
**Séverine BESSON** , cheffe du Pôle Équipements Électriques et de Gestion, Centre d'Études des Tunnels
**Jean-Christophe MATHIEU**, directeur adjoint de la cybersécurité, Groupe SNCF
**Fabien COURAJOUD**, chef de service, BOUYGUES Energies & Services

➤ **ATELIER 5**

**Métiers & formations de la cybersécurité : faire de cette filière un point fort sur les territoires en Auvergne-Rhône-Alpes**

**Sophie CRUZ**, conseillère régionale Auvergne-Rhône-Alpes, Présidente d'Auvergne-Rhône-Alpes Orientation
**Guillaume COLLARD**, co-fondateur, CSB School
**Christian MARTINEZ**, responsable du département cyberdéfense, responsable du CERT, ENEDIS
**Clémence PHILIPPE**, membre, CEFCYS
**Diane RAMBALDINI**, présidente, ISSA France
**Quentin NICAUD**, directeur commercial et des partenariats, Elysium Security – Root-Me PRO

➤ **ATELIER 6**

**La communication de crise dans la gestion de crise cyber : des clefs pour réagir quand on est victime d'une cyberattaque**

**Laetitia BLANDIN**, consultante experte en communication
**Laurent VERDIER**, chargé de mission sensibilisation – risque numérique, Cybermalveillance.gouv.fr
**David GARCIA**, RSSI, Groupe Casino et Filiales

**16h00** ■›› **PAUSE CAFE – NETWORKING – ESPACE DE RENCONTRES**

**17h00** ■›› **CONFERENCE**

**« Comment sensibiliser les jeunes a la sécurité numérique »**

**Astrid FROIDURE**, senior advisor, CyberCercle
**Daniel COISSARD**, directeur des Usages Numériques, Département du Rhône
**Adjudante Malika WAVELET**, conceptrice en planification et gestion de crise, conseillère en sécurité économique, état-major de la Région de Gendarmerie Auvergne-Rhône-Alpes
**Diane RAMBALDINI**, présidente, ISSA France
**Hadi EL KHOURY**, vice-président, ISSA France

# Les intervenants

## Renaud PFEFFER

**Vice-président en charge de la sécurité**
**Région Auvergne-Rhône-Alpes**

## Sophie CRUZ

**Conseillère régionale**
**Région Auvergne-Rhône-Alpes**


©Céline Vautey

Sophie Cruz est conseillère régionale depuis 2015, très impliquée dans le domaine de la formation. Elle fait partie des commissions : C17 Formation continue et apprentissage – C14 Relations internationales – C15 Education et lycées.
Elle préside également Auvergne-Rhône-Alpes Orientation qui co-organise avec leurs partenaires la « Caravane des métiers ». Il s'agit d'un forum itinérant novateur dédié à l'orientation et la découverte des métiers. Ce projet collectif vise à mutualiser les moyens d'information des acteurs engagés pour la promotion des métiers, afin de proposer aux différents publics une offre de service complète et attractive au plus près des territoires. Durant deux semaines, une dizaine de véhicules et d'engins de démonstration menés par le bus de l'orientation parcourent la région à la rencontre des publics : collégiens, lycéens, étudiants, familles, adultes en reconversion et demandeurs d'emploi.

## Christophe GUILLOTEAU

**Président**
**Département du Rhône**

Christophe Guilloteau est depuis 2015 président du département du Rhône, il a été réélu en 2021. Il est également 1er vice-président du SDMIS et vice-président de l'Assemblée des départements de France en charge des relations avec l'Assemblée Nationale.
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 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 a été 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.
Christophe Guilloteau est Chevalier de l'Ordre National du Mérite et Chevalier du Mérite agricole, Capitaine de vaisseau dans la Réserve citoyenne de la Marine et Membre de la Réserve citoyenne Cyberdéfense.

## Bénédicte PILLIET

**Présidente**
**CyberCercle**


Crédit photo Alain Zimeray

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

## Daniel COISSARD

**Directeur des Usages Numériques**
**Département du Rhône**

Après avoir dirigé le GIP Maximilien (2017-2021), première plateforme d'e-administration, et développé la plateforme e-bourgogne, la toute première plateforme de marchés publics (2008-2016), Daniel COISSARD a rejoint, courant septembre 2021, le département du Rhône, en tant que Directeur des Usages Numériques. Fort de 30 ans d'expérience dans le domaine informatique (développement de jeux dans les années 80, formation, réseaux-télécommunication et gestion de projets de dématérialisation de procédures administratives et facturation), son travail est toujours axé sur :

- L'organisation, la coordination et la conduite de projets ouverts et innovants.
- La relation et la satisfaction de mes clients (internes ou externes).
- La sécurité des biens, des données et des personnes.

Ses motivations au quotidien :

- définir une stratégie, la décliner en plans d'action et piloter sa mise en œuvre,
- créer de nouveaux services numériques sécurisés répondant à un besoin ou une évolution réglementaire,
- optimiser le fonctionnement de l'organisation et coordonner l'action des développeurs, des chefs de projets et des clients,
- innover dans la recherche de solutions et l'optimisation de résultats,
- construire en commun une dynamique d'équipe et contribuer à développer le potentiel de chacun.

## Maître François COUPEZ

**Avocat fondateur**
**Level Up Legal**

François Coupez est un des senior advisors du CyberCercle. Avocat à la Cour, il a fondé et dirige le cabinet d'avocats Level Up Legal. Ancien responsable du droit des nouvelles technologies du Groupe Société Générale ou encore fondateur du cabinet ATIPIC Avocat, il met sa double compétence en droit et technologies de l'information au service des entreprises internationales, des institutionnels, des ETI ou encore des scale up, afin de les conseiller et de les assister face à leurs contraintes réglementaires. Vice-président du club R2GS, il est titulaire du certificat de spécialisation en Droit des nouvelles technologies délivré par le Conseil National des Barreaux, de la certification ISO 27 001 lead implementer niveau avancé ainsi que du certificat de Délégué à la Protection des Données (DPO – référentiel de la CNIL – certification AFNOR et APAVE). 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 plus de 20 ans dans le Master 2 « Droit du multimédia et de l'Informatique » de l'Université Paris 2 Panthéon-Assas, à Paris Dauphine ou encore au CNAM. 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).

## Astrid FROIDURE

**Chargée de Relations Publiques**
**Avant de Cliquer**

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

## Yoan ISSARTEL

**Co-fondateur**
**Elysium Security - Root-me PRO**

Yoan Issartel est co-fondateur de la Société Elysium Security et de Root-Me PRO, version pro de la fameuse plateforme Root-Me dédiée à l'apprentissage de la cybersécurité. En tant que CTO, Yoan orchestre les projets et opérations de cybersécurité des deux sociétés. Avec plus de 10 années d'expérience en sécurité défensive, son expertise permet d'intervenir dans des contextes souvent sensibles pour répondre à des problématiques de sécurité complexes : réponse à incident, audit de sécurité, conception d'architecture sécurisée, déploiement de solutions de sécurité, recherche et développement, ...

