CYBER CERCLE

24 OCTOBRE 2023
LYON

RENCONTRES CYBERSÉCURITÉ
AUVERGNE-RHÔNE-ALPES

#RCYBERARA
#TDFCYBER

La Région
Auvergne-Rhône-Alpes

DOSSIER PARTICIPANT

RCyberAra

Hôtel de Région - Lyon
24 OCTOBRE 2023

Crédit photo Alain Zimeray

Bénédicte PILLIET
Présidente du CyberCercle

Edito

Dans son Panorama de la Cybermenace 2022, l'ANSSI constate que, si la menace cyber reste élevée, elle touche de moins en moins d'opérateurs régulés et se déporte sur des entités moins bien protégées, que ce soit les collectivités ou les PME-PMI, acteurs de la supply chain. Cela nécessite un « passage à l'échelle » pour rependre les propos de Vincent Strubel, directeur général de l'ANSSI, que nous avons reçu au CyberCercle au début du mois.

Cette évolution, nous l'avions au CyberCercle anticipée dès 2014, en créant notamment des événements fédérateurs et pédagogiques en région, à destination des acteurs publics et privés pour favoriser le développement d'une culture de cybersécurité et renforcer leur résilience face à un risque qui, d'année en année, ne cesse de se développer.

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 en région, susciter des projets fédérateurs, être force de propositions pour les élus… sont les moteurs de notre action et de notre motivation sur les territoires.

C'est le sens de notre dynamique en région Auvergne-Rhône-Alpes depuis 2019.

Cette 5ème édition des Rencontres Cybersécurité Auvergne-Rhône-Alpes s'annonce très riche, autour d'un programme diversifié qui montre le panel très vaste des enjeux de cybersécurité, et des intervenants de grande qualité que je remercie de leur intervention.

Permettre dans un contexte de menace accru, encore renforcé par une situation géopolitique complexe et la perspective des J0 de Paris 2024, 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 deux axes majeurs de cet événement.

Cette journée est une occasion, ici, en Auvergne-Rhône-Alpes, d'échanger sur ces sujets majeurs avec des experts, de travailler ensemble, de mieux connaître les dispositifs dans lesquels les acteurs peuvent s'inscrire pour faire de ce territoire, un territoire plus attractif et plus résilient.

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

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.

Je remercie nos partenaires qui nous permettent le niveau organisationnel de qualité de ces Rencontres : Avant de Cliquer, la Banque des Territoires – Groupe Caisse des Dépôts, BlueFiles, le Groupe La Poste, le CEA, CERTitude NUMERIQUE, CSB.CHOOL, Cybermalveillance.gouv.fr, Elysium Security, ENEDIS, l'ILERI, proofpoint, la Région Auvergne-Rhône-Alpes, Root-Me Pro, le cabinet S.B. & B.D, Stormshield, la Wild Code School.

Je remercie également nos soutiens, collectivités, ministères, 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 inclure l'ensemble des acteurs d'un territoire et de la Nation.

C'est une des raisons pour laquelle nous avons intégré cette année dans cette journée, une nouvelle dimension, « Osez la Cyber », pour que les jeunes puissent découvrir le sujet de la sécurité numérique et de ses métiers au travers d'ateliers interactifs et de « pitchs métier » de professionnels. C'est aussi en s'adressant à la jeunesse que nous ferons de la sécurité numérique un élément de culture partagée par tous.

Un adage célèbre, souvent repris, affirme : « *Seul, on va plus vite. Ensemble, on va plus loin.* » Pour nous au CyberCercle, « *Seul, on ne va nulle part. Ensemble, on va plus loin… et plus vite.* »

Cette 5ème édition des Rencontres de la Cybersécurité Auvergne-Rhône-Alpes s'inscrit dans cette philosophie de plus en plus fondamentale pour faire face collectivement aux enjeux actuels de la sécurité numérique, avec ses impacts économiques, sécuritaires ou sociétaux.

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

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
Gérer une crise cyber : le RETEX de la Mairie d'Aix-les-Bains
François FUMU TAMUZO, Directeur des systèmes d'information, Mairie d'Aix-les-Bains

9h30-10h00
Enjeux de sécurité et Intelligence artificielle
Général de brigade Patrick PERROT, Coordonnateur IA, Gendarmerie Nationale

10h00-10h30
Sûreté - sécurité et cybersécurité
Jérôme SAIZ, Senior advisor, CyberCercle
Kevin GOMART, Senior advisor, CyberCercle

10h30 ■›› **PAUSE CAFE – NETWORKING – ESPACE DE RENCONTRES - STANDS**

11h00 ■›› **WORKSHOPS – DEMONSTRATIONS EN PARALLÈLE**
Deux sessions horaires : à 11h00 et à 11h45

➤ **« L'état de la menace. Comment répondre à cette problématique »**
David EUDELINE, Expert, Avant de Cliquer

➤ **« Le Référentiel de Compétences Cyber »**
Accompagner les prestataires de services informatiques dans le développement de leurs compétences dans ce domaine
Laurent VERDIER, Directeur Formation - Pédagogie et Sensibilisation, Cybermalveillance.gouv.fr

➤ **« Briser la chaîne d'attaque »**
Loïc GUEZO, Directeur Stratégie Cybersécurité, Proofpoint

➤ **« Cybersécurité, aller au-delà du hacking »**
Guillaume COLLARD, Directeur des opérations, CSB.SCHOOL
Thomas SCHEINER, Directeur Général, BPR SECURITY

➤ **« Quels sont les attendus des fonds d'investissement en cybersécurité ? »**
François CHARBONNIER, Investisseur Confiance numérique, Banque des Territoires

➤ **« Mise en œuvre en entreprise d'une filière cybersécurité dans les régions, de la stratégie initiale à la réalisation »**
Sébastien POCHON, Référent cybersécurité en Directions Régionales Auvergne et Limousin, Enedis
Charles-Edouard OUKRAT, RSSI adjoint, Enedis

➤ **« Sortir du syndrome de Kaa et protéger ses données »**
Philippe LOUDENOT, Cyber Security Strategist, BlueFiles

➤ **« MFA et 2FA, de l'attaque à la défense. Connaître les risques pour mieux protéger son environnement »**
Yoan ISSARTEL, co-fondateur, CTO
Adel ALLAM, consultant cybersécurité, Elysium Security – Root-ME-PRO

➤ **« Améliorer l'efficacité opérationnelle Cyber dans votre organisation : démonstration technique de l'XDR »**
Julien PAFFUMI, Product Portfolio Manager, Stormshield

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

14h30 à 16h30
■›› SESSION ATELIERS (RÉSERVÉS AUX PROFESSIONNELS) ET CONFERENCE (OUVERTE)
Les participants sont invités à choisir de participer à un des ateliers ou à la conférence.
Placés sous les règles de Chatham House, les ateliers durent deux heures 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. A l'issue une fiche est réalisée avec « point de situation, enjeux, défis et propositions ».