## Adel ALLAM

**Auditeur Cybersécurité**
**Elysium Security - Root-me PRO**

Adel Allam est Auditeur Cybersécurité au sein de la Société Elysium Security. Titulaire d'un Master 2 en sécurité informatique, Adel est un passionné qui organise et participe à de nombreux CTFs nationaux depuis des années. Depuis 2020, Il déploie ses compétences au sein des équipes Elysium Security en tant qu'Auditeur Sécurité et est investi dans de nombreux projets phares notamment liés aux tests d'intrusion en tant que lead de l'équipe offensive. Adel est également très actif au sein de l'équipe Root-Me Pro pour la création, l'organisation et l'animation de multiples challenges et CTFs.

# Les intervenants

## Sébastien VIOU

**Directeur cybersécurité produit et Cyber-Evangéliste**
**Stormshield**

Fort de 18 ans d'expériences dans le domaine de la Cybersécurité, chez des intégrateurs, opérateurs et société de conseils, Sébastien a participé à des projets de sécurité pour les secteurs Bancaires, Défense, Aéronautique et Public, aussi bien sur des architectures sensibles que des audit pour des PME locales.
Aujourd'hui Directeur cybersécurité produit et Cyber-Evangéliste pour Stormshield, il contribue au développement de la confiance et de l'expertise de l'entreprise auprès de nos partenaires et de nos clients.

## Dr Michel DUBOIS

**Directeur scientifique et technique**
**Direction de la cybersécurité**
**GROUPE LA POSTE**

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

## Général de division Bernard CLOUZOT

**Commandant en second**
**Région gendarmerie Auvergne-Rhône-Alpes**
**Gendarmerie pour la zone de défense et de sécurité Sud-Est**

Le Général de division Bernard Clouzot est ingénieur de formation de l'école spéciale de St Cyr. Il a été auditeur de la 9ème promotion du collège interarmées de défense (2002) et auditeur de la 3ème promotion du cycle interministériel de management de l'État (2014).
Après un parcours de commandement territorial, commandant la région de gendarmerie de Midi-Pyrénées puis commandant la région de gendarmerie d'Occitanie, en 2019 il est officier général chargé de la fonction retour d'expérience, chef de la cellule nationale de retour d'expérience de la gendarmerie nationale à Paris. Depuis 2022, le Général de division Bernard CLOUZOT est le Commandant en second de la région de gendarmerie Auvergne-Rhône-Alpes et la gendarmerie pour la zone de défense et de sécurité Sud-Est. Parmi ses nombreuses décorations, le Général de division Bernard CLOUZOT est officier de la Légion d'honneur et Commandeur de l'ordre national du Mérite.

## Laurent VERDIER

**Chargé de mission sensibilisation risque cyber**
**Cybermalveillance.gouv.fr**

Laurent Verdier a rejoint le dispositif Cybermalveillance.gouv.fr en septembre 2020 en tant que chargé de mission pour contribuer à l'animation et au développement de la sensibilisation des publics au risque cyber.
Officier de police mis à la disposition du dispositif par le ministère de l'Intérieur, il mettra à profit son expertise en matière de cybercriminalité et son expérience acquises dans ce domaine depuis 2002 à la Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI) de la Préfecture de Police, à la Direction Centrale du Renseignement Intérieur (DCRI) puis au sein du Centre de Cyberdéfense de l'ANSSI.

## Loïc GUEZO

**Directeur, Stratégie Cybersécurité**
**Proofpoint**

Dans le cadre de son poste de Directeur en Stratégie Cybersécurité, Loïc Guézo a pour missions de superviser le développement stratégique de Proofpoint auprès de ses clients et partenaires dans la zone Europe du Sud, ainsi que d'intervenir en tant qu'expert pour représenter l'entreprise au sein de l'écosystème.
Fort de 25 ans d'expérience, Loïc Guézo conseille les grandes entreprises sur leurs stratégies de défense en matière de cybersécurité, et s'assure que les clients de Proofpoint aient une vision cohérente des menaces avancées d'aujourd'hui et de la protection de leurs collaborateurs, de leurs données et de leurs marques afin d'être mieux protégées.
Précédemment Loïc Guézo a occupé différentes fonctions dans le secteur informatique depuis 1988, notamment chez Trend Micro, EDF (système de contrôle nucléaire) Sagem (Ingénieur d'Etude pour l'OTAN), au sein de l'Agence Française de Développement (Responsable Informatique Outre-Mer) et chez IBM France (CTO Security Services).
Reconnu comme expert dans le domaine de la sécurité de l'information et de la gestion des risques, Loïc Guézo est régulièrement interrogé par les médias et agences de presse internationales et a été identifié comme faisant partie du « Top100 des cyber influenceurs français » en 2019.
Loïc anime l'écosystème en travaillant avec les médias et différentes associations professionnelles telles que le CLUSIF (Club de la Sécurité de l'Information), le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique), ou encore l'ARCSI (Association des Réservistes du Chiffre et de la Sécurité de l'Information). Depuis octobre 2018, il est également réserviste citoyen de la Police Nationale au sein du réseau des référents cybermenaces zonaux.
Loïc Guézo est diplômé de l'Université Paris XIII, d'un Mastère Spécialisé « Open Source & Sécurité » de l'Ecole Centrale Paris.

## Florent POINDRON

**Investisseur dans la confiance et souveraineté numériques**
**Groupe Caisse des Dépôts**

Florent Poindron est investisseur dans la confiance et souveraineté numériques. Diplômé d'un Master en Ingénierie financière de l'Université Lyon II et d'un Diplôme Universitaire en Droit des entreprises en difficulté de l'Université Paris Sorbonne, Florent a travaillé au sein de l'Assemblée nationale (commission des finances) en tant que collaborateur parlementaire et au sein du ministère de l'Economie, des Finances et de la Relance en tant que chargé de restructurations d'entreprises en difficulté ayant des effectifs compris entre 50 et 400 salariés. C'est à la suite de ces riches expériences que Florent a intégré le Groupe Caisse des Dépôts début 2022.

## Sébastien DARTIGALONGUE

**Co-fondateur**
**Elysium Security - Root-Me PRO**

Sébastien Dartigalongue est co-fondateur de la Société Elysium Security et de Root-Me PRO, version pro de la fameuse plateforme Root-Me dédiée à l'apprentissage de la cybersécurité. En tant que CEO, Sébastien assure notamment la cohérence de la stratégie et le développement des activités des deux sociétés. Avec plus de 10 années d'expérience en sécurité défensive, son expertise permet d'intervenir sur des problématiques notamment liées principalement à la gouvernance : stratégie de sécurité, analyse de risque, sensibilisation, formation, ...

## Jacques FOURNIER

**Directeur de recherche et Responsable de programme cybersécurité**
**CEA Leti**

Jacques Fournier est directeur de recherche (HDR), responsable de programme cybersécurité et adjoint au chef de Service Sécurité des Systèmes Embarqués et Composants au sein de l'institut Leti du CEA. Ses thématiques d'intérêts portent sur la sécurité des systèmes embarqués en général, plus particulièrement sur la cryptographie, la conception matérielle et les couches basses logicielles. Avant de rejoindre le CEA en 2009, Jacques Fournier a travaillé pendant plus de 8 ans au laboratoire Sécurité de Gemplus/Gemalto. Titulaire d'un diplôme d'ingénieur de Centrale-Supélec, il a ensuite effectué un Master à Georgia Tech (USA) et un doctorat en informatique à l'Université de Cambridge (UK).

## 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 LOUDENOT

**Senior advisor**
**CyberCercle**

Philippe Loudenot est senior advisor du CyberCercle depuis 2018.
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 autorités administratives indépendantes en matière de cybersécurité. En 2014, Philippe Loudenot rejoint le HFDS des ministères chargés des affaires sociales en tant que FSSI. Référent Cybersécurité de la Région des Pays de la Loire à partir de 2020, il a rejoint en juillet 2022 la société BlueFiles comme Cyber Strategist.
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, membre du CESIN et du club EBIOS.

# Les intervenants

## Daniel LAZZARONI

**Chef de Branche 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 et chef de projet durent de nombreuses années, puis Ingénieur de vente, responsable commercial régional puis grand compte. Depuis 2007 il est Chef de Branches Energie et Transport.
Depuis plus de 35 ans M. Lazzaroni est au service de la sécurité dans les transports, par câbles, routes, rails, sur la plupart des ouvrages en France et à l'export en suivi des partenaires et de l'écosystème du transport.

## Fabien COURAJOUD

**Chef de service, division Mobilité**
**Bouygues Energies & Services**

Fabien Courajoud, Chef de service chez Bouygues Energies & Services au sein de la division Mobilité.
Entré chez Bouygues Energies et services en 2016 en tant que Chef de groupe, il encadre et dirige des projets de type tunnel durant 3 ans. Dans le cadre de l'évolution du service, il devient chef de service et prend la direction de l'agence du Bourget du lac et la gestion de grand projet Routier mais également de transport guidé.
Depuis 2018, il est en charge de la gestion du projet Fréjus en groupement avec Spie et Technositaf. BYES est responsable des infrastructures réseaux, GTC et pilotage de la Cybersécurité dans un contexte binational avec des contraintes de sécurité élevées.
M. Courajoud a passé plus de 20 années professionnelles dans le monde des infrastructures souterraines. Pour le CERN dans le cadre d'activité de maintenance puis sur la conception des systèmes électriques du LHC et pour EGIS durant 8 ans sur la conception et réalisation des tunnels routiers sur le territoire national et international.

## Christian MARTINEZ

**Responsable du département cyberdéfense,**
**Responsable du CERT**
**ENEDIS**

Ingénieur de développement de formation, Christian Martinez a recruté par Enedis en 2008 en tant que responsable des infrastructures en datacenter et depuis 2019, il gère la mise en place et est responsable du CERT Enedis.
Le CERT est en charge de la surveillance cyber du SI de l'entreprise et de la lutte contre le piratage informatique.

## Séverine BESSON

**Ingénieur travaux publics chez CETU**
**Cheffe du Pôle Equipements Electriques et de Gestion**

Depuis 2018, Séverine Besson, ingénieur travaux publics, est cheffe du Pôle Equipements Electriques et de Gestion chez CETU (Centre d'Etudes des Tunnels). Elle a en charge l'encadrement des chargés d'études du pôle et de la centrale d'inspection des équipements (9 personnes).
Elle a en charge :

- d'améliorer la connaissance des enjeux et du fonctionnement des équipements de tunnel dont éclairage, alimentation électrique, vidéo DAI, réseaux automatismes, GTC supervision, cyber sécurité, sureté de fonctionnement,
- d'accompagner les maitres d'ouvrage dans les projets de construction ou de rénovation de tunnels : assistance à maitrise d'œuvre ou à maitrise d'ouvrage, expertises techniques, contrôles de thématique,
- le pilotage d'actions de recherche appliquée sur les équipements : co-encadrement d'une thèse ENTPE/CETU sur l'éclairage Led des tunnels, mise en place du partenariat de recherche DELTA (démonstrateur éclairage Led du tunnel d'Antony),
- de contribuer à l'évolution des textes réglementaires et des guides techniques : révision du guide sur la détection automatique d'incident par analyse d'image, document d'information sur le comportement au feu des câbles
- de participer aux groupes de travail nationaux et internationaux (Afnor comité X90X et TC4-53 de la Commission Internationale de l'Eclairage),
- et de participer à la mise en place de la démarche qualité (pilote de l'activité « participation aux missions de maitrise d'œuvre » au sein du processus Ingénierie).

Elle est issue de l'École Nationale des Travaux Publics de l'État de Lyon, Voie d'approfondissement maritime et fluvial.

## Guillaume COLLARD

**COO – Associé**
**CSB School**

Guillaume Collard a été formé sur les bancs de l'université Lyon 3 avant de rejoindre l'entreprise Solvay. Convaincu de la nécessité d'avoir une service dédié à la cybersécurité, Guillaume a réuni autour de lui une équipe d'experts. Devenu Responsable de la cybersécurité IT du groupe et face à une pénurie de talents de plus en plus forte, Guillaume a décidé de co-fonder la première école supérieure de management exclusivement dédiée à la Cybersécurité, la CSB.SCHOOL. Dans la logique de cette création, Guillaume a relevé le défi de reprendre la direction de Workinlive, une entreprise de formation numérique.

## Diane RAMBALDINI

**Présidente**
**ISSA France**

Diane Rambaldini est fondatrice de la société Crossing Skills. Elle propose aux entreprises du Conseil et de la Pédagogie en sécurité numérique, considérant qu'une meilleure lisibilité et accessibilité de la cybersécurité est un pré requis à son adoption par les acteurs économiques.
Experte en gestion des risques informationnels, elle conseille, audite et forme les entreprises sur des aspects de gouvernance et de réglementation, notamment sur le volet cyber des lois de programmation militaire et, en tant que DPO certifiée, sur la réglementation de la vie privée (RGPD).
Diane Rambaldini est juriste de formation et titulaire de trois Master Pro en Droit et Stratégie de la sécurité, Gestion des Risques et en Criminologie. Elle a également été auditrice de l'Institut d'Etudes et de Recherche pour la sécurité des entreprises auprès de la Gendarmerie Nationale (10ème Promotion). Elle a fait ses débuts au sein du Groupe Thales.
Elle est en parallèle présidente et cofondatrice de l'association ISSA France Security Tuesday dont la vocation est d'informer et d'éduquer différents publics à la protection numérique. Elle est co-auteure du premier cahier de vacances en sécurité numérique Les As du Web sorti en 2018 et du livre Envie de Cyber publié en 2021 aux éditions Studyrama.

## Jean-Christophe MATHIEU

**Directeur adjoint de la cybersécurité,**
**Groupe SNCF**

Jean-Christophe Mathieu a démarré sa carrière en tant que chef de projet dans le monde de l'intégration de systèmes industriels dans des domaines aussi variés que la sidérurgie, l'automobile, l'agroalimentaire, les transports et ce à travers le monde...
Il rejoint ensuite le groupe SIEMENS au sein du secteur Industry en tant qu'ingénieur d'assistance technique, puis devient référent technique national pour les réseaux et la cybersécurité des systèmes industriels.
Successivement Product and Solution Security Officer puis coordinateur cybersécurité pour le groupe Siemens en France il a conduit l'ensemble des travaux pour la labellisation des formations, la certification et la qualification par l'ANSSI pour une large gamme de produits Siemens.
Il a également activement participé aux travaux de l'Agence Nationale pour le sécurité des systèmes d'information (ANSSI) pour la cybersécurité des systèmes industriels ainsi qu'aux travaux européens (ERNCIP, ENISA) en matière de protection des infrastructures critiques.
Au sein d'Orange cyberdéfense en tant que global head of industrial cybersecurity, il crée et développe au niveau mondial les activités liées à la protection des systèmes industriels.
Aujourd'hui Directeur Adjoint cybersécurité à la SNCF il coordonne l'ensemble des équipes en charge de la protection numérique opérationnelle du groupe de transports.