➤ **CONFERENCE OUVERTE**
Les serious games comme outils de sensibilisation à la cybersecurité : présentation
Thibault RENARD, Expert en intelligence économique et prospective - Animateur de la Commission « Manipulations de l'information », Association des auditeurs IE de l'IHEDN - Senior advisor, CyberCercle

➤ **ATELIER 1**
La Charte Informatique : un document majeur de la protection cyber des employeurs et des collaborateurs pour toute organisation
Maître François COUPEZ, Avocat - Senior advisor, CyberCercle

➤ **ATELIER 2**
Cybersécurité, IA & innovation
Général de brigade Patrick PERROT, Coordonnateur pour l'IA, Gendarmerie Nationale
Bruno CHARRAT, Adjoint au directeur de la recherche technologique, CEA
Dr Michel DUBOIS, Directeur technique, Direction de la Cybersécurité, Groupe la Poste
Guillaume COLLARD, Directeur des opérations, CSB.SCHOOL

➤ **ATELIER 3**
Sécurité économique, sécurité numérique : protéger l'information, valeur de l'entreprise, à l'heure du numérique
Philippe LOUDENOT, Cyber Evangelist, BlueFiles
Alix MADET, Déléguée régionale à la sécurité économique, SISSE

➤ **ATELIER 4**
Cybersécurité industrielle : enjeux et spécificités
Thomas SCHEINER, Directeur Général, BPR SECURITY
Vincent NICAISE, Industrial Partnership & Ecosystem Manager, Stormshield

➤ **ATELIER 5**
Les étapes clefs de la gestion de crise cyber – atelier interactif
Jérôme SAIZ, Senior advisor, CyberCercle
Laurent VERDIER, Directeur Formation - Pédagogie et Sensibilisation, Cybermalveillance.gouv.fr
Didier LAGE, Commandant Divisionnaire Honoraire, Réserviste coordonnateur, Chargé de prévention Cybermenaces, Réseau des experts cybermenaces, Direction zonale de la police judiciaire de Lyon

16h30 à 17h30
■›› RAFRAICHISSEMENT - NETWORKING - ESPACE DE RENCONTRES - STANDS

Les intervenants

Renaud PFEFFER

Vice-président délégué à la sécurité
Région Auvergne-Rhône-Alpes

©DR Renaud Pfeffer

François FUMU TAMUZO

Directeur des systèmes d'information
Mairie d'Aix-les-Bains

Général de brigade Patrick PERROT

Coordonnateur IA et stratégie de la donnée
Gendarmerie Nationale

Officier de gendarmerie, docteur en intelligence artificielle (IA), le général de brigade Patrick Perrot a combiné des fonctions de commandement opérationnel à l'exercice de la science dans la lutte contre la criminalité. Auteur de différentes publications dans le domaine de l'intelligence artificielle, des sciences forensiques comme du renseignement, il est à l'origine de nombreux développements en IA au profit de la sécurité : reconnaissance de locuteur, reconnaissance faciale, analyse décisionnelle et est également en charge d'enseignement au sein de différentes universités. Il est chercheur associé au sein de la Chaire Law, Accountability and Social Trust in AI portée par la Professeure Céline Castets-Renard, ANITI (Artificial and Natural Intelligence Toulouse Institute).
Actuellement au Service de la Transformation, il occupe la fonction de coordonnateur pour l'intelligence artificielle et chargé de mission Stratégie de la donnée au profit de la Gendarmerie nationale.

Bénédicte PILLIET

Présidente
CyberCercle

Crédit photo Alain Zimeray

Bénédicte Pilliet est depuis 2011 présidente du CyberCercle, cercle de réflexion, d'échanges et de rencontres sur la sécurité et la confiance numériques qu'elle a créé. Diplômée de Sciences Po Paris, elle 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 est créatrice et responsable pédagogique du Certificat Sécurité Numérique à l'Université Paris-Dauphine et du séminaire "Politiques publiques de cybersécurité et Relations Internationales" du M2 "Politiques de Défense-Sécurité et RI" à l'Université de Toulouse 1 Capitole. Femme engagée, elle est Lieutenant-colonel de réserve (citoyenne) de l'armée de Terre depuis 2007, membre du Cercle Fontenoy, et a œuvré en tant que responsable du rayonnement pour la Réserve Citoyenne de Cyberdéfense de 2012 à 2018. Elle est également membre fondateur du Cercle K2 et membre du CESIN. Bénédicte Pilliet est titulaire de la Médaille de la Défense nationale, échelon or, agrafe cyber, et de la Médaille des Services Militaires Volontaires, échelon bronze.

Jérôme SAIZ

Senior advisor
CyberCercle

Jérôme SAIZ est consultant en protection des entreprises et fondateur de la société OPFOR Intelligence, où il accompagne les entreprises dans la gestion des crises cyber. Il intervient également en tant que Crisis Manager & Incident Handler @ CERT-Intrinsec.
Il est auditeur de l'Institut National des Hautes Etudes pour la Sécurité et la Justice (18e session SNS), titulaire du titre RNCP-1 d'expert en protection des entreprises et certifié CT CERIC en sûreté / lutte contre la malveillance par le Centre National de Prévention et de Protection (CNPP), réserviste citoyen auprès de la Mission Numérique de la Gendarmerie Nationale, membre du Cybersecurity and cybercrime Advisors Network (CyAN) et senior advisor du CyberCercle.
Jérôme SAIZ a été auparavant expert sécurité, responsable de la communauté RSSI au sein de la société Qualys, un éditeur de solutions d'analyses de vulnérabilités, et journaliste spécialisé dans les questions de cyberdéfense. Il a enseigné durant 11 ans à l'école d'ingénieurs EPITA (cycle Systèmes, Réseaux & Sécurité) et au Centre National de Prévention et de Protection. Il intervient également au profit de nombreux autres centres d'enseignements (Université Paris Dauphine, Pôle Universitaire Léonard de Vinci, etc.).