## Clémence PHILIPPE

**Membre**
**CEFCYS**

Cofondatrice et COO au sein de la société EXAMIN, conformité réglementaire, cybersécurité. Elle y est désormais directrice des opérations.
Clémence Philippe est également membre de la communauté SISTA et de l'association CEFCYS (Cercle des Femmes de la Cybersécurité). Formée à l'ISMAPP, master Affaires européennes puis à l'université Paris 1 Panthéon-Sorbonne, DESS Droit du numérique et des nouvelles techniques, elle fût avocate associée chez Welaw avocats, avocats spécialistes en droit des nouvelles technologies, de l'informatique et de la communication.

## Quentin NICAUD

**Directeur commercial et des partenariats**
**Elysium Security - Root-Me PRO**

Quentin Nicaud est directeur commercial et des partenariats au sein d'Elysium Security et de Root-Me PRO, version pro de la fameuse plateforme Root-Me dédiée à l'apprentissage de la cybersécurité. Quentin assure notamment le développement commercial des deux sociétés, noue des partenariats stratégiques au sein de l'écosystème et participe à de nombreux évènements. Son parcours atypique lui permet de traiter des sujets aussi bien sur le territoire national qu'à l'international.

## Laetitia BLANDIN

**Consultante en stratégie de communication**
**Chargée de cours de communication de défense**
**Université Paris 2 Panthéon-Assas**

Consultante en stratégie de communication, Laetitia Blandin a fait l'ensemble de sa carrière dans la défense ; d'abord dans les domaines de l'intelligence économique – auprès de Bertin Technologies, TransWorldSearch (cabinet de conseils – étude pour un groupe de défense) et du GICAT (Groupement des Industries de Défense et de Sécurité terrestres et aéroterrestres) – puis de la communication externe et d'influence – elle a été directrice de la Communication et des Etudes économiques du GICAT, directrice de la Communication externe de Nexter (Groupe KNDS) et dernièrement chef du pôle influence de la DICoD (Délégation à l'Information et à la Communication de Défense) du ministère des Armées. Elle est chargée de cours de communication de défense à l'Université de Paris 2. Laetitia Blandin est diplômée du Master 2 Défense, Géostratégie et Dynamiques industrielles (Paris 2), d'un Master 2 en Histoire contemporaine (Paris 4) et d'un Master 1 en Science politique (Paris 2), et elle est auditrice de la 69ème promotion de l'IHEDN – Politique de Défense.

# Les intervenants

## Adjudante Malika WAVELET

**Conceptrice en planification et gestion de crise**
**Conseillère en sécurité économique**
**Etat-major de la région de gendarmerie**
**Auvergne-Rhône-Alpes**

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


## David GARCIA

**RSSI**
**Groupe CASINO et Filiales**

Après 5 ans en société de services comme consultant à travers toute la France, il rejoint le Groupe Casino pour une prestation qui durera 3 ans. Embauché Casino, il prend la responsabilité de différentes équipes au sein de la production, pour finir par piloter l'ensemble des serveurs, San et stockage de la DSI. En 2016 il rejoint la DSSI en tant que RSSI adjoint, puis en tant que RSSI en 2017. En 2018 et à la demande de la Direction Générale il fonde la Sécurité Groupe dont il prend la responsabilité : en plus de son rôle de RSSI Casino, il pilote l'ensemble des RSSIs des filiales, Cdiscount Monoprix et Franprix pour les plus importantes en France, mais aussi toute la partie Amérique du Sud qui représente 50% du Groupe Casino.
Son approche de la sécurité se base sur son expérience au sein de la Production : avoir une approche pragmatique compatible avec les contraintes métiers et DSI, se focaliser sur la continuité de service, et ne croire que ce qu'il peut vérifier directement ...

## Hadi EL-KHOURY

**Vice-président**
**ISSA France**

Hadi détient un diplôme d'ingénieur électrique en télécommunications de l'Ecole Supérieure d'Ingénieurs de Beyrouth (ESIB), Université Saint Joseph (USJ) et un Mastère Spécialisé en Sécurité des Systèmes Informatiques et des Réseaux de Télécom ParisTech.

Durant les 21 dernières années, Hadi a conseillé, audité, formé et entraîné des dizaines d'organisations à travers le monde, dans les secteurs privés et publics, sur les questions de cybersécurité et de gestion des risques numériques. Il détient plusieurs prix et distinctions en matière d'innovation en sécurité numérique.
Hadi intervient régulièrement dans les écoles, universités, conférences, événements et médias au sujet de la cybersécurité et du numérique.
Son approche pédagogique est fortement reconnue et plébiscitée, de l'aveu des milliers d'auditeurs ayant suivi ses formations ou assisté à ses présentations.
Hadi est co-auteur du cahier de vacances "Les As du Web" pour les 7 ans et plus, édité par l'ISSA France Security Tuesday et de l'ouvrage « Envie de Cyber » pour les 15 ans et plus, paru aux éditions Studyrama début 2022.

RENCONTRES
CYBERSÉCURITÉ
AUVERGNE-RHÔNE-ALPES

# MERCI À NOS PARTENAIRES & SOUTIENS

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

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

PARTICULIERS, ENTREPRISES,
COLLECTIVITÉS TERRITORIALES :

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

**PIRATAGE**

**ARNAQUE**

**CHANTAGE**

**VIRUS**

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

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

# MISSIONS
## DU DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

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

# MEMBRES

PREMIER MINISTRE

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE LA JUSTICE

MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

MINISTÈRE DES ARMÉES

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

proofpoint®

# Protégez les personnes. Défendez les données.

Neutralisez les menaces avancées.
Protégez vos données.
Modernisez la conformité.
Solutions de cybersécurité centrées sur les personnes Proofpoint.

**En savoir plus :**
Proofpoint.com/fr

proofpoint®

Protect people. Defend data.

Sensibilisation à la sécurité

# Instaurez une culture de sensibilisation à la sécurité informatique

Les meilleures formations de sensibilisation à la sécurité informatique pour modifier le comportement des utilisateurs et transformer leur vulnérabilité en résilience.