Kevin GOMART

Senior advisor
CyberCercle

Diplômé de l'université Paris XI en informatique, de l'ICN Business School et de l'université Paris II Pantheon-Assas en science politique, Kevin Gomart a débuté sa carrière par un service militaire volontaire comme chef de bureau au sein d'une unité commando de la Marine Nationale. Entré par la suite au Ministère de l'intérieur comme chargé de mission sécurité économique, il évolue jusqu'à être nommé adjoint au chef d'une unité en charge du traitement de la menace cyber.
Expert en protection globale des entreprises, diplômé de l'IHEMI (Institut des Hautes Études du Ministère de l'Interieur, ex-INHESJ), il rejoindra en février 2019 le groupe IDEMIA en tant que responsable de la conformité sécuritaire. Il est depuis janvier 2021 en charge de la protection physique et de la gestion de crise pour le groupe ainsi qu'Officier de Sécurité.
Il est Senior Advisor du CyberCercle depuis 2018 sur les thématiques de Sûreté et de renseignement.

Laurent VERDIER

Directeur Formation - Pédagogie et Sensibilisation
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.

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.

David EUDELINE

Expert
Avant de Cliquer

Expert engagé dans le domaine de la cybersécurité, il a rejoint l'entreprise Avant de Cliquer en décembre 2022, où il exerce ses compétences pour sensibiliser les individus et les organisations à la sécurité informatique et aux menaces cyber.
Il aime développer les compétences en cybersécurité des utilisateurs et promouvoir la vigilance nécessaire. Grâce à son expertise, il contribue à créer un environnement en ligne plus sûr pour tous.

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.

Les intervenants

Thomas SCHEINER

Directeur Général
BPR SECURITY

Thomas Scheiner travaille depuis 25 ans, à Lyon, dans le conseil et l'ingénierie, toujours comme responsable d'entités opérationnelles, avec succès, dans la data, les infrastructures IT, la pharmacie et dans le secteur nucléaire. Aujourd'hui Directeur Général de BPR.SECURITY, une société de conseil spécialisée en cybersécurité, Thomas met à profit ses compétences pour mener à bien un projet ambitieux entre conseil et formation.

François CHARBONNIER

Investisseur Confiance numérique
Banque des Territoires

François Charbonnier est investisseur à la Caisse des Dépôts, positionné sur les secteurs de confiance et la souveraineté numériques, ainsi que la legaltech. Ingénieur et actuaire de formation, il a antérieurement travaillé à l'Agence nationale de sécurité des systèmes d'information (ANSSI) auprès des différents secteurs privés et sur les réglementations cyber afférentes – LPM et directive NIS.

Sébastien POCHON

Référent cybersécurité
Directions Régionales Auvergne et Limousin
Enedis

Sébastien Pochon est référent cybersécurité en directions régionales Auvergne et Limousin chez Enedis. Son objectif « Déployer la culture de cybersécurité au plus proche des métiers »
Cartographier des risques cyber et définir la maturité de chacune des 2 Directions Régionales,
Proposer et conduire une feuille de route garantissant la mise en oeuvre d'actions de couverture,
Acculturer l'ensemble des salariés aux bonnes pratiques de cybersécurité par la sensibilisation ou la communication – 1600 salariés,
Gérer les incidents locaux avec l'appui technique du pôle cyber national.
Il fût auparavant appui du RSSI Enedis – Pôle Cybersécurité, afin de contribuer au déploiement de la cybersécurité à l'échelle d'Enedis en assurant l'intégration des Directions Régionales dans la filière cyber. Et chargé de mission Sûreté du Patrimoine – Secrétariat Général Enedis pour proposer et déployer un référentiel de solutions avec animations et outils associés au service des processus d'Enedis.

Philippe LOUDENOT

Cyber Security Strategist
BlueFiles

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.
Philippe Loudenot est senior advisor du CyberCercle depuis 2018.

Charles-Edouard OUKRAT

RSSI adjoint
Enedis

Charles-Edouard OUKRAT est Adjoint RSSI d'Enedis, il est en charge de l'animation de la Filière cyber de l'entreprise. Son objectif le renforcement de la Cyber sécurité à travers l'animation d'un réseau de référents cyber présent dans chaque directions d'Enedis.
Membre du CESIN, il a plus de quinze ans expérience en cyber sécurité, avec une expertise particulière sur la gouvernance et l'accompagnement de RSSI et de chefs d'entreprise. Il a aussi eu une carrière d'entrepreneur et a participé à un dépôt de brevet concernant une technologie de zéro-trust adaptée à l'OT.

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, ...

Julien PAFFUMI

Product Portfolio Manager
Stormshield

Julien Paffumi fait ses premières armes au sein de la R&D d'Arkoon, en tant qu'ingénieur Qualité. Il va ensuite former directement les administrateurs et acquiert une connaissance étendue de leurs besoins – expérience précieuse pour son rôle suivant de Product Manager des firewalls Arkoon Fast360, puis de la console d'administration centralisée Stormshield Management Center. En tant que Product Portfolio Manager, il a maintenant un rôle transverse qui lui permet de nourrir son éternelle curiosité avec une approche plus globale des solutions Stormshield.

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.

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).