**En savoir plus :**
Proofpoint.com/fr

LES JEUNES IHEDN

# ENGAGEMENT

## De la jeunesse

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

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

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

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

**Propulser l'en**

Passerelle entre les l'association offre transformer vos idé

**Développer l**

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

Que vous souhaitiez pro développement, tout est

# NOS ACTIONS

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

### ngagement !

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

### Promouvoir l'expertise innovante

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

### a connaissance

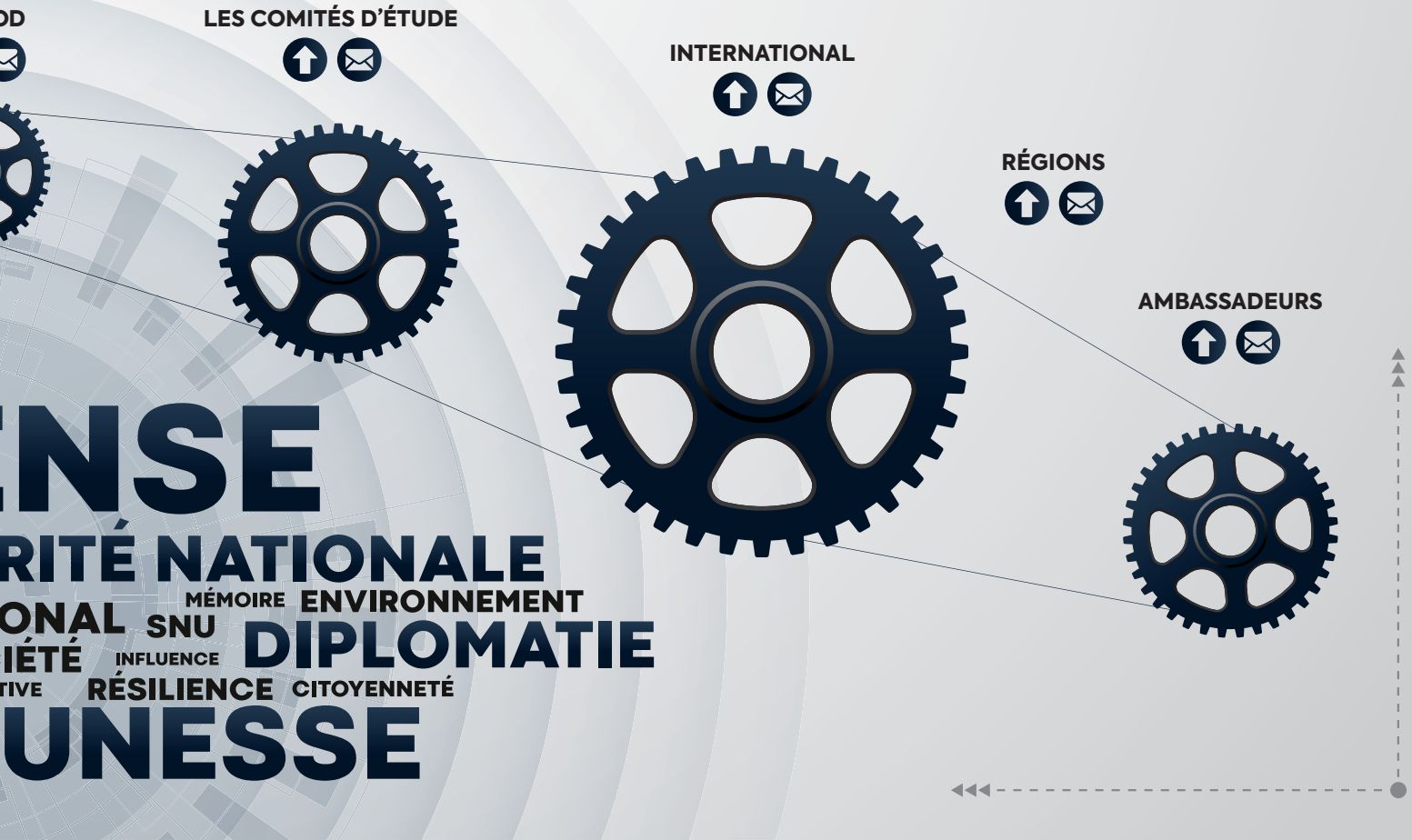
association organise une centaine de rs et visites sur des sujets généralistes ou e avec l'actualité.

### Fédérer un réseau international

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

# NOTRE ORGANISATION

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




Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin d'assurer la cybersécurité de leurs infrastructures critiques, de leurs données sensibles et de leurs environnements opérationnels. Les technologies Stormshield, certifiées et qualifiées au plus haut niveau européen, répondent aux enjeux de l'IT et de l'OT afin de protéger leurs activités.

**Notre mission : cyber-séréniser nos clients pour qu'ils puissent se concentrer sur leur cœur de métier, si cruciale pour la bonne marche de nos institutions, de notre économie et des services rendus aux populations. Choisir Stormshield, c'est privilégier une cybersécurité européenne de confiance.**

En France, **Stormshield détient plusieurs Visas de Sécurité de l'ANSSI**. En Espagne, nous sommes également le seul éditeur de pare-feux à avoir obtenu les deux qualifications « Producto CCN Aprobado » et « Producto CCN Cualificado ».

**Nos solutions sont alignées sur les meilleurs standards**. Nos expertises et la robustesse de nos produits nous permettent d'accompagner les entreprises dont la criticité cyber est extrême. Et surtout, lorsque l'IT & l'OT deviennent des éléments vitaux sur les plans économiques, sociétaux, techniques et humains, il est primordial d'être cyber-résilient.

## Des technologies de confiance

Stormshield propose un portefeuille de produits mature permettant une large couverture des besoins de protection des environnements IT/OT. Nos expertises nous permettent d'accompagner les entreprises dont la criticité est extrême par rapport aux problèmatiques de cybersécurité. C'est pourquoi, nous œuvrons dans le développement d'une protection durable contre les menaces les plus avancées, au travers de trois gammes de produits.

STORMSHIELD NETWORK SECURITY

Une gamme de pare-feux & VPN de nouvelle génération

STORMSHIELD DATA SECURITY

Un chiffrement de bout en bout multi-devices et multi-applications

STORMSHIELD ENDPOINT SECURITY

Une protection avancée des postes et serveurs Windows

La gamme Stormshield Network Security englobe une offre industrielle via la mise à disposition de pare-feux renforcés, le SNi40 et le SNi20 (les seuls pare-feux industriels qualifiés par l'ANSSI), pour les environnements à fortes contraintes. Ces boîtiers de sécurité, co-désignés avec des partenaires industriels de renom, s'intègrent facilement aux environnements opérationnels et garantissent une détection et protection sans aucun impact sur l'activité industrielle.

Par ailleurs, Stormshield a lancé en 2021 le SNxr1200, un pare-feu ultra durci qui répond parfaitement aux exigences et enjeux complexes de la sécurité des environnements critiques. Développé en respectant un certain nombre de standards militaires, il dispose de nombreuses certifications environnementales lui permettant d'être déployé dans des contextes contraints.

## Un réseau mondial de partenaires certifiés

**Stormshield, c'est aussi un réseau de partenaires de confiance, qui portent nos engagements et qui nous permettent de faire rayonner nos valeurs françaises et européennes bien au-delà de nos frontières.**

Nous avons créé ce qui est le 1er réseau de partenaires cybersécurité en France. Stormshield, c'est plus de 800 partenaires certifiés sur le territoire (plus de 1500 personnes par an) et plus globalement, une présence dans 40 pays qui nous permettent d'avoir une visibilité et une présence au plus près de nos clients.

Cette proximité se révèle déterminante pour co-construire des offres de sécurité plus simples et plus fiables qui proposent une alternative robuste aux solutions américaines et israéliennes. Des solutions de confiance, auditées en toute transparence et garanties sans backdoors !

Pour en savoir plus : www.stormshield.com

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

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

# CONFIANCE, QUALITÉ, EXPERTISE : LE LABEL EXPERTCYBER

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

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

## 1 QU'EST-CE QUE LE LABEL EXPERTCYBER ?

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

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

## 2 QUI SONT LES PRESTATAIRES LABELLISÉS ?

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

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

## 3 QUI PEUT FAIRE APPEL À UN PRESTATAIRE LABELLISÉ EXPERTCYBER ?

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

## 4 POURQUOI FAIRE APPEL À UN PRESTATAIRE LABELLISÉ ?

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

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

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

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

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

PLUS D'INFORMATIONS SUR
**WWW.EXPERTCYBER.FR**

# SUR TOUS LES FRONTS

ELYSIUM SECURITY

## PRODUITS NEMESIS

Solutions souveraines

En tant que Dirigeant, DSI ou RSSI, vous êtes garant de la sécurité du système d'information de votre organisation. Le marché de la cybersécurité fourmille de solutions qui s'avèrent bien souvent insuffisantes, complexes ou trop coûteuses.

Les challenges sont nombreux, le risque omniprésent et de nombreuses questions se posent.

**C'est en partant de ces constats que nous avons développé la suite NEMESIS :**
une suite de sécurité souveraine, conçue pour offrir une protection globale, opérationnelle et accessible à tous types d'organisations.

### VOS PROBLÉMATIQUES

- EXPOSITION ACCRUE À LA MENACE
- MANQUE DE VISIBILITÉ SUR VOTRE PROTECTION RÉELLE
- MANQUE DE RESSOURCES ET DE COMPÉTENCES
- ACCESSIBILITÉ DES SOLUTIONS DE PROTECTION

## NEMESIS UNIFIED PROTECTION

Grâce a des capacités unifiées de détection et de réponse aux incidents de sécurité, **NEMESIS UP (SIEM, SOAR, INTEL)** agit comme un système d'alarme dédié.

Il offre une **protection centralisée en temps réel** des systèmes d'information de tous types (IT/OT) tout en vous permettant de **réduire vos coûts d'exploitation** et de **répondre à vos obligations de conformité.**


- **SIEM** — CORRÉLER LES INFORMATIONS DE SÉCURITÉ ET DÉTECTER LES MENACES
- **SOAR** — ORCHESTRER ET AUTOMATISER LES PROCESSUS DE RÉPONSE AUX INCIDENTS
- **INTEL** — ENRICHIR, CONTEXTUALISER ET OPTIMISER LES FONCTIONS DE DÉTECTION ET RÉPONSE

- PROTECTION CONTINUE <24/7>
- VISION GLOBALE ET UNIFIEE
- ACCESSIBLE À TOUS

## NEMESIS SECURE LOG

Avec NEMESIS SL : **centralisez, archivez, protégez** et consultez l'ensemble des **traces et événements de sécurité** générés par votre système d'information. Idéal pour réaliser des investigations numériques ou répondre aux exigences de conformité.

## NEMESIS OPEN xDR

Avec NEMESIS Open xDR : **raccordez des solutions de sécurité complémentaires** et **open source** sur une interface unique afin de centraliser leur gestion quotidienne et réduire les coûts d'exploitation associés.

# DE VOTRE PROTECTION

ELYSIUM SECURITY

## COMPTOIR SÉCURITÉ

**Vous manquez d'une expertise ou de temps pour traiter une problématique de sécurité ?**

L'abonnement au Comptoir Sécurité Elysium vous permet de profiter d'un lien permanent et privilégié avec nos experts sous des délais garantis et d'accéder à des ressources opérationnelles accessibles 24/7.

## SERVICES OFFENSIFS ET DEFENSIFS

Des réponses concrêtes pour une défense adaptée, cohérente et conforme aux normes et bonnes pratiques.

- Tests d'intrusion & Audit de sécurité
- Investigation & Réponse à incident
- Conseil & Expertise technique

## FORMATIONS EN CYBERSECURITÉ

Des formations pour tous niveaux, conçues et animées par des experts et s'appuyant sur des environnements pratiques innovants (dont Root-Me PRO).

Qualiopi processus certifié — RÉPUBLIQUE FRANÇAISE

RootMe PRO

## ROOT-ME PRO

**La version Pro de la fameuse plateforme Root-Me ( plus de 500K membres) qui fédère une communauté de passionnés de la cybersécurité autour de nombreux challenges et CTF.**

- ✓ CHALLENGEZ, ENTRAINEZ ET SUPERVISEZ VOS ÉQUIPES
- ✓ ORGANISEZ DES CTFS ET ÉVÉNEMENTS CYBER
- ✓ RECRUTEZ DES EXPERTS
- ✓ COMMUNIQUEZ AUPRES DE LA COMMUNAUTÉ ROOT-ME

ELYSIUM SECURITY — RootMe PRO

pro.root-me.org

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

# LE RÉSEAU DES RÉFÉRENTS CYBERMENACES

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

## UN CONSTAT

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

## 3 AXES OPÉRATIONNELS STRATÉGIQUES

**AXE 1**

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

**AXE 2**

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

**AXE 3**

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

## LA MISE EN ŒUVRE DU RÉSEAU

**Par qui ?**

Le réseau est constitué :

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

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

**Pour qui ?**

Le réseau s'adresse principalement :

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

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

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

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

## VOUS ÊTES VICTIME D'UNE CYBERATTAQUE ?

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

## LE RÉSEAU DES RÉFÉRENTS CYBERMENACES

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

### CONTACTS

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




POLICE NATIONALE

# CSB.SCHOOL

## N'étudiez pas la cybersécurité, vivez-la !


Un campus de 2500m2 entièrement dédié à la formation en cybersécurité : informatique, industrielle, gestion de crise et gouvernance/risques/conformité

**Bachelor Spécialiste en cybersécurité**

**Mastère Manager en cybersécurité**

**Formation Intra-Entreprise**

Des formations 100% cybersécurité conçues et délivrées par des experts.
Plus d'information par mail : contact@csb.school ou sur notre site internet www.csb.school

CYBERSECURITY BUSINESS.SCHOOL

39 rue de la Cité - 69003 LYON

# N'étudiez pas la cybersécurité, vivez-la

## Plus qu'un slogan, une réalité à la CSB

En tant que citoyen et professionnel en cybersécurité, j'ai acquis la conviction que l'éducation était la clé pour relever les défis posés par les transitions écologique et numérique, qui convergent et transforment en profondeur le monde dans lequel nous vivons.

Pas de transition écologique sans transition numérique, pas de transition numérique sans cybersécurité.

Cette conviction est partagée par toute l'équipe de la CSB.SCHOOL, qui met son enthousiasme et sa passion au service d'une ambition forte :

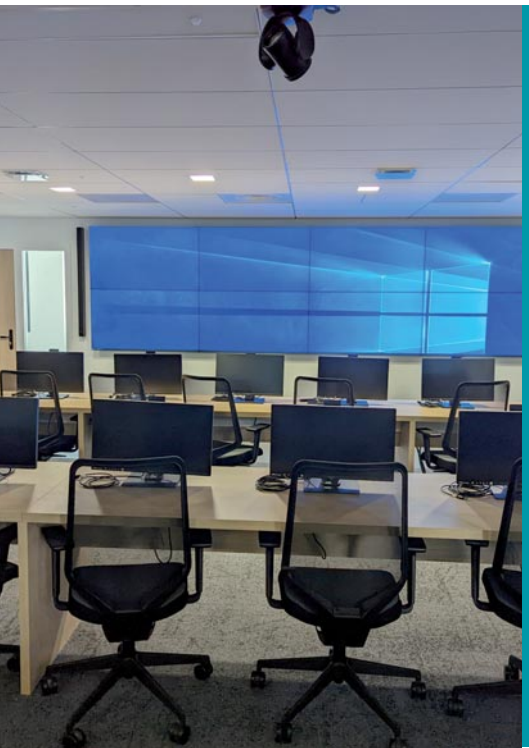
former des talents en cybersécurité qui contribuent aujourd'hui et demain à un monde plus juste, plus sûr, plus responsable.