Thibault RENARD

Senior advisor
CyberCercle

Thibault RENARD est senior advisor du CyberCercle depuis 2018.
Expert Intelligence Economique – Prospective – Anticipation du risque numérique, et après avoir été en poste à la Mission Economique de l'Ambassade de France en Autriche, il a été jusqu'à fin 2019 Responsable Intelligence Economique à CCI FRANCE, établissement national fédérateur et animateur des Chambres de Commerce et d'Industrie. Après deux ans passés ensuite à la DICOD du ministère des armées, il est aujourd'hui à la Direction Générale de l'Armement.
Thibault RENARD est administrateur au syndicat Français de l'Intelligence Economique (Synfie) et animateur de la Commission « Manipulations de l'information » de l'Association des auditeurs IE de l'IHEDN.
Titulaire d'une Maîtrise de Science Physiques et d'un DESS Intelligence Économique et Développement de l'Entreprise, auditeur du Centre des Hautes Etudes du ministère de l'Intérieur (2023), il intervient par ailleurs sur l'Intelligence Economique Européenne et Territoriale, sur l'Esprit Critique, ainsi qu'en Sensibilisation à la cybersécurité via le multimédia, en écoles de Commerce et d'Ingénieur, universités et instituts (IHEDN).

Maître François COUPEZ

Senior advisor
CyberCercle

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).

Les intervenants

Bruno CHARRAT

Adjoint au directeur de la recherche technologique
CEA

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

Vincent NICAISE

Industrial Partnership & Ecosystem Manager
Stormshield

Vincent Nicaise est en charge du développement des partenariats technologiques et commerciaux avec les acteurs de l'automatisme et de la cybersécurité industrielle pour Stormshield. Vincent a auparavant contribué à la construction d'une offre de cybersécurité pour l'IoT au sein d'Atos et a développé l'activité commerciale d'une start-up pour une sonde de détection de cyberattaques dédié aux systèmes industriels. Son parcours professionnel lui a permis de travailler depuis plus de 20 ans dans l'édition de logiciel et dont 9 dans le domaine de la cybersécurité industrielle.

Alix MADET

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

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

Didier LAGE

Commandant Divisionnaire Honoraire
Réserviste coordonnateur
Réseau des experts cybermenaces,
Direction zonale de la police judiciaire de Lyon

Didier LAGE, commandant divisionnaire de police honoraire. Actuellement coordonnateur du Réseau des Experts Cyber Menaces (RECyM) de la Direction Nationale de la Police Judiciaire pour la région AURA. Spécialisé en SSI et investigations Cyber depuis le début des années 90 à travers un certain nombre de postes à Interpol, à la Police Scientifique, et au sein d'un groupe de police européen qui a posé les premières "pierres" organisationnelles en matière de lutte contre la délinquance numérique (European Working Party on Information Technology Crime).


RENCONTRES
CYBERSÉCURITÉ
AUVERGNE-RHÔNE-ALPES
MERCI
À NOS
PARTENAIRES
& SOUTIENS

BANQUE des TERRITOIRES

Caisse des Dépôts GROUPE

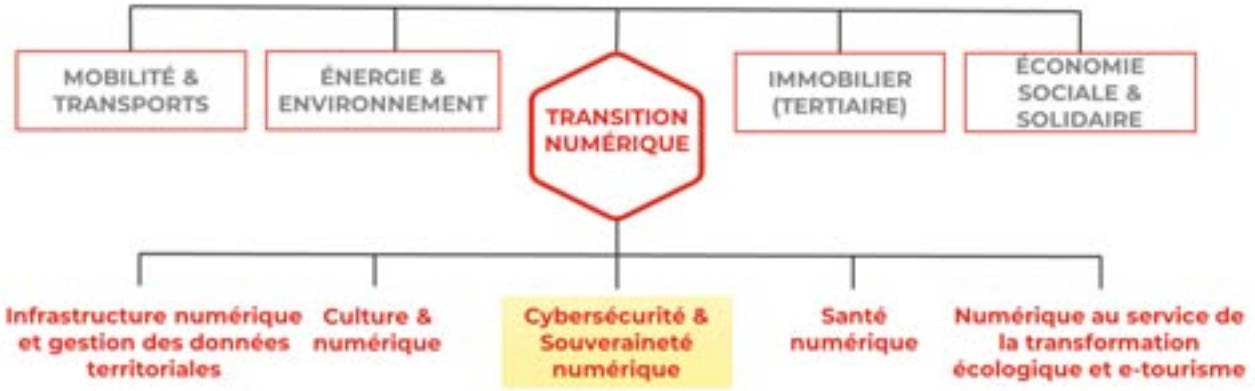
« L'un des 5 métiers du groupe Caisse des dépôts »

Olivier SICHEL
Directeur de la Banque des Territoires

La Banque des Territoires a permis, depuis sa création en 2018, de multiplier les projets essentiels au quotidien, sur tous les territoires.

En cinq ans, nous avons donné vie à une idée si simple qu'elle pouvait sembler utopique : créer, au sein du groupe Caisse des Dépôts, une banque à impacts pour accompagner tous les acteurs des territoires dans la mise en œuvre de leurs projets d'intérêt général.

La Banque des Territoires : un investisseur souverain…



… au service de la sécurité du numérique territorial…

2020 : un positionnement institutionnel sur la sécurité du numérique territorial…

- *Un guide pédagogique à destination des élus des collectivités*
- *4 vidéos de sensibilisation réalisées avec Cybermalveillance.gouv.fr*

… renforcé en 2021 avec l'AMI/AAP « Sécuriser les territoires » (PIA / France 2030)

- *3 projets en environnement hospitalier et collectivités*
- *Une enveloppe de 20 M€ pour faire émerger les solutions de cybersécurité adaptées aux territoires*

… et de son financement direct !

Cibles d'investissement : 3 axes métier

- Cybersécurité
- Confiance & souveraineté numérique
- Economie de la donnée & *datahubs*

Modalités d'investissement

- Startups : amorçage, séries A & B
- Co-entreprises : projets stratégiques
- Réponse aux enjeux des territoires

AvantdeCliquer.com
L'humain au cœur de la cybersécurité

Un programme innovant de sensibilisation AUTOMATIQUE créée SUR MESURE pour développer des réflexes de cybersécurité !

Réduisez le risque d'hameçonnage sereinement grâce à notre Algorithme intelligent.

Avant de Cliquer divise par 10 le risque de cyberattaque grâce à la sensibilisation de vos collaborateurs sans besoin de l'intervention du responsable informatique.

"Ayez l'esprit tranquille, on s'occupe de tout !"

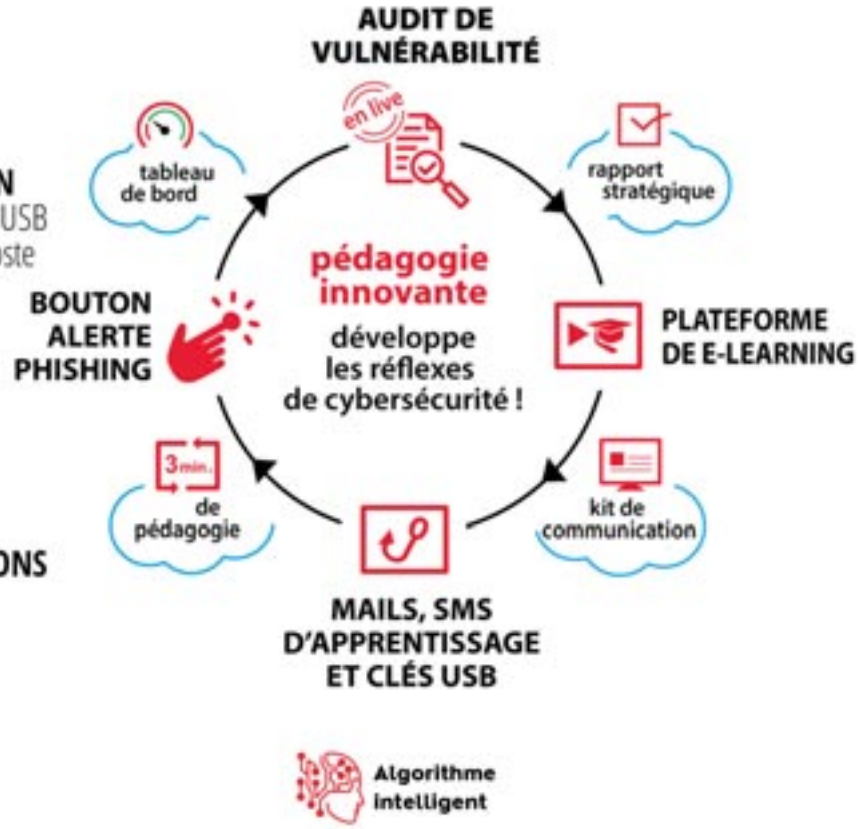
Conçu, crée et hébergé en France

APPRENTISSAGE THÉORIQUE
kit de communication et plateforme d'e-learning

APPRENTISSAGE PAR L'ACTION
E-mails automatiques ciblés, SMS, USB
Sensibilisation immédiate sur le poste

ACCOMPAGNEMENT
Chargé(e) de compte dédié(e),
Actions spécifiques à l'organisation
Programme personnalisé

REMONTÉE D'INFORMATIONS
Tableaux de bord
Bouton Alerte Phishing



Faites de vos collaborateurs des acteurs efficaces de la lutte contre le Phishing.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

LES ESSENTIELS DE VOTRE SÉCURITÉ NUMÉRIQUE

LES MENACES	COMMENT RÉAGIR SI VOUS ÊTES VICTIME ?
L'HAMEÇONNAGE **VOL DE DONNÉES** Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (*phishing*) !	• **NE COMMUNIQUEZ JAMAIS** d'information sensible suite à un message ou un appel téléphonique • Au moindre doute, **CONTACTEZ DIRECTEMENT L'ORGANISME** concerné pour confirmer • **FAITES OPPOSITION** immédiatement (en cas d'arnaque bancaire) • **CHANGEZ VOS MOTS DE PASSE** divulgués/compromis • **DÉPOSEZ PLAINTE** • **SIGNALEZ-LE** sur les sites spécialisés
LES RANÇONGICIELS **EXTORSION D'ARGENT** Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (*ransomware*) !	• **DÉBRANCHEZ LA MACHINE D'INTERNET** et du réseau local • En entreprise, **ALERTEZ LE SUPPORT INFORMATIQUE** • **NE PAYEZ PAS** la rançon • **DÉPOSEZ PLAINTE** • **IDENTIFIEZ ET CORRIGEZ** l'origine de l'infection • Essayez de **DÉSINFECTER LE SYSTÈME** et de déchiffrer les fichiers • **RÉINSTALLEZ LE SYSTÈME** et restaurez les données • **FAITES-VOUS ASSISTER** par des professionnels
L'ARNAQUE AU FAUX SUPPORT TECHNIQUE **ESCROQUERIE FINANCIÈRE** Votre ordinateur est bloqué et on vous demande de rappeler un support technique ? Vous êtes victime d'une arnaque au faux support !	• **NE RÉPONDEZ PAS** • **CONSERVEZ** toutes les preuves • **REDÉMARREZ** votre appareil • **PURGEZ LE CACHE**, supprimez les cookies et réinitialisez les paramètres de votre navigateur • **DÉSINSTALLEZ** tout nouveau programme suspect • Faites une **ANALYSE ANTIVIRUS** • **CHANGEZ TOUS VOS MOTS DE PASSE** • **FAITES OPPOSITION** auprès de votre banque si vous avez payé • **DÉPOSEZ PLAINTE**
LE PIRATAGE DE COMPTE **VOL DE DONNÉES** Vous constatez une activité anormale ou inquiétante sur vos comptes ou applications (messagerie, réseaux sociaux, sites administratifs, banques, sites e-commerce...) ? Vous êtes peut-être victime d'un piratage de compte !	• **CHANGEZ VOTRE MOT DE PASSE** piraté sur tous les sites ou comptes sur lesquels vous pouviez l'utiliser • **VÉRIFIEZ** que les coordonnées de récupération de votre compte (e-mail, téléphone) n'ont pas été modifiées • **PRÉVENEZ VOTRE BANQUE** • **PRÉVENEZ TOUS VOS CONTACTS** de ce piratage • **SAUVEGARDEZ** les preuves • **DÉPOSEZ PLAINTE** si le préjudice le justifie

ATTEIGNEZ LE CŒUR DE L'ÉTAT-MAJOR !

opération hexagone

- **Incarnez de jeunes agents de renseignement en phase finale de formation.** Affrontez vos adversaires en utilisant vos connaissances pour obtenir les précieux badges de renseignement. Le premier à valider le niveau d'habilitation maximal pourra se rendre au cœur de l'État-Major pour remporter la partie.