Cette ambition se traduit par notre engagement à rendre la cybersécurité accessible au plus grand nombre et à soutenir tous les acteurs du secteur, au travers de nos parcours de formation hybride développés par des professionnels de la cybersécurité et de l'enseignement.

Nous sommes animés au quotidien par le plaisir de transmettre et d'apprendre, à vos côtés.

*Patrice Chelim.*
*Directeur de la CSB*

## ZOOM SUR :



Réplique d'un véritable Centre Opérationnel de Sécurité (SOC), il permet aux étudiants de s'exercer au plus près des conditions réelles ; il couvre à la fois les environnements informatiques (IT) et industriels (OT).

Le simulateur est au cœur d'un processus complet de gestion des attaques : de la détection, en passant par le confinement, l'éradication et enfin la remédiation.

Avantde Cliquer .com

L'humain au cœur de la cybersécurité

Vous êtes décideur…

# Divisez /10
## le risque de cyberattaques.

## Développez la vigilance de vos utilisateurs et gagnez en sérénité

STOP

## Pour en finir avec le phishing !

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

# 3 outils complémentaires

en live

**UN AUDIT DE VULNERABILITÉ**

**L'APPRENTISSAGE PAR L'ACTION**

**UN BOUTON ALERTE CYBER**

conçus / hébergés / développés en FRANCE

# Les outils
## Avant de Cliquer

### UN AUDIT DE VULNERABILITÉ

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

### UN BOUTON ALERTE CYBER

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

### L'APPRENTISSAGE PAR L'ACTION

**Un algorithme intelligent**

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


**Notre solution EN VIDEO**

### SENSIBILISATION SUR POSTE DE TRAVAIL

**Envoi d'e-mails de faux phishing**

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

**Une sensibilisation immédiate**

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

**Montée en compétences personnalisée**

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

**Ecrans de veille éducatifs**

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

**Plateforme de e-learning**

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

**Test de la clé USB**

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

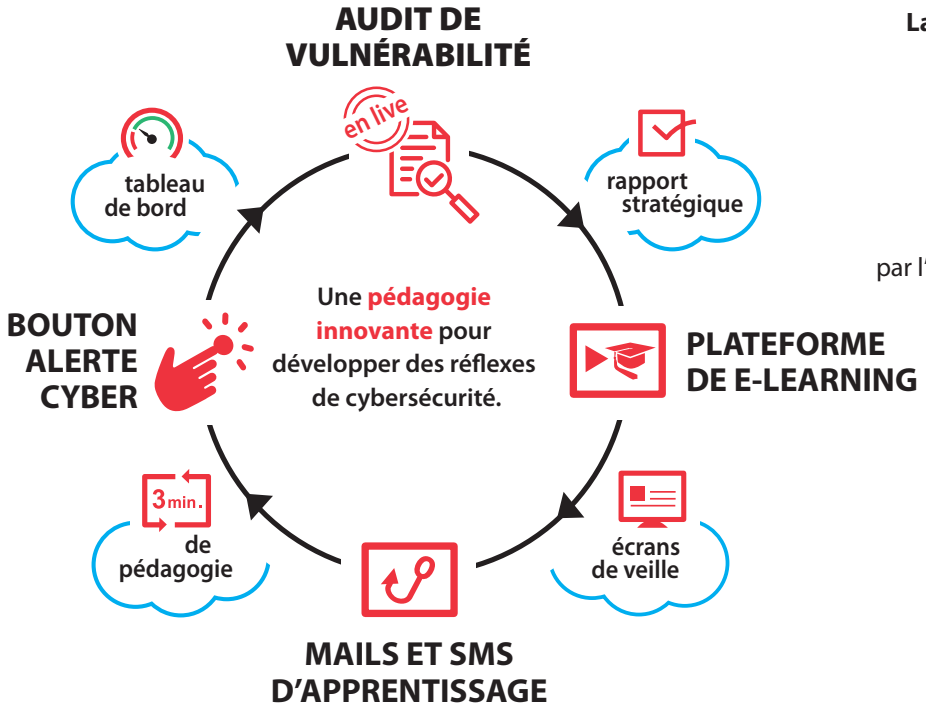
SOLAINN ACHATS INNOVANTS · bpifrance · UNIVERSITE · C.A.I.H. Centrale d'Achat de l'Informatique Hospitalière · Éditeur référencé UGAP-SCC · UGAP · The 2021 French CYBER-SECURITY STARTUPS radar · WAVESTONE

# Les formules
## Avant de Cliquer

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

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

## LA SOLUTION COMPLETE : des réflexes acquis




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

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

**Solution SaaS**

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

### 2 MOIS EN TASK FORCE : parer à l'urgence

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

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

# Vous êtes décideur…

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

## RGPD

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

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

**Avant de Cliquer** en 2021 c'est :

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

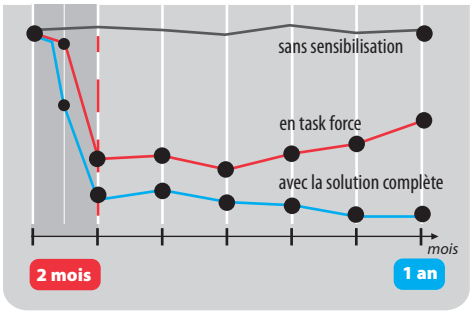
**13 langues sous-titrées Français/anglais**
*Allemand, Anglais, Bulgare, Espagnol, Hongrois, Italien, Mandarin, Polonais, Portugais, Roumain, Russe, Turque, Ukrainien.*

## Niveau de risque

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

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

### Evolution des clics




Avantde Cliquer .com

**L'humain au cœur de la cybersécurité**

**www.avantdecliquer.com**

Coordination technique et commerciale
**Carl : 06 31 37 41 50**

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

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

**Référencé CAIH**
Centrale d'Achat de l'Informatique Hospitalière

**Bpi France**
Solution pertinente pour sensibiliser les utilisateurs à la cybersécurité

**Référencé UGAP**
L'achat public responsable

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

conçus / hébergés / développés en FRANCE

Conception Limage : 09/2021

# CONCEPT REFENTIEL CHARTE LABEL S.B & B.D "CYBER ÉCO & ÉTHIQUE"

## NOTRE CABINET VOUS ACCOMPAGNE

## PAR UN PILOTAGE ANTICIPÉ, GLOBAL & TRANVERSAL

## Vous souhaitez engager une démarche d'amélioration continue S.B & B.D " Cyber Éco & Éthique " ?

Le concept de « Certification S.B&B.D - Cyber Éco & Éthique » a été dévoilé le 20 juillet 2022 à l'occasion de la présentation de notre Cabinet au Président du Campus Cyber suite à son intégration à l'augmentation du capital social de la Société SAS Campus Cyber.