- **Ce jeu de culture générale ludique et éducatif est bien plus qu'un simple jeu de société.** Son ambition s'inscrit pleinement dans l'axe d'action et d'engagement des Jeunes IHEDN en sensibilisant les joueurs aux thématiques de défense, de sécurité, de mémoire et de citoyenneté !

- **A vous de jouer en participant à notre campagne de financement participatif, c'est par ICI !**

L'intégralité des bénéfices générés seront reversés au **Bleuet de France**.

BlueFiles

ET LA SECURISATION DES ECHANGES DE DONNEES DEVIENT SIMPLE.

SÉCURITÉ SIMPLICITÉ 4S SOUVERAINETÉ SOBRIÉTÉ

Vous avez besoin de recevoir :

- Des pièces dans une démarche de recrutement ;
- Le rapport d'audit que vous attendez ;
- Des informations sensibles ;
- Le plan de votre commanditaire ;
- ...

Vous avez besoin d'envoyer des informations :

- Sensibles (RH, R&D, contrats, audits, bilan comptable, actes, etc.) ;
- Des pièces jointes volumineuses ;
- Protégées par la loi ;
- ...

Ces informations proviennent ou sont envoyées par des personnes ou des structures ayant ou non la solution BlueFiles :

- Prospects, clients, fournisseurs, commanditaires, avocats, professionnels de santé, experts comptables, etc.

Vous cherchez une solution qui soit :

- Simple à utiliser ;
- Souveraine ;
- Le moyen d'embarquer vos équipes à la protection des informations et à la sécurité numérique.

ADDIN OUTLOOK

PAGE DE DÉPÔT

JUSQU'À 4GO/ENVOI

RÉPONSE SÉCURISÉE

ACCUSÉ RÉCEPTION ET TRAÇABILITÉ

AUTOMATISATION

ET BIEN D'AUTRES : LDAP, SSO, 2FA COMPTES PARTAGÉS, FORMULAIRES...

CONTACTEZ NOUS DES MAINTENANT

contact@bluefiles.com

https://bluefiles.com

Il y a plus simple et surtout plus sûr pour sécuriser vos échanges de données sensibles de bout en bout !

BlueFiles

ET LA SECURISATION DES ECHANGES DE DONNEES DEVIENT SIMPLE.

Avec BlueFiles, vous faites le choix d'une solution de confiance qui vous accompagnera pour délivrer le meilleur de la protection des transferts de données, au service de votre entreprise et de vos partenaires dans un cadre éthique et souverain

C'est LA solution d'échange sécurisé d'emails et de fichiers, même volumineux, pour apporter sécurité, simplicité et traçabilité sur les échanges de données sensibles de vos collaborateurs.

- CHIFFREMENT DE BOUT EN BOUT
- VISA DE SECURITÉ DE L'ANSSI
- QUALIFIQUATION SECNUMCLOUD
- CERTIFICATION HDS

BlueFiles permet à votre entreprise d'être conforme avec les attentes réglementaires en garantissant facilement la sécurité et la confidentialité des échanges de données sensibles et à caractères personnels avec l'extérieur de votre entreprise, que le destinataire soit détenteur de BlueFiles ou non (pas d'installation de client lourd).

4S

https://bluefiles.com

proofpoint.

CORPORATE OVERVIEW

Protect people. Defend data.

Combat advanced threats. Protect your data. Modernize compliance.

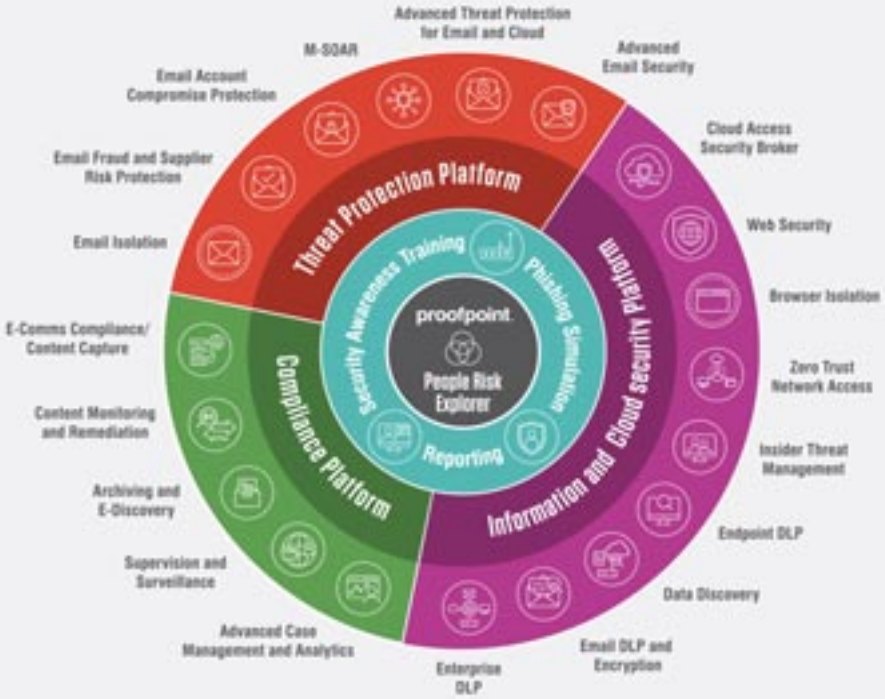
Today's cyber attacks target people, not just technology.

Attackers know your people are the easiest way into your organization. Defend them. Protect them. Empower them with Proofpoint.

Every day we protect the people at more Fortune 500 and Global 2000 organizations than anyone else.

People-Centric Cybersecurity Solutions

Solutions that work together. Solutions that build on each other. People-centric cybersecurity solutions to keep your business secure, in compliance and thriving.



Threat Protection Platform

Email and the cloud are today's primary attack vectors. Fight back with a people-centric approach that blocks attacks, secures cloud accounts and educates users. Our multilayered, holistic approach helps you:

- Secure the gateway and protect email
- Understand who is being attacked and how
- Automate incident response to remediate threats faster
- Change user behavior and help your people protect your organization
- Defend your domain and protect your brand
- Prevent account takeovers
- Prevent web-based threats and secure users' browsing activity

Information and Cloud Security Platform

Data doesn't lose itself. Prevent data loss from malicious, negligent and compromised users by correlating content, user behavior and external threats. Protect your data with better insight and streamlined investigations. Our modern solution helps you:

- Prevent sensitive information from leaking through email
- Safeguard cloud apps and protect users from cloud threats
- Connect the dots between content, user behavior and outside threats
- Manage insider threats and prevent data loss at the endpoint
- Protect confidential data while your employees are on the web

Intelligent Compliance Platform

Data-retention needs are exploding as organizations create more data on more communications platforms. Manage risk with a modern compliance and archiving solution for IT and legal teams. Our cloud-based, people-centric approach helps you:

- Capture and monitor data effortlessly
- Equip your team to scale and manage data growth
- Ease e-discovery and streamline review
- Simplify SEC, FINRA and IIROC compliance
- Ensure compliance on employee social media channels

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. Proofpoint.com

proofpoint.

1200-002-02-04 6/22

QUI SOMMES-NOUS ?

Quel champ d'action ?

Le GIP ACYMA agit contre la cybermalveillance au sens large, sous toutes ses formes et manifestations, quels que soient les supports (ordinateurs, réseaux sociaux, tablettes...) et le public (particuliers, entreprises, associations, administrations), tant qu'il y a une victime, et hors du périmètre d'intervention de l'ANSSI (opérateurs d'importance vitale, opérateurs de services essentiels).

Quelles sont les missions du GIP ?

Créé dans le but de lutter contre les actes de cybermalveillance, le GIP ACYMA mise sur une stratégie d'action articulée autour de trois axes clés :

1. ASSISTER LES VICTIMES D'ACTES DE CYBERMALVEILLANCE

grâce à la plateforme Cybermalveillance.gouv.fr, qui assure un service d'assistance en ligne aux victimes de cybermalveillance et une mise en relation avec des professionnels en cybersécurité référencés sur l'ensemble du territoire.

2. PRÉVENIR LES RISQUES ET SENSIBILISER SUR LA CYBERSÉCURITÉ

avec la réalisation de publications et de campagnes de sensibilisation et de prévention contre les cybermenaces, grâce à des contenus sous différents formats (vidéos, fiches, kit de sensibilisation, affiches, stickers, mémos...) et à travers l'accompagnement à la sécurisation des systèmes d'information des publics professionnels (entreprises, collectivités et associations) par des prestataires labellisés ExpertCyber.

3. OBSERVER ET ANTICIPER LE RISQUE NUMÉRIQUE

grâce à la remontée et l'analyse de données d'utilisation, qui permet d'accroître la connaissance de la menace numérique et ainsi adapter les actions d'assistance et de sensibilisation du dispositif Cybermalveillance.gouv.fr.

Quels publics ?

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

62 membres en 2023

COLLÈGE « ÉTATIQUE »

GOUVERNEMENT
Liberté
Égalité
Fraternité

PREMIÈRE MINISTRE

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

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER

MINISTÈRE DE LA JUSTICE

MINISTÈRE DES ARMÉES

MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

MINISTRE DÉLÉGUÉ CHARGÉ DE LA TRANSITION NUMÉRIQUE ET DES TÉLÉCOMMUNICATIONS

COLLÈGE « UTILISATEURS »

COLLÈGE « PRESTATAIRES »

COLLÈGE « OFFREURS DE SOLUTIONS ET DE SERVICES »

Les membres fondateurs

COLLÈGE « ÉTATIQUE »
- Première Ministre / SGDSN / ANSSI
- Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique
- Ministère de la Justice
- Ministère de l'Intérieur et des Outre-mer

COLLÈGE « UTILISATEURS »
- Association e-Enfance / 3018
- CCI France
- CLCV
- CPME

COLLÈGE « OFFREURS DE SOLUTIONS »
- France Assureurs

COLLÈGE « PRESTATAIRES »
- Cinov Numérique
- CNLL
- La Fédération EBEN
- Numeum

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

CSB.SCHOOL

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

CyberPrépa

Une prépa de 2 ans intégrée au parcours Spécialiste Cybersécurité pour se consacrer pleinement aux exigences du monde professionnel.

Spécialiste Cybersécurité

Conçu pour former les étudiants aux métiers techniques et favoriser leur insertion professionnelle, notre parcours en alternance délivre un Bac+3 reconnu par l'Etat (RNCP n°37987).

Responsable Cybersécurité

Ce programme en alternance sur 2 ans permet de maîtriser le socle de compétences fondamentales nécessaire à la fonction de responsable en cybersécurité (RNCP n°17285).

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

CSB SCHOOL

SUR TOUS LES FRONTS

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 concrètes 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 600K 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

RootMe PRO

pro.root-me.org

STORMSHIELD

Le choix européen de la cybersécurité

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

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'
conférences, atelie
techniques en prise

Que vous souhaitiez pro
développement, tout est

DIRECTION

LA PRO

DÉFE

RÉFLEXIONS SÉCU

SERVICE INTERNATI

INNOVATION CULTURE

UNION EUROPÉENNE SOC

PROSPECT

STRATÉGIE JE

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, e de nombreuses opportunités de ées en engagement concret.