Porté par des valeurs fortes, et une cause bien plus grande que notre entreprise, nous optons pour une Gouvernance Globale et Transversale des démarches « Sécurité, Conformité & Responsabilité Sociétale » d'Entreprise, en proposant notre « Référentiel S.B&B.D - Cyber Éco & Éthique », s'adressant à toute structure s'engageant à mener des process « Cyber Éco & Éthique », qu'elle soit débutante ou confirmée.

Les objectifs de cette démarche innovante :

- Valoriser tout engagement « Cyber Éco & Éthique ».
- Améliorer la « Qualité » de service et des pratiques.
- Proposer un « Pilotage Anticipé, Global & Transversal ».
- Garantir et maintenir une « Image de confiance ».
- Élargir l'« Attractivité & Valorisation » des acteurs, des périmètres liés.
- Mettre en lumière les « Potentiels & Initiatives » des acteurs concernés.

Le dispositif intègre également un accompagnement à destination des entreprises qui souhaitent lancer une démarche « Cyber Eco & Ethique », ou qui veulent encore progresser dans ces domaines (Qualité-RSE, Conformité & Cybersécurité).

CABINET S.B & B.D
DATA-DROIT PROTECTION ET EXPERTISE

**Pour plus d'informations :**
E-mail : contact@data-protection-expertise.fr
Téléphone : 06.29.51.96.54

# TOUR DE FRANCE DE LA CYBERSÉCURITÉ

#TDFCYBER

ESPACES DÉMOS
TABLES RONDES
FORMATION
NETWORKING
RECRUTEMENT
ATELIERS

@CyberCercle
@CyberTerritoire

# PRÉSENTATION DU CYBERCERCLE

## Missions / Vocation

Le CyberCercle est un cercle de réflexion créé en 2011 lorsque la sécurité numérique – la cybersécurité - n'était encore trop souvent qu'à ses débuts pour de nombreuses organisations et l'apanage des 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 d'échanges privilégiés pour les questions de sécurité et la confiance 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 numérique
- 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, de la défense, des territoires et des collectivités et de sujets thématiques comme la réglementation, l'innovation et la recherche, la formation, l'industrie 4.0, ...

# 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, nous ne devons pas oublier 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 mais aussi 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.

## Les activités

Les activités du CyberCercle s'articulent autour de matinales, de journées de rencontres, de publications et de modules de formation, orchestrées au travers de la définition d'un schéma de cohérence et d'organisation des thèmes et des actions.

En 2021, ce schéma s'est construit principalement autour de 3 thèmes principaux :

- Confiance numérique et **politiques publiques** au niveau national et européen : matinales et paroles d'expert
- Confiance numérique des **territoires** : TDFCyber, matinales Auvergne-Rhône-Alpes, matinales
- Financement de la sécurité numérique : TDFCyber, matinales en région

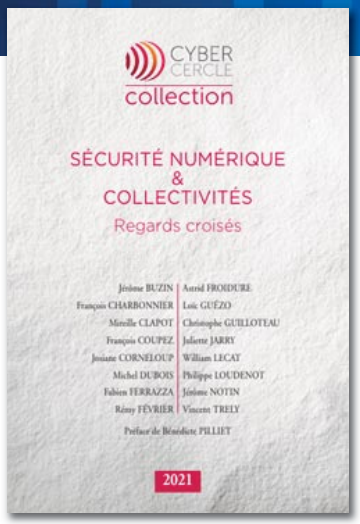

## Positionnement

Le CyberCercle a un positionnement unique.
Il est à la fois un :

- **un « think tank »** par la production de contenus, réflexions et propositions issues de travaux collectifs, par la diffusion d'analyses de personnalités et par son travail d'animation de communautés ;
- **un organisateur d'événements** par la création et la gestion d'événements adaptés pour diffuser les éléments d'acculturation à la sécurité numérique sur l'ensemble du territoire et valoriser le travail parlementaire ;
- **un acteur du conseil et de la formation** pour accompagner les infrastructures dans leur réflexion sur leur politique interne de sécurité numérique ;
- **un cadre d'influence** par son travail avec les pouvoirs publics.

Il représente un **cadre de confiance** qui œuvre sur des sujets d'intérêt collectif, une entité fédératrice en lien et partenariat avec de nombreuses associations et organisations publiques et privées.

Le CyberCercle a souvent été précurseur, parfois suivi ou imité, et après tout tant mieux. Cela montre que nous oeuvrons dans la bonne direction, dans ce domaine où les certitudes sont peu nombreuses et souvent de fausses amies, ce domaine qui demande en permanence d'être à l'écoute, de s'adapter, de réagir mais toujours **au service des métiers et de l'intérêt général**.





CYBER CERCLE PAROLE D'EXPERT

Affronter la tempête cyber



***GCA Éric BUCQUET***
*Directeur de la Direction du Renseignement et de la Sécurité de la Défense (DRSD)*
*Ministère des Armées*

L'attaque *SOLARWINDS* d'une sophistication incroyable visait le pré-positionnement d'agents logiciels dormants dans des systèmes d'information sensibles ou critiques aux États-Unis.

L'attaque de l'opérateur d'oléoducs *COLONIAL PIPELINE* a généré une crise de plusieurs jours sur toute la côte Est des États-Unis privée sa principale source de carburant et de kérosène.

Le récent siphonage des données de 700 millions d'utilisateurs de LinkedIn représente autant de possibilités par rebond de cyber malveillances, d'escroqueries ou de fraudes en tous genres, etc. La revente de données volées à des services de renseignement étrangers est désormais une option qu'il ne faut pas exclure.

Ces trois exemples récents sont symptomatiques du climat cyber actuel. La croissance du nombre d'attaques, de leur diversité, de leur intensité et de leur sophistication ne semble avoir aucune limite, aucune frontière. Les groupes mafieux se sont professionnalisés, certains ont formé des cartels, et ont acquis une telle expertise offensive que certains États n'hésitent pas à faire appel à leurs services

Selon l'agence européenne de cybersécurité (ENISA), 38% des acteurs malveillants seraient rattachés à des États-nations[1].

A quel type d'attaque cybernétique majeure, la France numérisée doit-elle se préparer ?

Les services spécialisés de l'État seront-ils en mesure de prévenir ou de faire face à un cataclysme numérique d'ampleur nationale ? Comment affronter la Tempête Cyber ?

**De l'amplitude et l'intensité d'attaques préoccupantes**

Une prise de conscience progressive de la menace est palpable, mais la réalité de cette dernière est probablement sous-estimée.

Le Président Macron déclarait, le 18 février 2021, à propos de la menace cybernétique, qu'elle était « extrêmement sérieuse, parfois vitale et touchait tous les secteurs ».

Interrogé par la commission des Affaires européennes du Sénat, le directeur général de l'agence européenne de cybersécurité (ENISA), Juhan Lepassaar a donné des chiffres vertigineux. En 2020, le coût des cybercrimes

[1]https://www.enisa.europa.eu/publications/report-files/ETL-translations/fr/etl2020-cyber-espionage-ebook-en-fr.pdf



# Quelques chiffres

**Le CyberCercle en quelques chiffres, depuis 2012 :**

- 111 Matinales à Paris
- 15 Matinales en région
- 35 journées de rencontres
- + de 600 intervenants
- + de 10000 participants
- un réseau de plus de 15000 contacts
- un compte Twitter de + de 10000 followers


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

# MERCI À NOS PARTENAIRES & SOUTIENS


CYBER CERCLE


CYBER CERCLE

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