Promouvoir l'expertise innovante

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

a connaissance

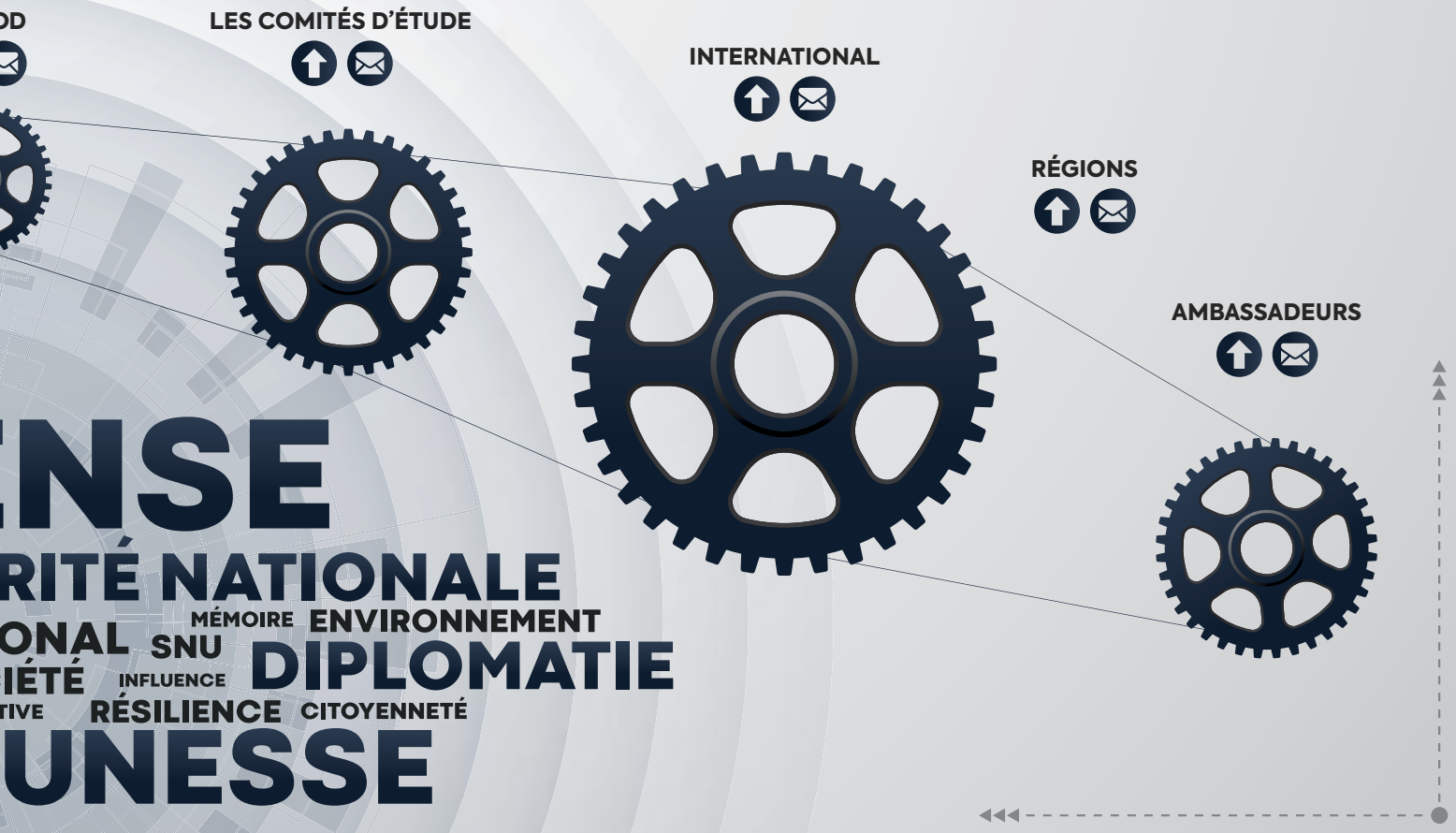
association organise une centaine de rs et visites sur des sujets généralistes ou e avec l'actualité.

Fédérer un réseau international

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

NOTRE ORGANISATION

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



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

CONSIGNES EN CAS DE CYBERATTAQUE

1 DÉBRANCHEZ LA MACHINE D'INTERNET OU DU RÉSEAU INFORMATIQUE

Débranchez le câble réseau et désactivez la connexion Wi-Fi ou les connexions de données pour les appareils mobiles.

2 N'ÉTEIGNEZ PAS L'APPAREIL

Certains éléments de preuve contenus dans la mémoire de l'équipement et nécessaires aux investigations seront effacés s'il est éteint.

3 ALERTEZ AU PLUS VITE VOTRE SUPPORT INFORMATIQUE

Votre support pourra prendre les mesures nécessaires pour contenir, voire réduire, les conséquences de la cyberattaque.

4 N'UTILISEZ PLUS L'ÉQUIPEMENT POTENTIELLEMENT COMPROMIS

Ne touchez plus à l'appareil pour éviter de supprimer des traces de l'attaque utiles pour les investigations à venir.

5 PRÉVENEZ VOS COLLÈGUES DE L'ATTAQUE EN COURS

Une mauvaise manipulation de la part d'un autre collaborateur pourrait aggraver la situation.

Pour vous informer sur les bonnes pratiques
et les principales menaces en matière de cybersécurité
rendez-vous sur :
www.cybermalveillance.gouv.fr

CABINET S.B & B.D DATA-DROIT PROTECTION ET EXPERTISE - NE PAS REPRODUIRE - NE PAS COMMUNIQUER DOCUMENT CONFIDENTIEL & PRIVE – NO COMMUNICATION & NO COPYRIGHT-V1.24-02-2022

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

CYBERCERCLE 2022 EN PHOTOS

CYBER CERCLE

CYBER CERCLE

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

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, ...

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.

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.

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

- Confiance numérique et politiques publiques au niveau national et européen
- Confiance numérique des territoires
- Financement de la sécurité numérique

Positionnement

Le CyberCercle a un positionnement unique.

Il est à la fois :

- 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.

Le CyberCercle depuis 2012

- 121 Matinales à Paris
- 23 Matinales en région (depuis 2019)
- 4 Matinées Défense & Cyber (depuis 2022)
- 37 journées de Rencontres
- + de 670 intervenants
- + de 10000 participants
- 106 Paroles d'Experts (depuis 2020)
- 22 senior advisors et ambassadeurs en région

MERCI À NOS PARTENAIRES & SOUTIENS

CYBER CERCLE

92 Cours Lafayette - 69003 Lyon • contact@cybercercle.com • cybercercle.com • @CyberCercle